People's Democratic Republic of Algeria

Ministry of Higher Education and Scientific Research

Abbes Laghrour- Khenchela-University

Faculty of economic-commercial and management sciences

Comparative Study On E-Authentication in E-Commerce

_Blockchain or Key Management Infrastructure

A Dissertation Submitted in Partial Fulfillment of the Requirements for the degree of Master

Submitted by:

- *Benyezza rana razen*

Supervised by:

Dr Nasraoui Dounia Zed

Board of examiners

EXAMINER	Dr. Nahid Habaz	KHENCHELA UNIVERSITY
SUPERVISOR	Dr. Nasraoui Dounia Zed	KHENCHELA UNIVERSITY
CHAIRPERSON	Dr. Hamrit Mohcene	KHENCHELA UNIVERSITY

JUNE 2024

Acknowledgements

In the name of ALLAH, the most gracious, the most merciful

We would first like to express our sincere and deepest gratitude to our supervisor**, Dr Nasraoui Dounia Zed** for her professional help and assistance during the realization of this dissertation.

Our greatest appreciation and thanks go to the board of examiners who accepted to read and evaluate our work through their competences and experiences mainly to **Dr Mohecene Hamrit** as well as to **Dr Nahid Habez**.

We gratefully wish to thank all our teachers to whom we owe all the respect especially , We would also like to thank our participants

Special thanks go to our families and friends for their moral support**.**

You Have Made a Positive Difference

Dedication

This thesis is dedicated to my incredible family.

To my parents, whose unwavering support, endless love, and countless sacrifices have provided me with the foundation to pursue my dreams. Your guidance and encouragement has been my compass throughout this journey. To my siblings, for always believing in me and offering their unwavering support and cheerfulness, which kept me motivated during the toughest times. Your companionship and understanding have been a source of strength and comfort.

To my friends, who have been my pillars of support, providing not only their friendship but also their encouragement and understanding. Your presence in my life has made this journey more enjoyable and bearable.

To my mentors and teachers, whose wisdom and knowledge have profoundly shaped my academic pursuits. Your dedication to teaching and your commitment to my growth have been truly inspirational.

Finally, to everyone who has played a role in this achievement, Your contributions, support, and encouragement have been invaluable, and I am deeply grateful for your presence in my life. This work is a testament to your belief in me and your unwavering support. Thank you for being a part of this journey.

Declaration

I hereby declare that the thesis entitled (Comparative Study on: E-Authentication in E-Commerce: Blockchain and Key Management Infrastructure) is original work prepared by me for the school year 2023/2024.

List of Main Abbreviation

BT: Blockchain Technology

E- A: Electronic Authentication

E-C: Electroni Commerce

KMI: Key Management Infastructure

T: Technolgy

List of Tables

List of Figures

List of Contents

Abstract

Doubtlessly, in the realm of E-Commerce technology plays pivotal role. Thus the rapid growth of current e-commerce has necessitated the development of robust electronic authentication (EA) mechanisms to ensure secure, valid and trustworthy transactions. Consequently, the current research aims to examine carefully the integration of blockchain technology and key management infrastructure (KMI) as outstanding pivotal solutions for enhancing electronic authentication in e-commerce, in a comparative study. Worthy noted that Blockchain, with its decentralized ledger, offers unparalleled security, transparency, and traceability, making it an ideal way for securing e-commerce transactions. Compared with KMI, the later provides essential services for the generation, storage, distribution, as well as management of cryptographic keys, which are extremely essential to secure communication and data protection. Therefore, this humble work underscores carefully the synergy between blockchain and KMI, demonstrating how their coupled usage can fortify electronic authentication processes. The research method adopted by the researcher is a comprehensive analysis of these technologies; this research aims to present a high quality framework that addresses current challenges in e-commerce security, ultimately contributing to the development of more resilient and trustworthy online commercial platforms.

Key Words:

Blockchain, KMI, E-Commerece, Comparative research.

Introduction

Interestingly, in the realm of e-commerce, security and privacy prove to be extremely important aspects, they are paramount concerns. As online stores, they handle a plethora of transactions, ranging from credit and debit card payments to electronic transfers (E Transfer) and platforms such as PayPal. Additionally, due to the sheer volume of financial transactions conducted on e-commerce platforms, they have become prime targets for cyberattacks. Consequently, they face a higher risk of being breached compared to other types of websites, thus e-commerce sector recognizes the urgency of addressing these security challenges and is in a continual process of bolstering its defenses. While efforts to educate customers on safe online practices are essential, they alone are insufficient. Consequently, e-commerce businesses are under pressure to enhance their security infrastructure to effectively combat evolving cyber threats and safeguard sensitive customer data.

Actually, security is important and necessary since e-commerce is become exponentially more popular, security is a top priority for all e-commerce businesses not only merchants in shopping, and yet any company that uses the internet for important transactions. It's a highly practical way to spend money on things you want to buy. However, to guarantee the confidence and ongoing in

order to maintain the trust and confidence of its customers, e-commerce websites need to be able to offer a higher level of security than the norm. This way, customers' personal and financial information will be protected against potential threats and their shopping experience will be safe and secure.

The topic of E-commerce authentification gains popularity and credence among recent researchers, Various studies highlight the importance of Blockchain and KMI in E authentification in E commerce. To name few, Friedman (2000), Whitten (2002), Basu (2003), Wang et al, (2009).

However little studies compared Blockchain and KMI technologies, on regard of this, and the major concern of this work is to empower the prosperity of E-commerce.

Research Main Question

For high quality secure E-commerce, this humble work aims to answer the primary research question:

1- How can the integration of blockchain technology and key management infrastructure (KMI) enhance electronic authentication in e-commerce to improve security and trustworthiness?

Actually minor research questions can be:

2- What are the similarities as well as the differences between both Blochchain technology and Key Management Infrastructure?
3- Which is the best for e-authentification, blockchain or key management infrastructure? Is it effective to couple both technologies?

Hypothesis of the Research

Based on the above mentioned research main questions, the researcher hypothesized that:

H1 Hypothesis: It is extremely effective to couple Blockchain technology with KMI for high quality authentication of E-commerce. In other words, the integration of blockchain technology with key management infrastructure (KMI) is effective since it significantly enhances the security and trustworthiness of electronic authentication in e-commerce by providing decentralized, immutable transaction records and robust cryptographic key management.

~~**H0 Null Hypothesis: The integration of both Blockchain and KMI is not effective for high quality e-commerce.**~~

The Aim of the Research Study

Interestingly, the primary concern aim of the research study is to critically investigate and demonstrate how the integration use of blockchain technology and key management infrastructure can maximize the effectiveness of electronic authentication in e-commerce, consequently enhancing the safe security and reliability of online transactions.

Other main aims can be stated as follow:

1. To Critically examine carefully the limitations of electronic authentication in e-commerce, by investigating the common challenges faced by consumers.

2. To compare in detailed study blockchain technology in providing secure, transparent, and tamper-proof transaction records with KMI technology. And in the same time to evaluate deeply the role of key management infrastructure in generating, storing, distributing, and managing cryptographic keys securely.

3. To generate wisely a high quality comprehensive framework wherein we couple blockchain and KMI to improve electronic authentication in e-commerec.

The Research Methodology

Unquestionably, in order to address critically the research above mentioned questions and test the validity of the research hypothesis, this work will employ a mixed method research approach, through combining qualitative

and quantitative methods to provide a comprehensive deep analysis. The researcher opted for explanatory sequential mixed methods design via the use of both online questionnaire coupled with an in depth interview with experts. The integration of numerical statistics and non-numerical findings will provide us with clear insights refarding the possibility and effectiveness of coupling Blockchain and KMI for effectice authentification in e-commerce.

The research methodology will include the literature review, presenting existing literature on electronic authentication in e-commerce, blockchain technology, as well as key management infrastructure. The aim behind the review of literature is to critically identify and state current challenges, why not aps, and limitations in the existing electronic authentication mechanisms. Identifying similarities as well as differences. Secondly, we will try to generate a framework wherein we integrate blockchain technology with key management infrastructure for electronic authentication in e-commerce. Stressing the components and functionalities of the framework, including smart contracts, decentralized identity verification, and key management processes. As a trial to collect data on transaction integrity, security breaches, and user trust levels before and after the implementation. Additionally the researcher would employ qualitative methods, via the use of in depth interview and students' attitude questionnaire, the aim is to gather insights from e-commerce platform users and administrators regarding their experiences and trust in the system. Consequently,

this methodology ensures a deep investigation of the research question and a robust validation of the hypothesis, providing valuable insights into the potential of blockchain and key management infrastructure in enhancing electronic authentication in e-commerce.

Remarkably, an extensive literature review will be conducted to establish a theoretical foundation of the topic. The main concern will cover current electronic authentication mechanisms in e-commerce, the inherent challenges and limitations, and the potential benefits of blockchain and KMI. We will draw conclusions from scholarly articles, industry reports, and case studies, the literature review will identify research main gaps in existing research and practice, providing a rationale for the proposed integration of both blockchain as well as KMI. All in all to evaluate the effectiveness of the framework, case studies are used. Well Data collection will involve both quantitative and qualitative methods. First, quantitative data will include metrics such as transaction speed, incidence of security breaches, and the effectiveness of key management processes. Second, qualitative data will be gathered through interview with experts and Questionnaire with e-commerce platform students, capturing their attitudes, experiences, as well as perceptions of security, and levels of trust in the system. Finally, the data gathered will be critically analyzed using statistical tools, tables and figures to measure the framework's impact on electronic authentication. To conclude, the hypothesis 1 that

integrating blockchain and KMI significantly enhances the security and trustworthiness of e-commerce transactions will be tested by drawing general conclusions of both research tools.

To sum up, the current study will conclude with a comprehensive evaluation of the findings. Discussing and highlighting how e-commerce platforms can benefit from coupling both blockchain and KMI for improved electronic authentication. Interestingly the research work would provide valuable insights and practical solutions for maximizing security in e-commerce through the creative integration of blockchain and key management infrastructure.

Chapter one: Theoritical Part Literature Review

Section One: Towards Effective E-Commerce

Introduction

Interestingly, electronic commerce , as refered to e-commerce, stands as the forefront of commercial activities as an extremely significant element of propsperity. That's why it is as an innovative approach to business, encompasses the buying and selling of goods and services through computer networks catering to the requirements of organizations, merchants, and consumers alike, aiming to reduce costs, enhance the quality of goods and services, and expedite the delivery of services. Interestingly, in online marketplaces, both buyers and sellers encounter significant uncertainty. Major concerns include security, trust, authentication, fraud, and risk of loss, which are frequently highlighted as key obstacles to the expansion of e-commerce. A crucial factor contributing to this uncertainty is the impracticality of traditional authentication methods based on physical inspection in the online environment. Merely automating conventional processes from physical marketplaces does not address the authentication challenges in e-commerce (Viriyasitavat, 2019).

Definition of Online Authentication

Without doubt, many definitions where given to online authentification. In this context, online authentication encompasses far more than just identification and validation. Here, we introduce a comprehensive framework for online authentication that offers several practical benefits (Battah, 2021). For example, we highlight the significant temporal aspect of authentication throughout the lifespan of transactional relationships. Additionally, we demonstrate how this framework can be used to evaluate existing authentication mechanisms, thereby aiding in the development of new methods and processes to more effectively authenticate the parties, products, and processes involved in online transactions. First, Authentication has been explored in various contexts, including secure and distributed computing, mobile systems, e-commerce, and autonomous computing. In much of the e-commerce literature, the focus on authentication tends to be confined to identification and identity validation, second, recent empirical studies indicate that consumer trust issues extend beyond mere identification, and these concerns are influenced by a range of demographic and cultural factors as well as site functionality, additionally, several models for trust mechanisms using software agents in autonomous computing environments have been proposed. And yet, there is still a need for systematic comparative research to develop a comprehensive understanding in this area. Aiming to find and

retrieve information for business decision-making, it is also utilized E-commerce is ideally suited to support the widespread business process reengineering that is currently taking place in many companies (Whitten, 2002).

Basic Features of Electronic Commerce

Significantly, it becomes necessary to agree on the basic aspects regarded in electronic commerce thus the pivotal aspect turns basically around processing information. This involves various types of business transactions, which can be broadly categorized as follows: first, interactions pattern that took place between a company and consumers via the use of public networks for home shopping. Such kind does employ encryption to ensure security, along with electronic forms of payment such as credit, debit, or electronic cash tokens (Sarda, 2022). Additionally, we would like to mention transactions with business partners utilizing Electronic Data Interchange (EDI). What is more is that kind of transactions geared towards information acquisition, such as market research involving technologies like barcode scanners for data collection, information processing to aid decision-making, and manipulation of information for tasks related to operations and supply chain management. Without forgetting the transactions aimed at disseminating information to potential customers including basically interactive advertising, sales, and marketing efforts (Bhatti, 2020).

Merits of Electronic commerce

Unquestionably, E-commerce is extremely useful for all consumers. It systematically benefits them in many ways including providing everytime services available during 24/7 operation (such as buying, selling, and browsing). Moreover, it has almost no regional restrictions, serving all consumers. Additionally it provides a large selection of goods and services, coupled with a large selection of payment methods (cash, debit card, credit card, and vouchers).

Electronic Authentication in the Context of E-Commerce

Remarkably, electronic authentication refers to the process of testing an electronic statement, in order to establish a level of confidence in the statement's reliability; in other words it is a critical process designed to verify the identity of users and ensure they are who they claim to be when accessing online services or conducting transactions (Whitten, 2002). This verification is essential for maintaining security, building trust, and preventing fraud in the digital marketplace. Well, it encompasses numerous methods, starting with user identification, which typically includes and necessitates providing a username and password but can also include other identifiers like email addresses or phone numbers. Authentication methods are different, they range from password-based systems, where users enter a strong varied+, complex password, to more advanced techniques like two-factor authentication (2FA), which requires an additional piece of information such as a code sent to a mobile device, and biometric authentication, which uses biological traits such as fingerprints or

facial recognition. Multi-factor authentication (MFA) extends this further by requiring multiple forms of verification from different categories, such as something the user knows (password), something the user has (security token), and something the user is (biometrics). Additionally, digital certificates and public key infrastructure (PKI) play a significant pivotal role, where digital certificates issued by trusted Certificate Authorities (CAs) authenticate users and devices, utilizing cryptographic keys to secure communications and verify identities. Single sign-on (SSO) systems enhance user experience by allowing a one-time authentication process to access multiple systems without repeated logins. Protocols like OAuth and OpenID Connect facilitate this by enabling users to log in using credentials from a trusted third-party service, streamlining the process and boosting security. Security tokens, generating one-time passwords (OTP), and protocols like Secure Sockets Layer (SSL) and Transport Layer Security (TLS), which ensure secure data transmission, further bolster this framework. What is doubly interesting is that, the importance of electronic authentication in e-commerce cannot be overstated as it protects against unauthorized access, data breaches, and fraud, thereby building consumer trust and helping businesses comply with regulations like GDPR, PCI DSS, and other data protection laws. However, the implementation of these systems is not without challenges; user resistance to additional authentication steps, the complexity and cost of advanced systems, and threats such as phishing and

social engineering remain significant concerns. And yet electronic authentication remains a cornerstone of safe secure e-commerce, ensuring transactions are safe, user identities are verified, and sensitive information is well-protected (Yu et al, 2017).

Security Protocols for Authentication

Noticably, it is significant to mention the famous security protocols in e-commerec. Well, there are typical techniques for e-commerce authentication to name few, first a user has tokens that they can use to verify their identity. In the context of authentication for e-commerce, users authenticate themselves via a network application or system. This token needs to be well-guarded and kept hidden or in a secret way. Additionally another technique is security via 36the use of PINs as well as passwords, they are made up of different alphanumeric or/and symbol combinations, making them more secure than predictable regular passwords, worthy noted that users' personal information are protected by creating encrypted channels for data exchange through the use of TLS and SSL during transmission. Moreover, as a user of a banking service or e-commerce website receives a password via SMS message, it's known as SMS-based authentication, this method is the most popular and highly recommended. Furthermore, when using symmetric-key authentication, the user and the authenticating server ought to share a unique key (Knirsch, 2019).

Importance of Electronic Authentication in E-Commerce

Vitally, this study sheds the light on Electronic authentication in e-commerce since it is extremely important in 21st century world of commerce. First of all, Electronic authentication in e-commerce is extremely necessary for several reasons, ensuring the consumers' security, trustworthiness, and smooth operation of online transactions and interactions, as far as it protects against unauthorized access by verifying the identity of users, which is essential step for safeguarding personal and financial information from hackers and cybercriminals. Complete protection againsy cybercrime helps to prevent data breaches and fraud. What is doubly important is that it effectively builds consumer trust. Only if customers guarantee that robust authentication measures are in place, they feel more confident in making purchases and sharing sensitive information online. Gaining Consumers' trust is the key aspect for the success of e-commerce platforms. Furthermore, why do consumers are really in need of electronic authentication since it helps e-commerce businesses comply with various regulatory requirements and standards, including the General Data Protection Regulation (GDPR) and the Payment Card Industry Data Security Standard (PCI DSS). Compliance with these regulations is not only legally mandatory but also demonstrates a commitment to protecting customer data, further enhancing trust and credibility.

What is more is that it balances security with user convenience, in more advanced methods like single sign-on (SSO) and multi-factor authentication (MFA) provide a secure yet seamless user experience, allowing customers to access multiple services with a single login.

Electronic Authentication: Rewarding Yet Challenging Process

Despite the fact that E Authentication has many advantages in e-commerce, many users declare that implementing electronic authentication also presents challenges. First, some users may be boarded by finding additional authentication steps cumbersome, and the complexity and cost of deploying advanced systems can be significant. More than that, users are facing persistent threats including phishing and social engineering that aim to bypass authentication measures. All in all the effective significance of electronic authentication in e-commerce cannot be overstated as it represents a fundamental aspect of ensuring that transactions are secure, user identities are verified, and sensitive information is protected (Sarda, 2022).

Definition of Blockchain

Actually, Blockchain, or "block chain," is a technology for storing and transmitting information that operates without a central controlling entity. Blockchain emerged in 2008 with Bitcoin. Originally, it was designed to create

this new financial asset, referred to as a crypto-asset managed by an algorithm without the intervention of a central authority.

Worthy noted that, the blockchain materializes as a distributed database within a community of users. This database, called a ledger, contains the history of all transactions carried out between users since the creation of the blockchain. Transactions are grouped into a succession of blocks linked together by a cryptographic process. Cryptography (from the Greek "crypto" meaning hidden and "graphy" meaning writing) relies on a mathematical hashing function that transforms input data into a unique numerical identifier, the "hash," ensuring the integrity of the data. This study is set to make significant contributions to e-commerce, cybersecurity, and blockchain technology integration. By thoroughly examining the complex interactions among these areas, the research aims to provide valuable insights for industry professionals, academics, and policymakers. The detailed analysis of current cybersecurity challenges in e-commerce highlights the critical need for improved security measures in digital transactions, emphasizing the importance of this study. By investigating blockchain's potential to enhance data security, ensure transparent transactions, and build trust in e-commerce, this research seeks to introduce transformative changes that could reshape the online business landscape (Bellini, 2020). The study's findings and nuanced understanding of blockchain's strengths and limitations in e-commerce are intended to aid practitioners and decision-makers

in strengthening security protocols and optimizing transactional processes. Additionally, this study is not just a conclusion but a starting point for future researchers, outlining unexplored areas and challenges in this evolving field. By pointing out future research opportunities, potential solutions to current limitations, and the necessity of continued investigation, this study aims to inspire and guide subsequent research. The importance of this research lies in its potential to revolutionize e-commerce security, drive innovation, and create robust, secure, and trustworthy e-commerce platforms that protect user data and build consumer and business confidence. Thus, this study is crucial not only for its immediate findings but also for the roadmap it provides for advancing e-commerce security through blockchain technology integration.

History of Blockchain Technology

Interestingly, According to Resnick and R. Zeckhauser Blockchain technology's origins trace back to 2008, when Satoshi Nakamoto created Bitcoin. Nakamoto introduced blockchain as a decentralized system to track Bitcoin transactions. Initially, people conflated blockchain with Bitcoin, but by 2014, it became clear that blockchain had broader applications beyond digital currency (Bellini, 2020). This realization spurred investments to explore its potential in other fields. While blockchain achieved success with cryptocurrencies like Bitcoin and Ethereum, its secure and decentralized nature allowed it to expand into various sectors such as data sharing, supply chain

management, healthcare, and finance. These sectors adopted blockchain for its ability to ensure data reliability and integrity. Thus, blockchain has evolved from being synonymous with Bitcoin to becoming a versatile technology impacting numerous aspects of the digital world (Battah, 2021).

In e-commerce, blockchain technology proves valuable, particularly in supply chain management. It enables companies to track products from origin to end consumer, creating an immutable and transparent audit trail. This helps verify the authenticity and origin of products, preventing counterfeit items from entering the supply chain (Casino, 2019). Blockchain also streamlines processes like inventory management, order fulfillment, and payment reconciliation, enhancing overall supply chain visibility and reducing inefficiencies. Additionally, blockchain can transform e-commerce payments and financial transactions by enabling direct peer-to-peer transactions, eliminating intermediaries, and reducing delays, fees, and security risks. Smart contracts automate payment settlements based on predefined conditions, reducing fraud and speeding up processing. Moreover, blockchain enhances data security and privacy in e-commerce. It uses encryption to protect personal and transactional information, safeguarding it from unauthorized access. Users gain greater control over their data, allowing them to grant specific permissions and address privacy concerns linked to centralized platforms.

The integration of blockchain in e-commerce aims to enhance transaction security (Casino, 2019) . By implementing a decentralized and tamper-resistant system, blockchain provides a robust framework for securing sensitive transaction data. Advanced cryptographic techniques ensure information integrity, making it difficult for unauthorized parties to tamper with or access critical data. Blockchain's transparency feature fosters trust by allowing all transaction participants real-time access to the same information (Norberg, 2019). Additionally, smart contracts automate and secure the execution of predefined terms in agreements, reducing disputes and increasing the reliability of e-commerce transactions. In summary, using blockchain in e-commerce strategically enhances security measures for online transactions, ensuring the safety and reliability of the digital marketplace.

Needed Aspects in Blokchain Technology

To effectively ensure the use of Blockchain, various aspects are needed. First of all, the identification of each party (including the buyer as well as the seller) is carried out through a cryptographic process, each user has a private key that allows them to sign their transactions, a public key that can only be associated with the private key, enabling the verification of the authenticity and integrity of transactions, additionally, the address, a combination of letters and

numbers derived from the public key and comparable to a bank account identifier, thus the use of the key pair ensures the integrity and security of transactions between users, each identified by their public address (Norberg, 2019) .

Understanding the Blockchain Technology

Interestingly, Blockchain authentication is an innovative process that leverages the decentralized and immutable nature of blockchain technology to verify and secure identities in digital interactions. Understanding it necessitates understanding how the approach utilizes a distributed ledger system where each transaction or piece of data is recorded in a kind of block, linked to previous blocks, and secured through cryptographic hashing. A special feature of blockchain authentication being decentralized; there is no single point of control or failure, as the ledger is maintained by a network of nodes, each having a copy of the entire blockchain, resulting in high availability and resistance to fraud. Moreover, the immutability of blockchain records means that once data is written to the blockchain; it cannot be altered or deleted, providing a permanent and verifiable record of authentication events. Another significant feature is the transparency and traceability of transactions. Regarding these features ob blockchain, each step in the authentication process is logged and can be traced back through the blockchain, making it easy to audit and verify the integrity of the data. It systematically also often employs smart contracts, which are self-

executing contracts with the terms of the agreement directly written into code. Yakubov (2018) declared that these smart contracts can automate authentication processes, reducing the need for intermediaries and enhancing efficiency. Cryptographic techniques, such as public and private keys, are integral to blockchain authentication. Whereby Users are assigned a unique public key and a corresponding private key, which they use to sign transactions and verify their identity (Norberg, 2019) . Blockchain technology has been adopted within the value chain and supply chain sectors to prevent unauthorized access and fraudulent activities. Its implementation ensures data integrity, prevents tampering, and enhances trust, transparency, and comprehensive traceability of transaction records. Researchers present detailed insights into their proposed approach, offering a blockchain-based solution that seamlessly integrates both the value chain and supply chain through the use of a blockchain lattice. The core elements of blockchain concepts integrated into the proposed operational model include a distributed network, a shared ledger, consensus algorithms, and cryptographic digital transactions. Consequently, the PRODCHAIN network enables a fully transparent and secure system.

Blockchain has been a buzzword for a while now, but there's still plenty of confusion on what it is exactly. Although it's closely associated with Bitcoin, blockchain is not a type of cryptocurrency. It's not a programming language. It's a new technology. The blockchain is essentially a completely secure online

ledger that keeps a record of every transaction made at a given place. Blockchain technology enables users to share and securely store digital assets. It has applications for payment processing, product searches, and even customer service. Blockchain enhances the security of online financial transactions, creating a beneficial situation for both brands and buyers. Additionally, it offers numerous other advantages, such as reducing costs, streamlining business processes, accelerating transaction times, and enhancing the overall customer experience (Wang, 2009). Although blockchain technology is relatively new, its growing popularity in ecommerce platforms can be attributed to the significant benefits it offers to both merchants and consumers. Industry experts concur that while blockchain technology holds immense potential, it is still in the early stages of adoption. As it evolves, blockchain is expected to become a fundamental component of the new financial and ecommerce ecosystem.

Merits of Blockchain Technology

Sugnificantly, the Blockchain technology proves to be extremely vital method in e-authentification as well as in e-commerce (Brunner, 2019). Providing users' security is unique feature in itself, the advantages of blockchain authentication are in fact numerous, as it significantly maximizes security by reducing the risk of data breaches and fraud. The decentralized and immutable feature of blockchain makes it extremely difficult for hackers to alter or corrupt the data. Providing top security method, additionally it increases transparency

and trust among parts in e-commerce including users and sellers, due to the fact that all transactions are recorded on a public ledger, users and organizations can verify the authenticity of identities and transactions, fostering greater trust in digital interactions. Moreover it remarkably streamlines and automates processes through smart contracts, reducing administrative overhead and costs associated with manual verification and authentication. Additionally, it provides users with greater control over their personal data. Instead of relying on centralized entities to manage and secure their information, users can control and share their data as needed, enhancing privacy and reducing the risk of misuse. All in all its authentication supports interoperability and scalability, ss it can be integrated across different platforms and services, ensuring consistent and secure authentication in a variety of contexts. To make it short blockchain authentication represents a transformative creative approach to digital identity verification, offering enhanced security, transparency, efficiency, and user control. Finally, Blockchain authentication in e-commerce is increasingly recognized for its potential to revolutionize digital transactions by providing enhanced security, transparency, and efficiency. From various perspectives, including those of consumers, businesses, and regulators, the importance of blockchain authentication in e-commerce is substantial. From the consumer's perspective, blockchain authentication significantly enhances security and privacy. Traditional e-commerce platforms often require users to share sensitive

personal information, which is stored in centralized databases that can be vulnerable to hacking and data breaches. Blockchain, with its decentralized nature, mitigates these risks by distributing data across a network of nodes. Regulators and policymakers view blockchain authentication as a means to enhance compliance and security standards in e-commerce. Blockchain can help ensure compliance with data protection regulations like the General Data Protection Regulation (GDPR) by providing transparent and immutable records of how data is used and shared. This capability can assist businesses in demonstrating their adherence to regulatory requirements, thereby avoiding fines and legal issues. Moreover, the inherent transparency and traceability of blockchain can aid in anti-money laundering (AML) and know-your-customer (KYC) processes, which are critical in preventing illicit activities in the financial aspects of e-commerce. The importance of blockchain authentication in e-commerce extends beyond security and efficiency to encompass broader economic and social impacts. By fostering greater trust and reducing fraud, blockchain can expand market participation, especially in regions where trust in digital transactions is low. This increased participation can drive economic growth and innovation. Additionally, blockchain's potential to provide secure digital identities can empower individuals without access to traditional banking services, promoting financial inclusion. All in all, blockchain authentication in e-commerce offers a multifaceted array of benefits, enhancing security, trust,

and operational efficiency while supporting regulatory compliance and economic inclusion. Its decentralized, transparent, and immutable characteristics make it a powerful tool for addressing many of the challenges faced in the digital commerce landscape today. As the technology continues to change its impact on e-commerce is likely to become even more profound, transforming the way online transactions are conducted and secured.

Barriers to Blockchain Technology

Unfortunately, implementing blockchain authentication in e-commerce entails navigating a landscape with some barriers as well as challenges; it is a rewarding yet challenging journey. First obstacle is scalability, as blockchain networks generaly struggle to handle the high volume of transactions typical in e-commerce environments, while the decentralized feature of blockchain can lead to congestion and delays, impacting transaction processing times and increasing costs. In addition to ensuring a seamless user experience poses another hurdle. Blockchain technology, with its intricate cryptographic mechanisms and management of cryptographic keys, can be daunting for non-technical users. That’s why implementing the Blockchain technology necessitates careful design and a framework to profit effectively and rationally. Additionally, regulatory uncertainty presents complexity in the process itself. E-commerce businesses must contend with a rapidly evolving regulatory landscape governing blockchain and cryptocurrencies. Also, compliance with data

protection, financial transaction, and consumer rights regulations across multiple jurisdictions can be challenging and resource-intensive. More than that, security risks also loom large, in the same regard that blockchain offers robust security features, it is not impervious to threats, furthermore vulnerabilities in smart contracts, weaknesses in consensus mechanisms, and the specter of 51% attacks are among the security risks that e-commerce businesses must address. The costs associated with both implementing and developing blockchain authentication is prohibitive. Blockchain technology is still in its nascent stages, and there is a lack of understanding and awareness among businesses and consumers alike. Overcoming skepticism and resistance to change requires comprehensive education and outreach efforts (Brunner, 2019). Privacy concerns also loom large. While blockchain offers transparency and immutability, it raises questions about data privacy. E-commerce businesses must ensure that sensitive customer information is handled securely and in compliance with privacy regulations. Achieving a balance between transparency and privacy is extremely crucial for maintaining user trust and confidence. To conclude, a collaborative effort from businesses, regulators, and technology providers are urgently needed. Innovation, research, and ongoing development are essential to surmounting the obstacles associated with implementing blockchain authentication in e-commerce (Yakubov , 2018) . Dahal et al. examine the effectiveness of blockchain technology in securing e-commerce transactions and preventing

fraudulent activities. This study explores the application of blockchain across various e-commerce platforms, assessing its capability to enhance transaction security and mitigate fraud risks. The research identifies several benefits of blockchain for securing e-commerce transactions. A key finding highlights the immutability of blockchain records, which prevents tampering with transaction data once recorded. This characteristic significantly hinders fraudulent manipulation, thereby maintaining data authenticity and integrity. Additionally, cryptographic security is emphasized as a vital element that enhances transaction safety in blockchain technology. Techniques such as digital signatures, hash functions, and encryption algorithms ensure secure and confidential transactions, preventing unauthorized access to transaction data.

Another important finding is the role of decentralized consensus in validating and confirming transactions through a network of nodes rather than a central authority. This decentralized approach makes it extremely difficult for fraudsters to manipulate or alter transactions, as compromising numerous nodes is highly challenging. Furthermore, the study highlights the use of smart contracts to automate e-commerce transactions, executing them based on predetermined rules and conditions.

Jiang, Ji et al. (2021) conduct a thorough examination of the integration of blockchain technology into e-commerce platforms, particularly focusing on Small and Medium Enterprises (SMEs). This research establishes a conceptual framework that outlines the structure of blockchain-powered e-commerce platforms specifically designed for SMEs. They identify three primary applications that demonstrate how this platform helps SMEs effectively manage security and privacy concerns. The researchers consider blockchain technology an apt solution for SMEs' challenges, as it ensures the authenticity and transparency of data. By using blockchain to record and track all information, the issue of product counterfeiting is effectively addressed. For SMEs, blockchain's chain structure guarantees data authenticity and transparency, while its encryption algorithm resolves the conflict between data privacy and information sharing. Additionally, smart contracts automate the execution of transactions based on predefined conditions. However, despite the potential of blockchain technology to address privacy and security issues in e-commerce platforms for SMEs, some challenges remain. A significant ongoing issue is ensuring the authenticity of data before it is recorded on the blockchain, which can expose all nodes to the risk of fraudulent or misleading source data. Looking ahead, the integration of blockchain technology into e-commerce presents promising opportunities for exploration and advancement. As the digital landscape evolves, future research should focus on optimizing and refining

blockchain applications to enhance the security of online transactions. Given the ongoing evolution of cyber threats, gaining a comprehensive understanding of how blockchain technology interacts with emerging security challenges is crucial. Exploring innovative approaches to integrate blockchain with other advanced technologies like artificial intelligence and machine learning holds potential for fortifying the e-commerce sector against evolving cyber threats.

Additionally, future research efforts should prioritize the development of standardized protocols and frameworks to facilitate seamless integration of blockchain across diverse e-commerce platforms. Addressing issues such as scalability, interoperability, and user adoption will be essential for the widespread and effective implementation of blockchain solutions. Collaboration between academia, industry experts, and regulatory bodies will be instrumental in creating an enabling environment for blockchain adoption in e-commerce, fostering a secure and resilient digital marketplace.

Furthermore, research initiatives should delve into the socio-economic implications arising from the adoption of blockchain in e-commerce. This investigation should consider aspects such as user trust, regulatory compliance, and the broader economic impact on businesses. Understanding the lasting effects of blockchain integration on consumer behavior and market dynamics

will provide valuable insights necessary for shaping future policies and strategies.

Key Management Infrastruction (KMI)

Interestingly, a Key Management System (KMS) serves as a centralized mechanism for distributing and storing all keys utilized by an organization. It can vary widely, from basic software applications to intricate hardware setups. Basic, open-source options typically use a standard database server to store keys, encrypting them within the database. And yet given the critical nature of key management, a well-designed system should incorporate a hardware security module for key processing, or at least contemplate this as a viable option. In simpler terms, a Key Management System is like a master key holder for an organization, ensuring all keys are kept safe and accessible. While basic systems might use regular computer setups to store encrypted keys, it's crucial to consider adding hardware security measures to enhance protection, especially as the importance of these keys grows.

KMI in E-Commerce

In fact, key management infrastructure (KMI) in e-commerce is extremely issential for ensuring secure transactions and protecting sensitive information of users. It perfectly encompasses the processes, technologies, as well as policies

used to create, distribute, store, and revoke cryptographic keys that encrypt data and authenticate users and devices. Towards enhancing the users' security, effective key management minimizes the risk of unauthorized access, data breaches, and fraud by ensuring that only authorized entities can decrypt and access sensitive information. This involves utilizing secure key generation methods, robust key distribution mechanisms, and rigorous access control measures, what is more is that KMI supports regulatory compliance by maintaining audit trails and facilitating regular key rotation and lifecycle management. In essence, KMI underpins the trust and security necessary for the smooth operation of e-commerce platforms.

Effectiveness of KMI in E-Commerce

Key management infrastructure (KMI) is fundamentally important in e-commerce for multiple reasons. Primarily, it plays a crucial role in data security by ensuring that sensitive information such as customer details, payment data, and personal identifiers are encrypted and protected from unauthorized access. This protection is achieved through the effective management of cryptographic keys, which prevents data breaches and maintains the confidentiality and integrity of information. Additionally, KMI is essential for robust authentication mechanisms, ensuring that only authorized users and systems can access the e-commerce platform. As Yu (2017) mentioned, this level of security fosters trust among customers, who need assurance that their transactions are secure and

their personal data is safe. Furthermore, e-commerce businesses are often subject to various regulations and standards, such as the Payment Card Industry Data Security Standard (PCI DSS) and the General Data Protection Regulation (GDPR). Proper key management helps these businesses comply with such regulations by providing secure encryption and maintaining detailed audit logs. Moreover, KMI significantly contributes to fraud prevention by securely managing keys used in digital signatures and encryption, ensuring that transactions are authentic and protected from tampering. This is crucial for protecting both the business and its customers from fraudulent activities. Additionally, by automating key management processes, e-commerce platforms can reduce the risk of human error, streamline their operations, and ensure that keys are updated and revoked as necessary. This not only improves the overall security posture of the platform but also enhances its operational efficiency and resilience. In essence, KMI is indispensable in e-commerce for safeguarding data, ensuring regulatory compliance, preventing fraud, and optimizing operational processes, all of which are critical for the sustainability and success of online businesses.

Key Aspects of KMI

The key features of key management infrastructure (KMI) in e-commerce are multifaceted and collectively ensure the robust security and smooth operation of online transactions. At its core, KMI provides advanced encryption

techniques to protect sensitive data such as customer information and payment details, safeguarding it from unauthorized access and potential breaches. This involves secure key generation, which creates strong cryptographic keys essential for encrypting and decrypting data. Additionally, KMI encompasses secure key distribution mechanisms, ensuring that keys are safely and efficiently delivered to the appropriate entities without risk of interception. Key storage is another critical feature, where cryptographic keys are stored in secure hardware modules or encrypted databases to prevent unauthorized access or theft. Furthermore, KMI supports comprehensive access control measures, allowing only authorized users and systems to manage or utilize the keys, thereby reinforcing the security of the e-commerce platform. Regular key rotation and lifecycle management are also integral features, involving the periodic updating and revocation of keys to mitigate the risks associated with key compromise and to comply with best security practices (wang, 2009). KMI additionally maintains detailed audit logs, which track all key management activities to provide a transparent and traceable record for compliance with regulations such as PCI DSS and GDPR. These logs are vital for forensic analysis in the event of a security incident, more than that KMI contains automated processes for key management tasks, reducing the likelihood of human error and enhancing operational efficiency. By integrating these features, KMI not only secures sensitive information and transactions but also ensures that e-commerce

businesses can meet regulatory requirements, prevent fraud, and maintain the trust and confidence of their customers and this is why users are demanding.

From Advantages to challenges of KMI

Key management infrastructure (KMI) in e-commerce is extremely effective in raisng the security of all users, though it has several important components that work together to provide strong security and seamless online transaction processing. Fundamentally, KMI offers cutting-edge encryption methods to secure private information, including credit card numbers and client profiles, against theft and other security lapses. This is the process of secure key generation, which yields robust cryptographic keys necessary for data encryption and decryption. Secure key distribution procedures are also included in KMI, guaranteeing that keys are efficiently and safely given to the right parties without running the danger of being intercepted. Another crucial component is key storage, which involves storing cryptographic keys in encrypted databases or safe hardware modules to thwart theft or unwanted access. Moreover, KMI facilitates extensive access control protocols, permitting only approved users.

Towards Effective E- Authentication in E-Commerce: Blockchain or Key Management Infrastucture

A Comparative Study

A comparative study involves between Blockchain technology and KMI is needed, it involves both similarities as well as differences. First of all, Blockchain and key management infrastructure (KMI) prove to be efficient methods of security in e-authentification in e-commerec, worthy noted that both play crucial roles in enhancing security and trust in e-commerce, and yet they operate differently and have distinct applications. As it is previously mentioned, Blockchain is a decentralized ledger technology that ensures transparency, immutability, and security of transactions through cryptographic hashing and distributed consensus mechanisms, enabling systematically secure peer-to-peer transactions without intermediaries, making it ideal for applications like cryptocurrency payments, supply chain tracking, and digital identity verification. While KMI is a also centralized framework that focused on the generation, distribution, storage, and management of cryptographic keys used to encrypt and decrypt data, authenticate users, and secure communications. In the time blockchain provides a transparent and tamper-proof record of transactions, KMI ensures that sensitive data within transactions remains confidential and is

only accessible to authorized parties and this is what users' demande. In one hand, Blockchain's decentralized nature can enhance security and reduce fraud risks but may face scalability and regulatory challenges. On the other hand, KMI, being centralized, offers more straightforward regulatory compliance and control but may present a single point of failure if not properly managed. Interestingly, both technologies are complementary in e-commerce, with blockchain providing a robust framework for transaction integrity and transparency, and KMI ensuring data security and privacy.

Differences between Blockchain and KMI in E- Commerce

Actually, Blockchain and key management infrastructure (KMI) are both critical for carefully securing e-commerce; however they differ fundamentally in many aspects including their design, implementation, as well as use cases, starting with Blockchain , it is a decentralized ledger technology that records transactions across a distributed network of computers, ensuring transparency, immutability, and tamper-proof records as a technology operating on a consensus mechanism, where each transaction is validated by multiple nodes, making it extremely resilient against fraud and hacking attempts in this regard it is particularly well-suited for applications requiring high levels of transparency and trust without relying on a central authority, such as cryptocurrency transactions, supply chain management, and smart contracts, this is in one

part Tschorsch (2016). In contrast, KMI is a centralized framework focused on the management of cryptographic keys used for encrypting data, securing communications between users, and authenticating them. Additionally, KMI encompasses processes such as key generation, distribution, storage, rotation, and revocation, ensuring that only authorized parties can access sensitive information. In the time wherein blockchain ensures that the integrity of transactions is maintained through its distributed ledger, KMI ensures the confidentiality and security of the data within those transactions by controlling access through cryptographic keys. More than that, blockchain's decentralized in its nature can complicate regulatory compliance and scalability, as every node in the network must process every transaction, potentially leading to performance bottlenecks. But, KMI's centralized approach makes compliance more straightforward and allows for more efficient key management practices, despite the fact that it introduces a single point of failure risk if not properly secured. Despite these differences, blockchain and KMI can be complementary; blockchain provides a secure and transparent framework for recording transactions, while KMI enhances security by ensuring that sensitive data is encrypted and accessible only to authorized users. In e-commerce, integrating both technologies can offer a comprehensive security solution that leverages the strengths of each:

blockchain for integrity and transparency, and KMI for confidentiality and access control, and this study appears to meet these demands (Tschorsch, 2016).

Smart Integration of Blockcha in Technology and KMI in E-Commerce

Interestingly, Blockchain and key management infrastructure (KMI) can indeed complement each other in e-commerce by combining their distinct strengths to create a more robust and secure environment. Blockchain provides a decentralized, immutable ledger that enhances transparency, trust, and security in transactions. Its distributed nature ensures that all participants have access to the same verified and tamper-proof records, reducing the risk of fraud and unauthorized alterations. This is particularly valuable for applications like supply chain management, digital identity verification, and financial transactions, where trust and integrity are paramount. On the other hand, KMI offers a centralized system for managing cryptographic keys, which are essential for encrypting data, securing communications, and authenticating users. By ensuring that only authorized parties can access sensitive information, KMI enhances data confidentiality and security (Yu et al, 2017). When integrated, these technologies can address each other's limitations and provide a comprehensive security framework for e-commerce. Blockchain's transparency and immutability can ensure transaction integrity, while KMI's robust key management can protect the confidentiality of the data within those transactions.

For example, blockchain can record transaction details transparently, but the actual data can be encrypted using keys managed by KMI, ensuring that even if the blockchain ledger is public, sensitive information remains secure (Wang et al, 2009). Additionally, KMI can facilitate secure access to blockchain networks by managing the cryptographic keys needed for user authentication and transaction validation. This integration allows e-commerce platforms to leverage the decentralized trust and transparency of blockchain while maintaining strict control over data security and access through KMI. In summary, by combining blockchain's strengths in ensuring data integrity and transparency with KMI's capabilities in managing encryption and access control, e-commerce businesses can achieve a higher level of security, trust, and efficiency. Blockchain and key management infrastructure (KMI) can be coupled together to serve e-commerce by leveraging their complementary strengths to create a highly secure, transparent, and efficient ecosystem. Blockchain's decentralized and immutable ledger technology ensures that every transaction is recorded in a tamper-proof manner across a distributed network, which enhances transparency and trust among all participants as Tschorsch mentioned (2016). This feature is particularly beneficial for e-commerce applications like supply chain management, where the provenance and authenticity of goods need to be tracked reliably, and for digital identity verification, where ensuring the integrity of user information is critical. However, while blockchain excels at maintaining an

unalterable record of transactions, it does not inherently provide robust mechanisms for securing the data within these transactions or controlling access to sensitive information. This is where KMI comes into play, offering centralized management of cryptographic keys that are essential for encrypting data and securing communications. By integrating KMI with blockchain, e-commerce platforms can encrypt sensitive data before it is recorded on the blockchain, ensuring that even if the blockchain ledger is publicly accessible, the data remains confidential and only decipherable by authorized parties. KMI manages the lifecycle of these cryptographic keys, including their generation, distribution, rotation, and revocation, thus providing a secure and efficient means of handling encryption and decryption processes. This integration ensures that while blockchain provides a transparent and immutable record of transactions, the actual data within those transactions is protected against unauthorized access. Moreover, KMI can facilitate secure access to the blockchain network by managing the cryptographic keys required for user authentication and transaction validation. This ensures that only verified and authorized users can initiate or approve transactions on the blockchain, further enhancing security (Brunner, 2019) . For instance, in an e-commerce scenario, when a customer places an order, the transaction details can be recorded on the blockchain for transparency, while the customer's payment information is encrypted and securely managed by KMI. This dual approach protects sensitive

information from breaches and ensures that all transactions are verifiable and tamper-proof. Additionally, the integration of blockchain and KMI can help e-commerce businesses comply with regulatory requirements by maintaining detailed, immutable audit trails (via blockchain) and ensuring data protection through strong encryption (via KMI). This synergy not only enhances security and trust but also improves operational efficiency by automating and streamlining key management processes, reducing the risk of human error, and ensuring that keys are updated and revoked as necessary (Viriyasitavat, 2019).

Conclusion

This study aims to provide comparative study between Blockchain and KMI in electronic authentification in e-commerec. This chapter examines carefully the theoretical part related to e-commerce, Blockchain technology, KMI and integrating them. All in all, coupling blockchain with KMI in e-commerce offers a comprehensive security solution that leverages blockchain's strengths in transparency and immutability with KMI's capabilities in data encryption and access control. This integration ensures secure, transparent, and efficient e-commerce operations, fostering greater trust and confidence among users and stakeholders.

Chapter Two:

Practical

Methodological

Part

Research Methodology

Introduction

Doubtlessly, in the time e-commerce develops each and every day, maintaining transaction security and user authentication continues to be a top priority of all users around the world. That is why two well-known approaches are examined in this comparative study: first of all key management infrastructure (KMI) and secondly blockchain-based authentication. Examining their efficacy, usefulness, and suitability for broad implementation in e-commerce systems is the goal and the primary aim of this methodological work. A mixed methods approach, the researcher opted for the explanatory mixed method design via the use of both Online questionnaire coupled with an in depth interview with experts in the domain of science computing and e-commerce. In other words, the study is conducted via the use of using a multimodal method; the research combines technical analysis, user experience assessment, and market viability analysis. Through a comparison of blockchain and KMI solutions, we want to provide insightful analysis of their relative merits and drawbacks, illuminating which strategy would be more appropriate in different e-commerce scenarios. Interestingly, this study offers useful advice for companies looking to improve their authentication methods in addition to adding

to the body of knowledge on e-commerce security. After a thorough investigation and comparison, we endeavor to empower stakeholders with the knowledge needed to make informed decisions regarding the implementation of authentication mechanisms in e-commerce environments.

Data Collection Tools

1. Computing Science Students' Attitude Online Questionnaire

Actually, the researcher used an online questionnaire, it is a structured research tool designed to gather data from participants in a systematic and standardized manner. Why a questionnaire as it serves as a valuable tool for collecting information on attitudes, opinions, behaviors, and demographics related to the topic under investigation. In this context of the comparative study on e-commerce authentication methods (blockchain or key management infrastructure), a questionnaire is instrumental in eliciting insights from computing science students regarding their perceptions, preferences, and experiences.

The primary concern and objective behind the use of the students' attitude questionnaire is understanding users' perceptions of blockchain and KMI authentication methods, evaluating the usability of each approach, and identifying potential barriers to adoption. The sampling of the questionnaire included 30 students in the science computing department in Abbes Laghrour

University khenchela master two case study, in fact all students responded kindly.

The Attitude Questionnaire Design

Unquestionably, regarding the research major objective, the Students' questionnaire included a mix of closed-ended as well as open-ended questions. Closed-ended questions provide quantitative numerical data that can be easily analyzed, while open-ended questions allow students to provide detailed qualitative non numerical insights. Questions are directly related to e-commerce authentication methods, security, preferences regarding authentication mechanisms, and willingness to adopt new technologies basically the one which integrates both Blockchain technology as well as key management infrustruction.

Piloting the Students' Attitude Online Questionnaire

In fact, 6 experts piloted the questionnaire before sending /sharing it with students of science computing master twi in Abbes Laghrour University in Khenchela. The primary aim of piloting it is to identify any ambiguities, inconsistencies, or problems with the wording of questions. Piloting helps ensure that the questionnaire is clear, comprehensible, and effectively captures the intended information. Interestingly, the questionnaire was administered through online Google form.

Research Data Analysis

Remarkably, after gathering data the researcher analyzed data using statistical techniques for closed-ended questions and thematic analysis for open-ended responses. Quantitative data are analyzed using software tools basically Excel and Jasp, while qualitative data requires manual coding and interpretation to identify recurring themes.

Questionnaire Analysis

Students' Questionnaire

Section One: Students' Personal Information

1. **What is your gender?**

- Male
- Female

Table 1. Students' Gender

Option	Male	Female
Number	**11**	**19**
Percentage	**36.66%**	**63.33%**

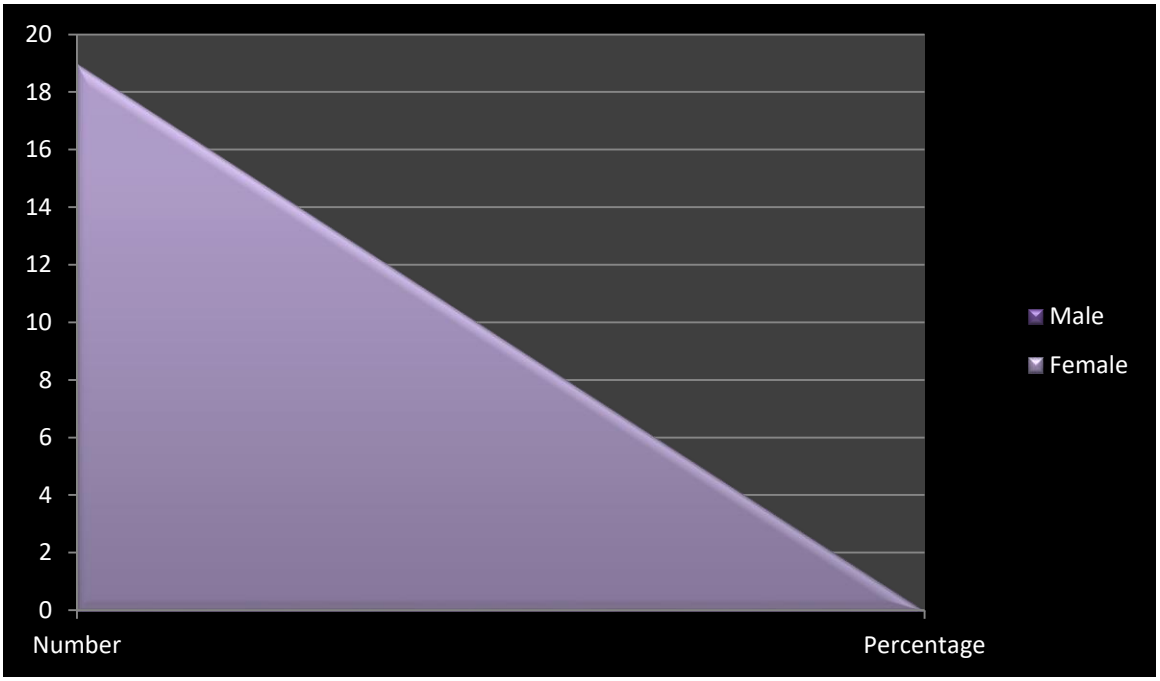

Figure 1. Students' Gender

Actually, the first question aims to collect data on the gender distribution of the students. According to Table as well as figure 1, which detail students' gender, 11 students identified as male, and 19 identified as female, representing 36.66% male and 63.33% female respondents. The higher percentage of female students suggests that the science computing class has a greater representation of females compared to males. Without doubt, the notable difference in percentages highlights the gender composition, which can be a relevant factor in analyzing the responses and understanding the demographic attitudes.

2. **What is your age?**

-23 years old

-25 years old

-More than 25 years old

Table 2. Students' Age

Options	23 Y	25Y	More than 25Y
Number	**05**	**20**	**05**
Percentage	**16.66%**	**66.66%**	**16.66%**

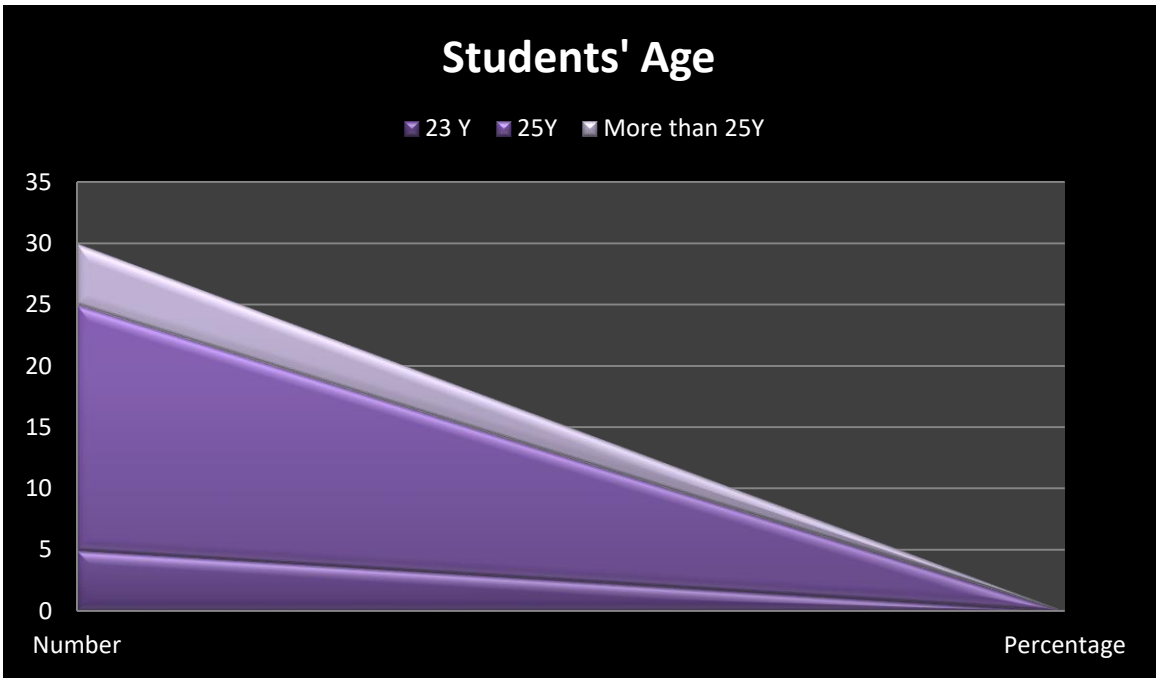

Figure 2. Students' Age

Interestingly, the question two gathers information regarding the age distribution of the students. As presented in Table and figure 2, the age options were 23 years old, 25 years old, and more than 25 years old. In fact, responses show that 5 students, or 16.66%, are 23 years old; 20 students, or 66.66%, are 25 years old; and another 5 students, or 16.66%, are more than 25 years old. Consequently, the majority of the students are 25 years old, making up two-thirds of the respondents when the equal percentage of students who are 23 years old and those who are older than 25 suggests a balanced distribution in these age groups, though significantly smaller compared to the 25-year-old group. The predominance of 25-year-old students might reflect a common age for individuals in this educational level.

Section Two: Blockchain and KMI

3. How familiar are you with crypto currencies?

-Familiar

- Not Familiar

-Very Familiar

Table 3. Students' Familiarity with Crypto Currencies

Options	Familiar	Not Familiar	Very Familiar

Number	**19**	**04**	**07**
Percentage	**63.33%**	**13.33%**	**23.33%**

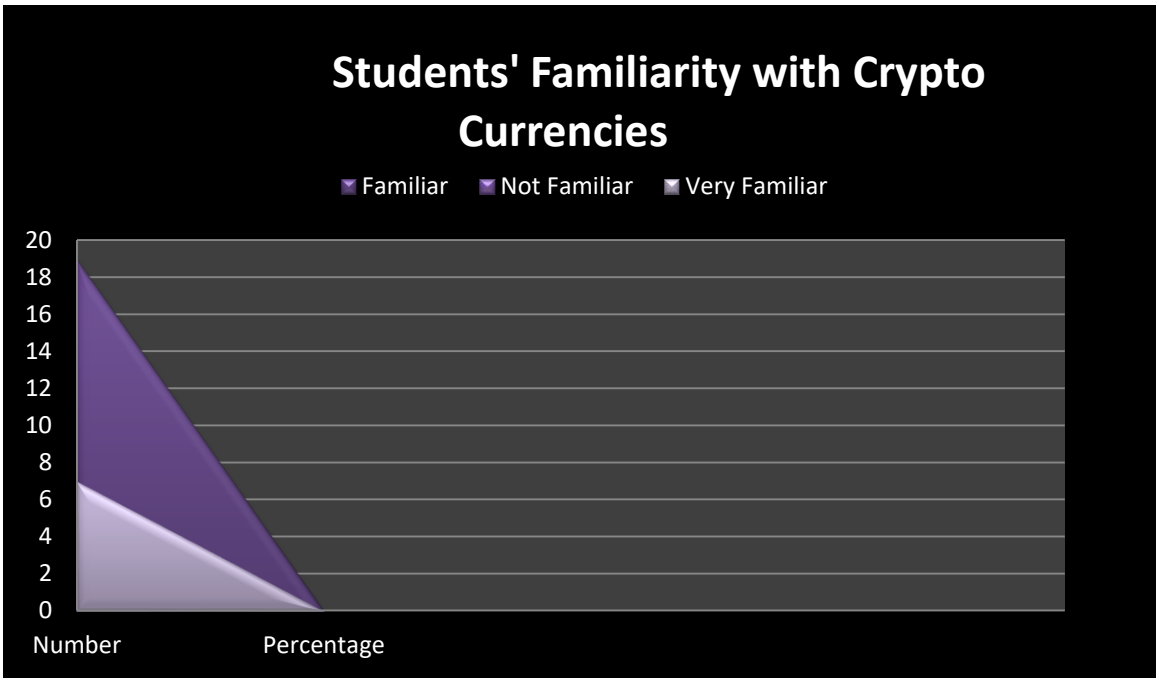

Figure 3. Students' Familiarity with Crypto Currencies

Unquestionably, as the table and figure 3 assess, students' familiarity with cryptocurrencies is marked, as detailed above in Table 3. The options for familiarity were "Familiar," "Not Familiar," and "Very Familiar." Actually, the results show that 19 students, or 63.33%, identified as "Familiar" with cryptocurrencies, while 4 students, or 13.33%, indicated they were "Not Familiar," and 7 students, or 23.33%, stated they were "Very Familiar." Without doubt, findings suggest that a significant majority of the students have at least a basic understanding of cryptocurrencies, with 63.33%

reporting being familiar, while the relatively small percentage of students who are not familiar with cryptocurrencies (13.33%) indicates that most students have some level of exposure to this topic. Additionally, the fact that 23.33% of the respondents consider themselves very familiar with cryptocurrencies shows that there is a substantial group with in-depth knowledge or experience in this area, therefore, this distribution of familiarity levels highlights a strong general awareness and interest in cryptocurrencies among the science computing students.

4. What do you think about blockchain?

Table 4. Blockchain Technology

Options	**Interesting Technology**	**Not Interesting Technology**
Number	**30**	**00**
Percentage	**100%**	**0%**

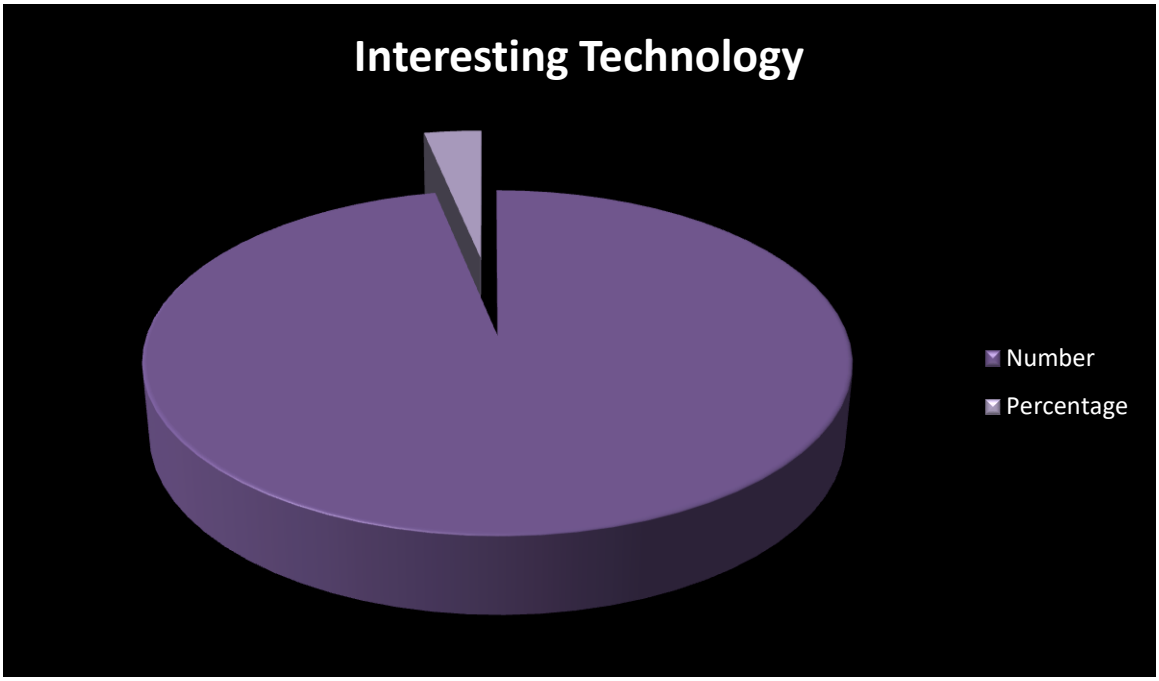

Figure 4. Blockchain Technology

Interestingly, table and figure 4 above explored students' opinions on blockchain technology, as outlined in Table 4. Well, the options were "Interesting Technology" and "Not Interesting Technology." The results were unequivocal: all 30 respondents, representing 100%, found blockchain to be an interesting technology.

The remarkable response indicates a strong and universal interest in blockchain among the students we deduce this since no student found blockchain uninteresting suggests that this technology is highly regarded and likely seen as valuable or important by the entire group. This is due to the fact that be the potential applications and innovations associated with

blockchain, particularly in fields related to science computing. The 100% positive response underscores the enthusiasm and curiosity that blockchain technology generates among students, reflecting its perceived relevance and importance in their academic and possibly future professional pursuits.

5. What is blockchain good for?

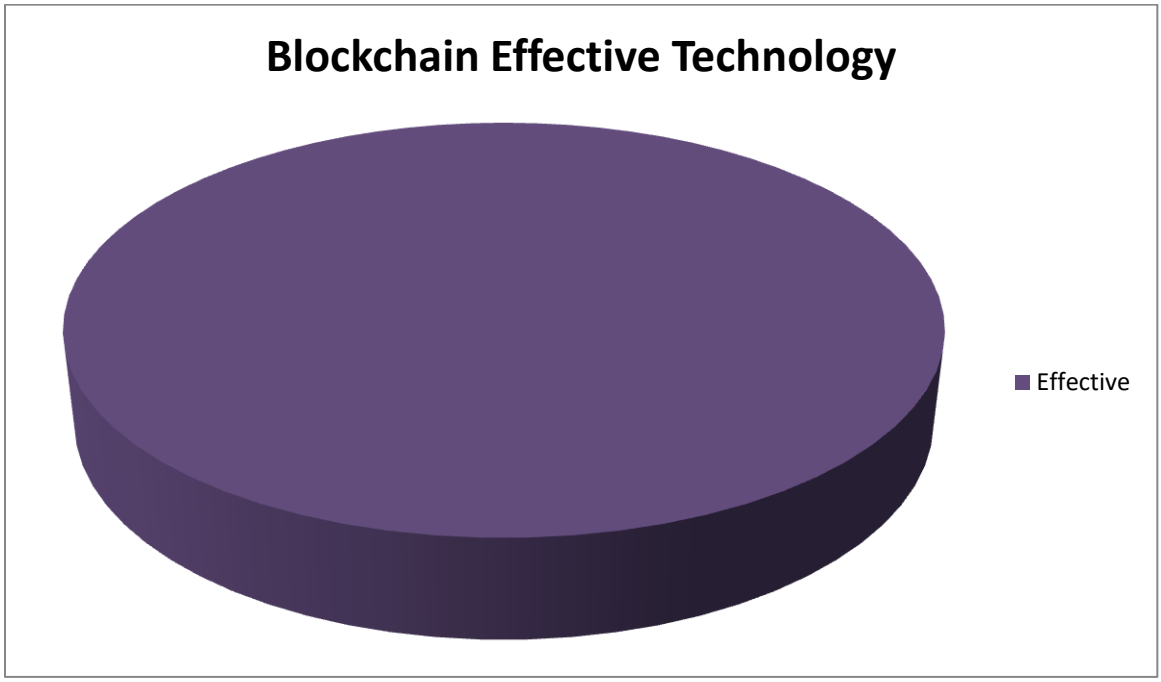

Figure 5. Effectiveness of Blockchain Technology

An interesting question is asked: "What is blockchain good for?", learners mentioned the multifaceted applications and benefits of blockchain technology. They remarkably highlighted blockchain's foundational feature: its decentralized and immutable ledger system. Learners added that blockchain is particularly useful for securely recording and verifying transactions across a distributed network without the need for intermediaries.

All students stated that The characteristic makes blockchain invaluable in industries such as finance, where it facilitates transparent and tamper-proof transactions, reducing the risk of fraud and enhancing trust. Most students emphasized blockchain's potential beyond finance, noting its applicability in various sectors, including e-commerce basically and supply chain management, healthcare, real estate, and voting systems. They might explain how blockchain enables the transparent tracking of goods along the supply chain, ensuring authenticity and reducing counterfeiting and rottenness (fraud). All in all, all students agreed that is effective because of blockchain's decentralized, transparent, and secure nature makes it suitable for a wide range of applications beyond traditional finances, stressing its potential to revolutionize various industries by enhancing transparency, security, and efficiency in transactions and data management.

6. Do you think that blockchain will change the way your company does business in the next three years?

Table 5. Blockchain and E-Commerce

Options	Yes	No
Number	**30**	**00**
Percentage	**100%**	**0%**

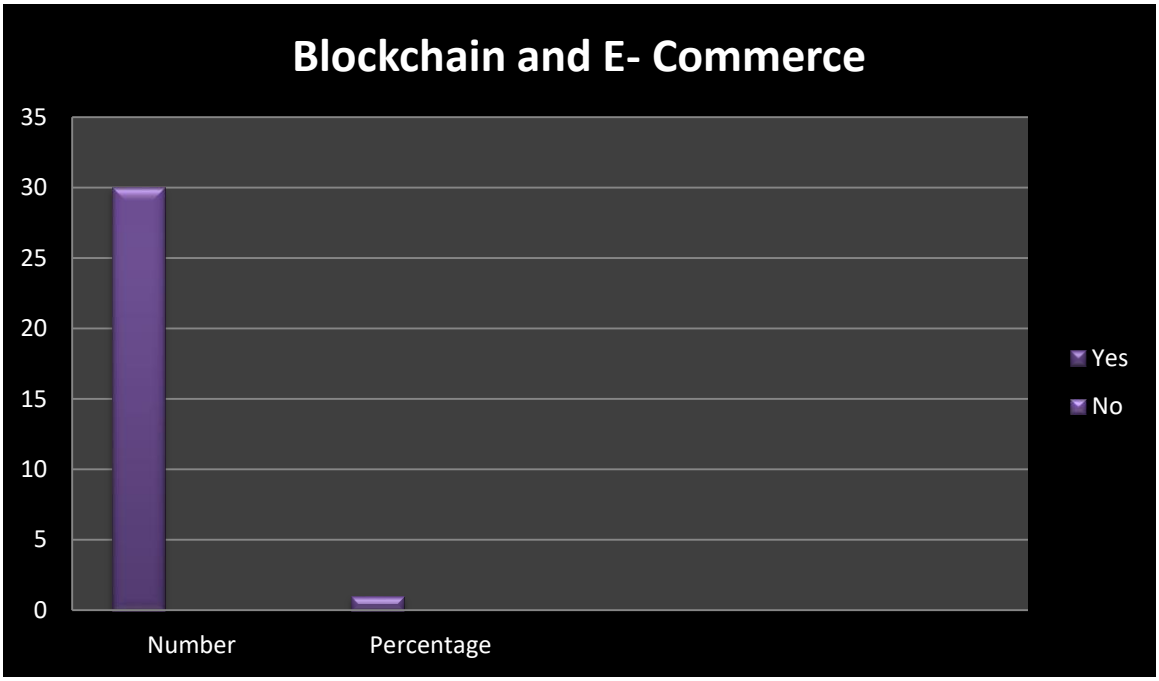

Figure 6. Blockchain and E-Commerce

Noticeably, Table 6 shows that, all respondents (100%) answered "Yes" to the question about blockchain and e-commerce; learners would likely emphasize the significant benefits and potential of integrating blockchain technology into e-commerce platforms. They explained how blockchain can revolutionize various aspects of e-commerce, including transaction security, transparency, and trust. They added that blockchain's decentralized ledger system can eliminate the need for intermediaries in e-commerce transactions, reducing costs and mitigating the risk of fraud. They reflected on how blockchain enables transparent and immutable records of transactions, providing greater accountability and fostering trust between buyers and sellers in online marketplaces and how

blockchain can enable innovative payment solutions, such as cryptocurrency payments, which offer faster and more secure transactions compared to traditional payment methods, We conclude that the integration of blockchain and e-commerce as a transformative and highly beneficial development, with the potential to enhance security, efficiency, and trust in online transactions and commerce.

7. Do you think that blockchain can help improve the future?

Table 6. Improving E-commerce Via Blockchain Technology

Options	Yes	No
Number	**30**	**00**
Percentage	**100%**	**0%**

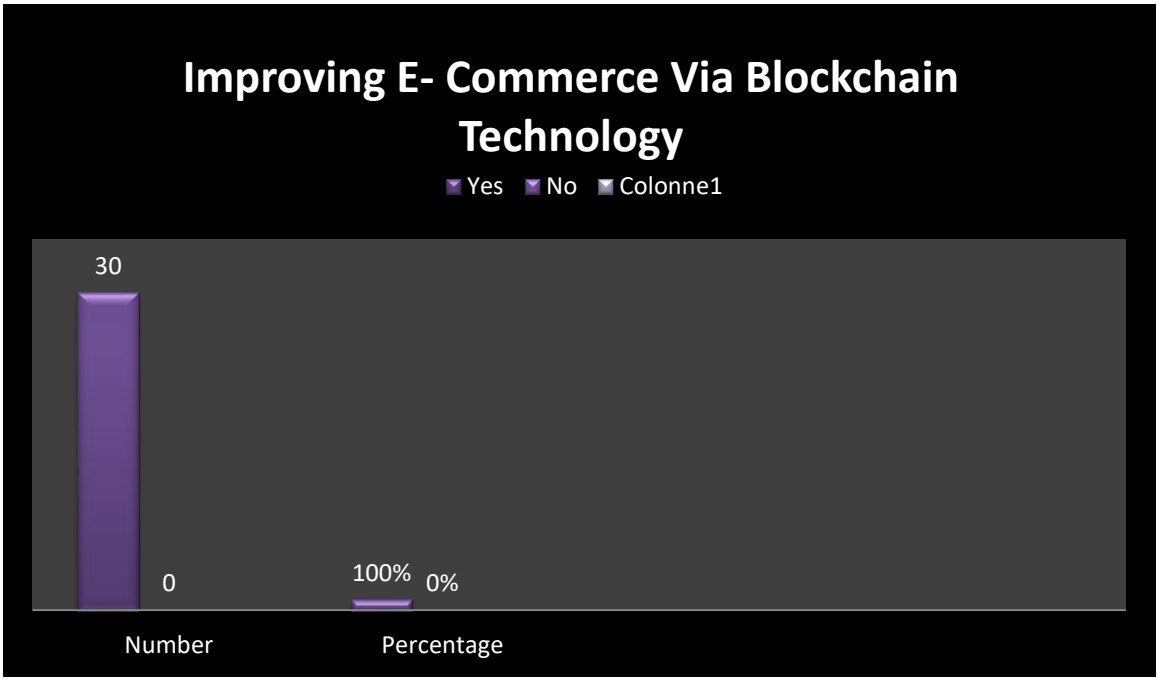

Figure 7. Improving E-commerce Via Blockchain Technology

Remarkably, where all respondents (100%) answered "Yes" to the question about improving e-commerce via blockchain technology, learners agreed on the potential benefits of leveraging blockchain to enhance e-commerce platforms. They strongly emphasized how blockchain technology offers solutions to various challenges faced by e-commerce, such as security, transparency, and efficiency. Most of them highlighted blockchain's decentralized nature, which can eliminate single points of failure and enhance the security of online transactions. They also mentioned enabling real-time tracking of products and ensuring their authenticity. They may also predict mentions of blockchain-based smart contracts, which can automate and enforce the terms of agreements between parties in e-commerce transactions, reducing the need for intermediaries and minimizing disputes. To conclude all students declared that blockchain technology as a powerful tool for improving the security, transparency, and efficiency of e-commerce platforms, ultimately enhancing the overall e-commerce experience for both businesses and consumers.

8. What is KMI?

Actually all students agreed that KMI refers to a comprehensive framework or system designed to securely generate, store, distribute, and

manage cryptographic keys used for encryption, decryption, authentication, and access control in digital environments, they added that KMI ensures the confidentiality, integrity, and availability of cryptographic keys throughout their lifecycle, facilitating secure communication, data protection, and identity management across various applications and systems, most of students stated that by centralizing key management functions and implementing robust security controls, KMI enables organizations to safeguard sensitive information, mitigate security risks, and comply with regulatory requirements related to cryptographic key management.

9. Is KMI good for e-commerce?

Table 7. Effectiveness of Key Management Infrastructure

Options	Yes	No
Number	**30**	**00**
Percentage	**100%**	**0%**

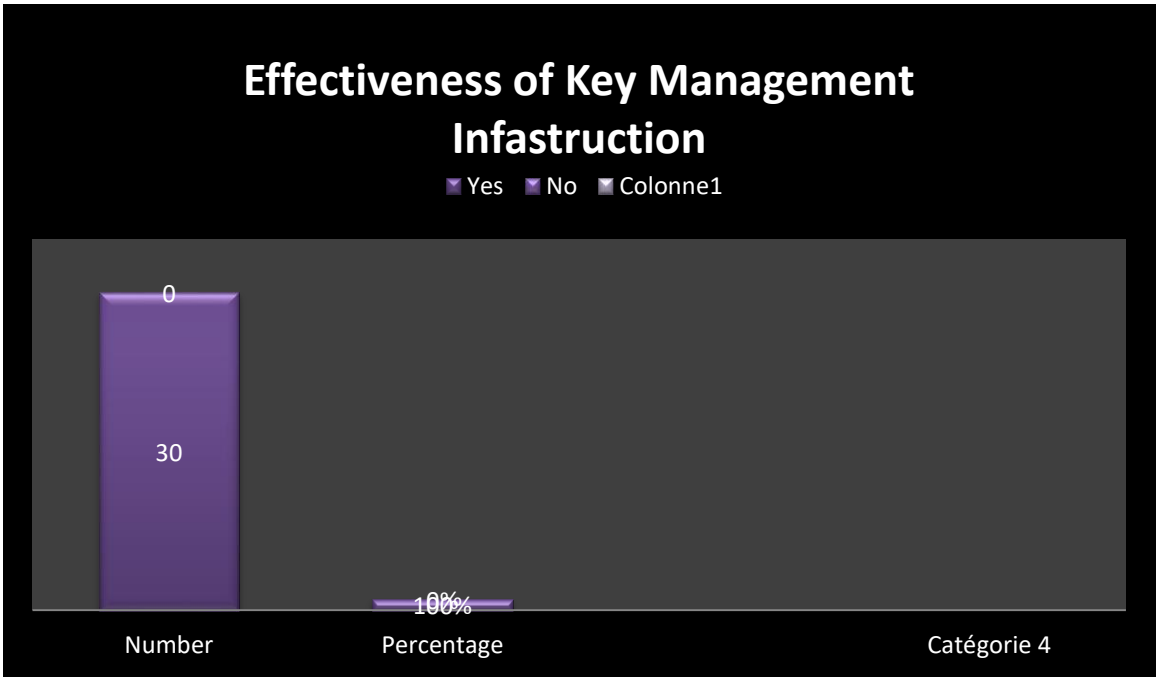

Figure 8. Effectiveness of Key Management Infrastructure

Without doubt, the questionnaire also addressed the effectiveness of Key Management Infrastructure (KMI) for e-commerce, as detailed in Table 9. The options were "Yes" and "No." All 30 respondents, representing 100%, indicated that KMI is good for e-commerce and this reflects students' awareness towards KMI in e-commerce. All the students recognized the importance and effectiveness and benefits of KMI in the context of e-commerce, doubtlessly the absence of any negative responses highlights a strong consensus regarding the positive role of KMI in ensuring secure and efficient management of cryptographic keys, which is crucial for protecting sensitive data and transactions in e-commerce. We deduce easily students' understanding of cybersecurity practices and their recognition of KMI as a

critical component in safeguarding online commercial activities. Interestingly the 100% positive feedback underscores the perceived reliability and necessity of KMI in the e-commerce domain among science computing students.

Section Three: Comparative Study between Blockchain and KMI

10. What are the similarities between Blockchain and KMI?

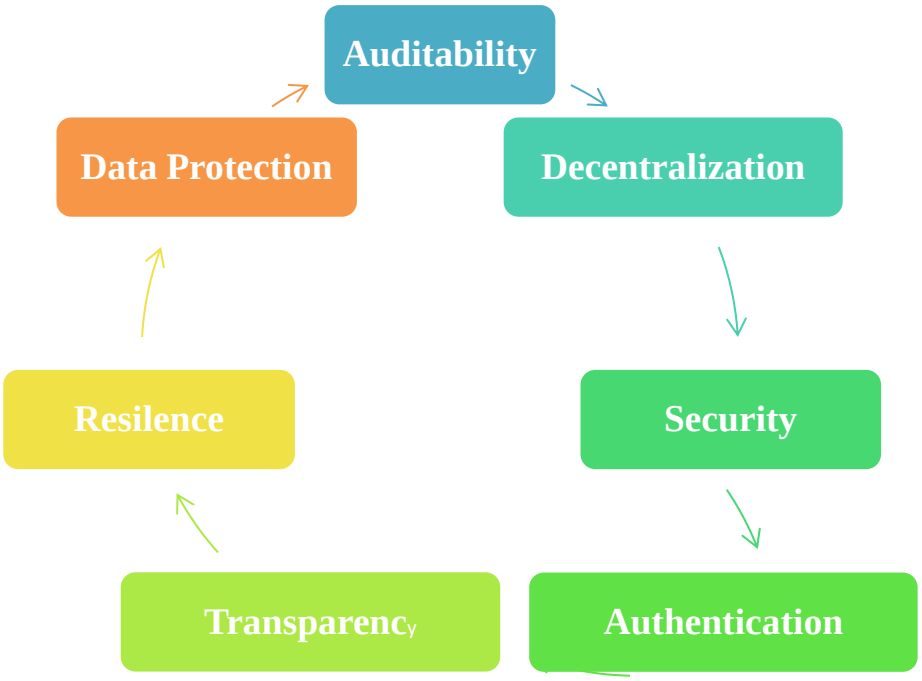

Figure 9. Similarities Betweeb Blockchain and KMI

Notably, most students found it difficult to draw similarities between blockchain technology as well as KMI, though others did. They stated that Blockchain and Knowledge Management Infrastructure (KMI) share several fundamental similarities despite serving different purposes. First students

mentioned that both are structured systems designed to securely store and manage data, in the time Blockchain utilizes a decentralized ledger to record transactions across a network of computers, ensuring transparency and immutability, similarly, KMI facilitates the organization, sharing, and utilization of knowledge within an organization by providing a centralized platform for accessing and managing information. Most students added that both technologies prioritize security, efficiency, and accessibility, aiming to streamline processes and enhance trust in data management.

11. What are the differences between Blockchain and KMI?

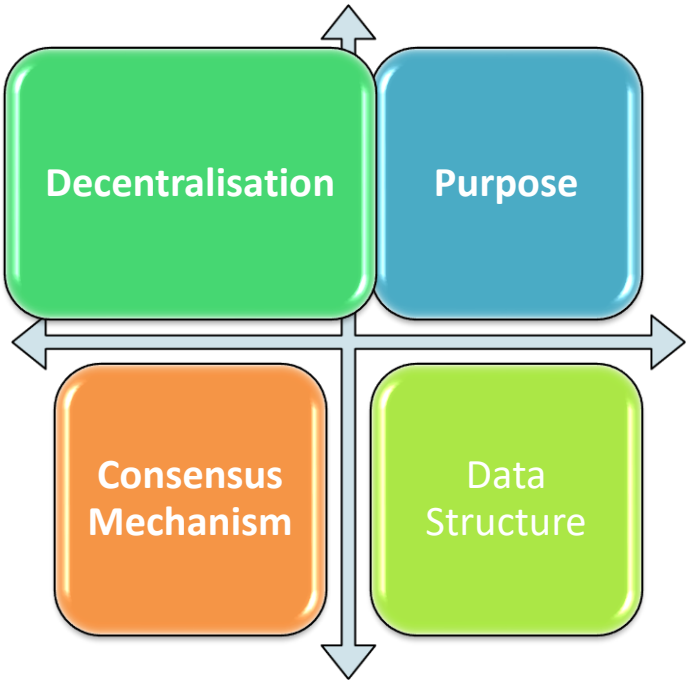

Figure 10. Differences Between Blockchain and KMI

Though learners share awareness towards blockchain technology and KMI in e-commerce for e-authentication, most of them fail to draw

differences between both. And yet, some students stated that Blockchain focuses on decentralized ledger for secure transaction recording, while KMI centralizes knowledge management within organizations to facilitate collaboration and innovation.

12. Do you think the integration between Blockchain and KMI will be effective technology?

Table 8. Integrating Blockchain and KMI

Options	Yes	No
Number	**30**	**00**
Percentage	**100%**	**0%**

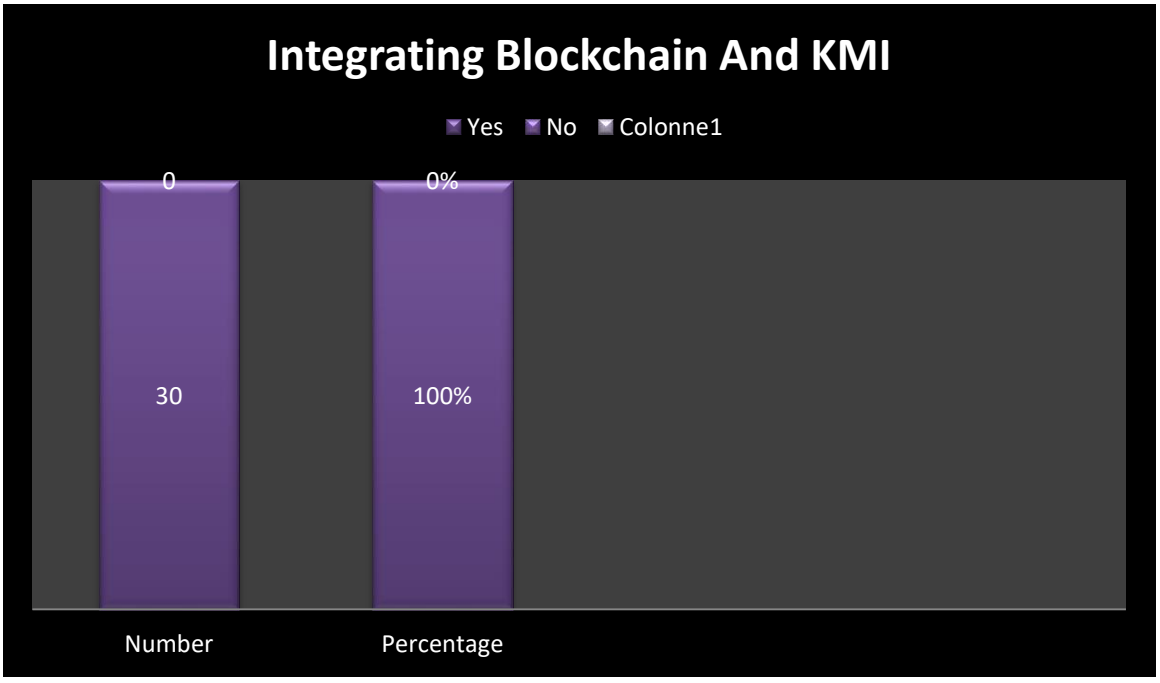

Figure 11. Integrating Blockchain and KMI

Reaching the most important question, it is related to students' perceptions towards the effectiveness of integrating blockchain and Key Management Infrastructure (KMI) technology, as presented in Table 12. the options provided were "Yes" and "No." Remarkably, all 30 respondents, constituting 100% of the sample, expressed a belief in the effectiveness of integrating blockchain and KMI. We deduce a strong consensus among the students regarding the potential benefits of integrating these two technologies. Actually, the absence of any dissenting opinions suggests a widespread understanding and confidence in the synergy between blockchain and KMI. This integration likely holds promise for enhancing security, transparency, and efficiency in various domains, including e-commerce and beyond. The 100% positive response rate indicates a high level of optimism and anticipation among science computing students regarding the transformative capabilities of integrating blockchain and KMI technologies.

13. Does the integration of Blockchain and key management infrastructure enhance the security and privacy of e-commerce transactions and user data?

Table 9. Security Via Blockchain and KMI

Options	Yes	No
Number	**25**	**05**
Percentage	**83.33%**	**16.66%**

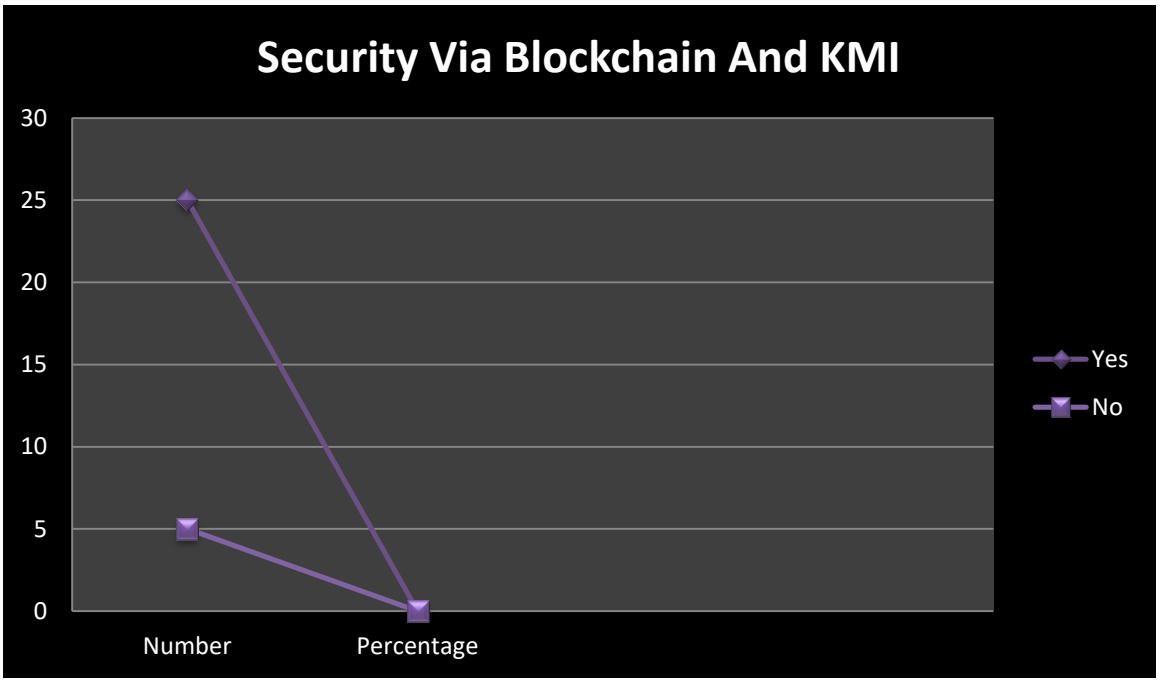

Figure 12. Securing E-authentication Process

14. - What are the key components of this integration, and how do they work together to ensure secure e-authentication processes?

Interestingly, in response to the question regarding the key components of the integration between blockchain and Key Management Infrastructure (KMI) for ensuring secure e-authentication processes, learners found difficulties to

answer. Though 10 students could identified that blockchain as a foundational component, leveraging its decentralized and immutable ledger to securely store cryptographic keys and authentication credentials, they emphasized the role of blockchain in providing a tamper-proof record of identity-related transactions, such as user registrations, logins, and digital signatures. Well, they explained how KMI systems facilitate the generation, storage, distribution, and revocation of cryptographic keys, ensuring their confidentiality, integrity, and availability, stressing the need for robust key management practices to prevent unauthorized access, mitigates security risks, and complies with regulatory requirements. Others added that blockchain-based smart contracts can enforce access control policies and authentication rules, while KMI systems manage the lifecycle of cryptographic keys associated with user identities and permissions.

15. Explain the benefits of the integration between Blockchain and KMI in e- authentication in e-commerce?

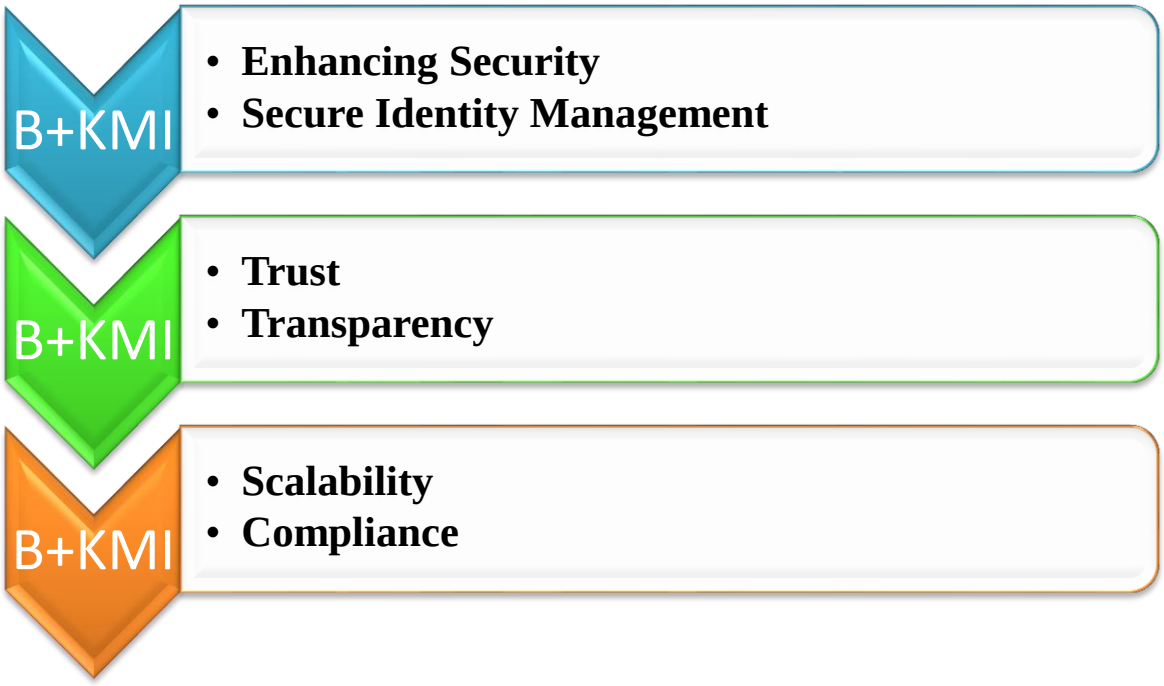

Figure 13. Benefits of Integrating Blockchain and KMI in E-authentication

After asking students about the benefits of integrating blockchain and Key Management Infrastructure (KMI) in e-authentication for e-commerce, learners were highlighting the numerous advantages this integration offers to online businesses and consumers alike. They mentioned that this would enhance security provided by the integration stressing that blockchain's decentralized and immutable ledger system, coupled with robust key management provided by KMI, ensures the secure storage and authentication of user identities and transactions. By leveraging cryptographic techniques and distributed consensus mechanisms, the integration can effectively protect against identity theft, fraud, and unauthorized access to sensitive data, thereby instilling greater trust and confidence in e-commerce platforms.

Additionally students mentioned the efficiency gains resulting from the integration. They explain how blockchain's automation capabilities, such as smart contracts, streamline e-authentication processes by automating identity verification, access control, and authorization workflows. Additionally, KMI's centralized management of cryptographic keys simplifies key lifecycle management, reducing administrative overhead and ensuring the timely revocation and renewal of keys as needed.

16. - What scalability considerations need to be taken into account when implementing Blockchain-based e-authentication with key management infrastructure in large-scale e-commerce platforms?

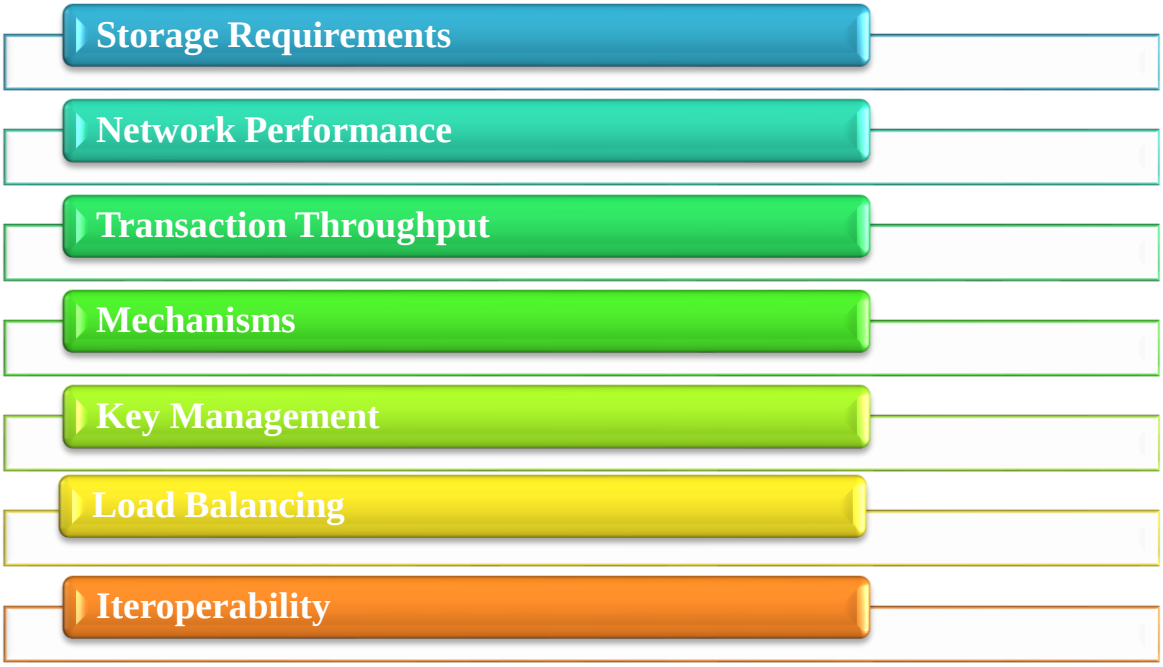

Figure 14. Scalability Considerations While Integrating Blockchain and KMI

Doubtlessly, in responding to the question regarding scalability considerations for implementing Blockchain-based e-authentication with key management infrastructure (KMI) in large-scale e-commerce platforms, learners highlighted the inherent scalability limitations of blockchain technology, particularly in terms of transaction throughput and network performance. They analysed the design of the blockchain consensus mechanism, such as Proof of Work (PoW) or Proof of Stake (PoS), impacts scalability and transaction processing speed, they also mentioned thatblockchain's growing storage requirements and the need for efficient data pruning and optimization techniques to manage increasing volumes of authentication data in large-scale e-commerce

platforms. They also mentioned the scalability challenges associated with KMI systems, particularly in managing cryptographic keys at scale. All of them mentioned the need for standardized protocols and interoperable interfaces to facilitate seamless communication and interoperability between different blockchain networks and KMI systems. All in all students considered factors such as blockchain scalability, KMI performance, and system interoperability, organizations can design scalable and resilient authentication solutions capable of supporting the growing demands of e-commerce platforms while ensuring security, reliability, and performance at scale.

17. Are there any emerging technologies or research areas that could further enhance the security and efficiency of this integration?

Table 10. Emerging Technologies

Options	Yes	No
Number	**25**	**05**
Percentage	**83.33%**	**16.66%**

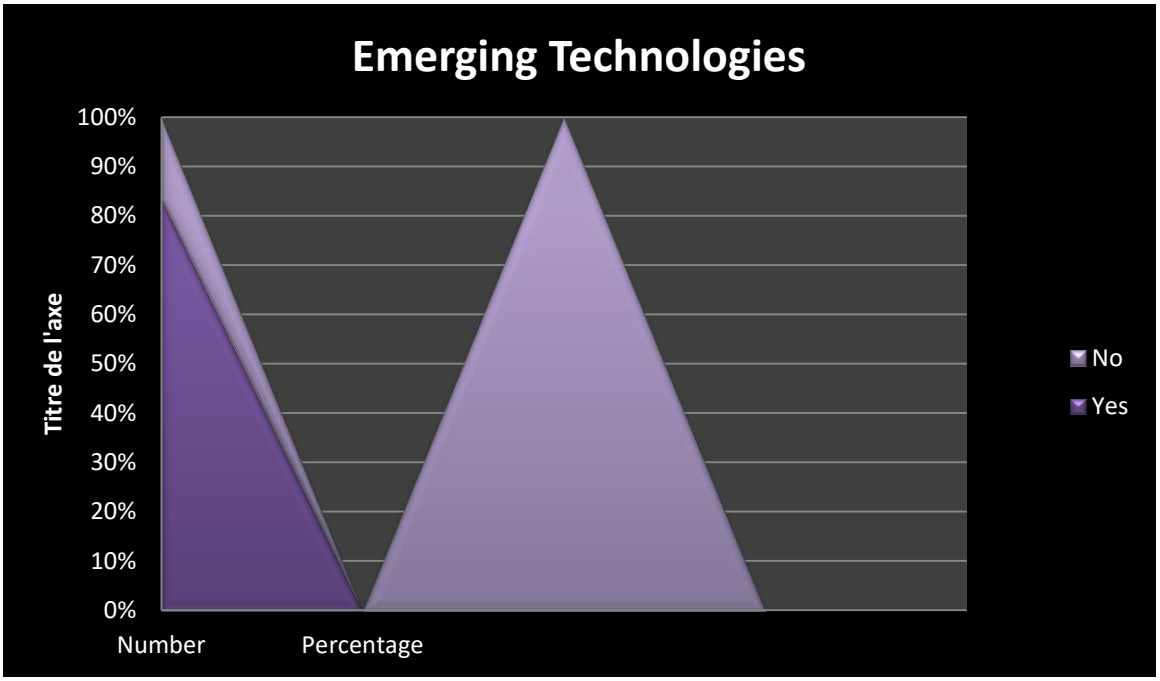

Figure 15. Emerging Technologies

Purposefully, the questionnaire also sought to explore whether there are any emerging technologies or research areas that could potentially enhance the security and efficiency of integrating blockchain and Key Management Infrastructure (KMI) technology, as shown in Table 17. Respondents were given the options "Yes" and "No." well the majority of respondents, 25 out of 30, representing 83.33%, believe that there are indeed emerging technologies or research areas that could further enhance the security and efficiency of this integration.

General Findings

All in all, the students' attitude online questionnaire shows that students are really aware of the importance of both technologies: blockchain as well as KMI in e-authentication in e-commerce. Though they shared similarities and differences it is extremely effective to integrate them for high quality e-authentication in e-commerce.

Additionally, Both blockchain and Knowledge Management Infrastructure serve as structured systems for managing data, albeit with distinct purposes and functionalities. Blockchain is primarily geared towards ensuring secure, transparent, and immutable transaction recording in a decentralized manner, particularly within financial and transactional contexts. It utilizes distributed ledger technology to record transactions across a network of computers, emphasizing security and decentralization as core principles. In contrast, KMI is designed to centralize knowledge management within organizations, providing a centralized platform for organizing, sharing, and accessing knowledge assets. Its focus lies in fostering collaboration, innovation, and the efficient utilization of information among employees. Despite their shared goal of structured data management, blockchain and KMI operate in different domains, with blockchain prioritizing transactional data security and decentralization, while KMI emphasizes knowledge sharing and collaboration within organizational contexts.

2. In-depth Interview with Experts

Purposefully, the rise of e-commerce has brought about significant advancements in digital authentication methods, ensuring secure and trustworthy transactions over the internet. Thus this study aims to conduct a comparative study on two prominent e-authentication technologies: Blockchain and Key Management Infrastructure (KMI). The focus is to understand their effectiveness, reliability, and overall impact on e-commerce security. Through a series of questionnaire as well as interview with professionals in the accounting field, who possess substantial experience in dealing with e-commerce security protocols, this study seeks to gather insights into the practical applications, challenges, and benefits of each authentication method. The findings will contribute to identifying the most efficient and secure authentication technology, providing valuable recommendations for e-commerce businesses aiming to enhance their digital security framework. 3 experts in accounting were asked 11 questions about the topic under investigation.

1. **Blockchain and KMI, According to you how can the two technologies be separated?**

Doubtlessly, the three experts in accounting stated that the two techniques can be separated by indicating differences in the form of points, where emphasis is placed on formal and substantive requirements. Additionally they stated that Blockchain and Key Management Infrastructure are two distinct authentication

technologies in e-commerce, each with unique characteristics in that blockchain operates on a decentralized ledger system, recording transactions across multiple computers to ensure transparency and security In the time it eliminates the need for a central authority, making it resilient against single points of failure. In contrast, KMI uses a centralized approach with a Certificate Authority (CA) that manages digital certificates and keys, creating secure communication channels but introducing potential vulnerabilities from a single point of failure. The three experts added that blockchain offers strong security through cryptographic algorithms and consensus mechanisms, providing a tamper-proof record of transactions. One expert appreciated the question he stated that "Understanding these differences blockchain's decentralization and robustness versus KMI's centralization and ease of integration is crucial for e-commerce businesses in choosing the appropriate technology for their security needs".

2. According to you, what formal Requirements we need?

Well, the three experts in the field of accounting stated that, the formal requirements may be:

-Electronic certifications.

-The authorities are the performer's role.

-Conditions to be met in electronic certifications.

-And these electronic certification certificates for key management infrastructure.

- Authorities and electronic certifications PKI.

-You need reliable electronic certification authorities.

We deduce clearly that according to experts in the field of accounting, the formal requirements for effective e-authentication in e-commerce include electronic certifications, the establishment of authoritative roles, specific conditions that electronic certifications must meet, and the issuance of electronic certification certificates for Key Management Infrastructure. Electronic certifications are essential for verifying identities and ensuring secure transactions. The authorities, such as Certificate Authorities (CAs) in KMI, play a crucial role in managing and validating these certifications. Additionally, the conditions that electronic certifications must meet involve strict adherence to security protocols and standards to maintain trust and integrity in digital transactions. These formal requirements are fundamental in creating a reliable and secure authentication framework for e-commerce.

3. What are the needed conditions?

Conditions to be met at the electronic certification service:

-The electronic certification authority must be accredited and meet specific criteria.

-Mechanisms must be in place to confirm users ' identity.

-Articles 7 and 15 of Law 15-04

Unquestionably, the above mentioned conditions by the three experts are required for an electronic certification service to be effective include several key elements. Firstly, the electronic certification authority must be accredited and meet specific criteria, ensuring it operates under recognized standards and regulations. Secondly, robust mechanisms must be in place to verify and confirm users' identities accurately, which is crucial for maintaining trust and security in digital transactions. Additionally, the service must comply with Articles 7 and 15 of Law 15-04, which likely outline further legal and operational requirements for electronic certifications. Well these conditions ensure that the certification process is reliable, secure, and legally compliant, thereby supporting the integrity of e-commerce activities.

4. **What are e-certificates?**

Electronic certification certificates:

-Adopt electronic certifications to confirm user identity and data integrity.

-It's provided by accredited electronic certifications.

Well, according to the three experts in accounting Electronic certification certificates, or e-certificates, are digital documents used to confirm user identity and ensure data integrity in electronic transactions. In the same regard, these certificates are issued by accredited electronic certification authorities, which adhere to specific standards and regulations to maintain security and trust. They added that by adopting e-certificates, businesses and users can securely

authenticate identities and verify the integrity of exchanged data, thereby enhancing the overall security of e-commerce operations.

5. **Does the role of an electronic certification service performer is a formal requirement?**

Yeah. It's to confirm the identity of the ends and the validity of the data.

All the experts in accounting agreed on the statement. They added Indeed, there is a formal necessity for the position of electronic certification service performance. This performer is in charge of issuing and overseeing electronic certification certificates; they are also commonly referred to as Certificate Authorities (CAs). Well, their responsibilities including validating user identities, guaranteeing certificate integrity, and upholding a reliable structure for electronic transactions. For the electronic certification process to be secure, dependable, and compliant with the law, the certification service provider needs to fulfill formal accreditation requirements. This guarantees that the integrity and validity of the electronic certificates may be trusted by all parties participating in e-commerce transactions.

6. What are the legal requirements for each technology?

-Key management infrastructure:

The legal requirements for key management infrastructure vary depending on the country or region.

-BLOCKCHAIN TECHNOLOGY:

There are currently no specific laws regulating the use of block chin for electronic certification. However, there are a number of

-Legal issues to be taken into account:

-Electronic certificates: PKI

-Smart contracts: BC

-The National Framework for Blockchain Technology, April 2022, was drafted in cooperation with the Liaison Regulatory Authority, the University of Hamad bin Khalifa and the University of Qatar.

-The role of an electronic certification service performer is a formal

Legal requirements for KMI are region-specific and focus on CA accreditation and secure key management. Blockchain lacks specific regulations but must consider legal issues related to electronic certificates (PKI) and smart contracts.

7. Explain it more.

Interestingly, experts mentioned that Legal requirements for digital certificates and electronic certification service providers encompass several crucial aspects. Firstly, digital certificates must adhere to specific standards such as X.509 or PKIX. Secondly, electronic certification service providers must obtain licensing from a competent government authority, as mandated by

Articles 7 and 15 of Law 15-04. Moreover, these providers are obligated to stay current with data protection laws, such as the General Data Protection Regulation (GDPR) in the European Union. Additionally, compliance with anti-money laundering and anti-terrorist financing laws is imperative, with particular emphasis on providers utilizing blockchain technology. Furthermore, for those employing blockchain, adherence to data protection regulations is essential. Finally, there must be legal clarity regarding the enforceability of smart contracts executed on the blockchain network.

8. **What is the difference between certificates and smart contracts?**

-It is led by reliable sources such as CA certification centers.

-Contains user identification information and public key.

-Used to verify user identity and signature of electronic transactions.

-They are subject to strict standards and safety standards.

-Implemented on the Block Chin network.

-They are self-executing codes that define the terms of agreement between two or more parties.

-It can be more efficient and transparent than traditional contracts.

In deed the three experts in accounting stated that Certificates and smart contracts serve distinct purposes in the realm of digital transactions, each leveraging different technologies and functionalities. Thus certificates, typically issued by Certificate Authorities (CAs), are authoritative digital documents that

contain user identification information and public keys. It is important to mention that these certificates are employed to verify the identity of users and validate electronic signatures in transactions. On the other hand, smart contracts are self-executing code stored on a blockchain network, designed to automatically execute and enforce predefined terms of agreement between parties when specific conditions are met. Unlike traditional contracts, which rely on intermediaries to enforce terms, smart contracts operate autonomously, eliminating the need for intermediaries and increasing efficiency and transparency in transactions. Smart contracts can facilitate a wide range of transactions, including financial transfers, asset exchanges, and automated processes, by executing predefined instructions encoded within the contract. certificates primarily serve the purpose of verifying user identity and signatures in electronic transactions, while smart contracts define and enforce terms of agreements in a transparent and automated manner. While certificates ensure the security and integrity of transactions, smart contracts enhance efficiency and transparency by automating contract execution on blockchain networks.

9. **What's stuck between technology and organizational metaphor?**

   -The organizational setup is directly related to technology, but is related to the actions taken by the parties involved in

   -Provision or use of technological services

Notably, The concept stuck between technology and organizational metaphor refers to the interplay between the organizational structure and the technology employed within an organization. While the organizational setup directly influences the adoption and utilization of technology, it also encompasses the actions and behaviors of the parties involved in providing or using technological services. Essentially, this metaphor encapsulates how the organizational framework shapes and interacts with technological systems and processes, emphasizing the intricate relationship between organizational dynamics and technological implementation.

10. **What are some of the common aspects to be addressed in the BLOCKING TECHNOLOGY REGULATIONS?**

-Some common aspects mentioned by experts include:

-The ability to remove data is based on the request of the authorities/legislations.

-Identification of individual responsibility for operations and restriction by the advantage of anonymity.

Well, in blockchain technology regulations, experts commonly address several aspects. These include the requirement to remove data based on authorities' or legislations' requests, ensuring compliance with legal obligations. Another aspect involves identifying individual responsibility for operations and limiting the advantages of anonymity, aiming to enhance accountability within blockchain networks.

11. **What are the regulations on the scope of the PLOCKING TECHNOLOGY SERVICES?**

-There are regulations on the scope of the service, how to use it, that are handled by the regulator of this domain.

Use.

- Each case requires the use of a different approach, which may include policy development, guidelines, or Machines, or regulatory frameworks.

-The Communications Regulatory Authority can support the issuance of regulatory tools that are required to facilitate

-Building Plocking Technology

Regulations regarding the scope of blockchain technology services are typically overseen by the relevant regulatory authority in the domain. These regulations govern how blockchain technology is utilized and implemented. Each case may necessitate a unique approach, which could involve the development of policies, guidelines, or regulatory frameworks tailored to specific contexts. Regulatory bodies, such as the Communications Regulatory Authority, can provide support by issuing the necessary regulatory tools to facilitate the development and implementation of blockchain technology solutions.

General Findings

All in all, Experts in the industry have emphasized a number of important factors about blockchain technology legislation and concerns based on the information provided:

First of all the importance of the Regulatory control, experts stated that the implementation and application of blockchain technology are acknowledged to require regulatory control consequently regulatory bodies are essential in creating rules, regulations, and structures that control its use and extent. Also the data management, why? because issues with data management in blockchain systems are frequently covered by regulations such as guaranteeing adherence to data protection laws and removing data upon court orders. What is more is that individual accountability as well as anonymity, experts stressed stressed the significance of recognizing personal accountability for blockchain network operations and limiting anonymity's benefits in order to improve accountability and adaptability as well. Additionally they insisted on support from regulatory authorities, all in all In order to install and use blockchain technology effectively, professionals understand how crucial regulatory supervision, data management, accountability, flexibility, and assistance from regulatory agencies are. For blockchain technologies to be successfully implemented across a range

of sectors and applications, compliance, accountability, and other factors must be taken into account.

Conclusion

In conclusion, the comparative study of e-authentication in e-commerce between blockchain and key management infrastructure underscores the multifaceted nature of security and efficiency considerations in online transactions. While blockchain offers inherent decentralization, immutability, and transparency, it also introduces complexities such as scalability challenges and regulatory compliance issues. On the other hand, traditional key management infrastructure provides a centralized approach to authentication but may lack the tamper-resistant properties and transparency of blockchain. Additionally, the trajectory of e-authentication in e-commerce is intricately intertwined with the dynamic interplay of technological advancements, regulatory mandates, and evolving industry norms. The field's progression hinges upon a comprehensive understanding of emerging trends, coupled with methodical comparative analyses. Without doubt through maintaining scholarly vigilance and conducting rigorous research inquiries, scholars and practitioners can drive forward the development of high quality authentication protocols that not only prioritize security and efficiency but also cultivate user trust and confidence in the digital marketplace to the maximum. This scholarly pursuit

stands as a pivotal endeavor in ensuring the continued integrity and resilience of online transactions in e-commerce.

List of References

1. Basu, A. and Muylle, S. Online support for commerce processes by Web retailers. *Decision*
2. Battah, Y. Iraqi, and E. Damiani, ‘‘Blockchain-based reputation systems: Implementation challenges and mitigation,’’ Electronics, vol. 10, no. 3, p. 289, Jan. 2021.
3. Bellini, Y. Iraqi, and E. Damiani, ‘‘Blockchain-based distributed trust and reputation management systems: A survey,’’ IEEE Access, vol. 8, pp. 21127–21151, 2020.
4. Bhatti, A.; Akram, H.; Basit, H.M.; Khan, A.U.; Raza, S.M.; Naqvi, M.B. E-commerce trends during COVID-19 Pandemic. Int. J. Future Gener. Commun. Netw. 2020, 13, 1449–1452.
5. Brunner, C., Knirsch, F., and Engel, D. (2019). SPROOF: A platform for issuing and verifying documents in a public blockchain. In *Proceedings of the 5th International Conference on Information Systems Security and Privacy*, pages 15–25, Prague, Czech Republic. SciTePress.
6. Casino, F. T. K. Dasaklis, and C. Patsakis, ‘‘A systematic literature review of blockchain-based applications: Current status, classification and open issues,’’ Telematics Informat., vol. 36, pp. 55–81, Mar. 2019, doi: 10.1016/j.tele.2023.11.006.

7. Dahal, S.B. Enhancing E-commerce Security: The Effectiveness of Blockchain Technology in Protecting Against Fraudulent Transactions. Int. J. Inf. Cybersecur. 2023, 7, 1–12.
8. Friedman, B., Kahn, P., and Howe, D. Trust online. *Commun. ACM 43*, 12 (December 2000), 34–40.*Support Systems 34*, 4 (Mar. 2003), 379–395
9. Jiang, J.; Chen, J. Framework of blockchain-supported e-commerce platform for small and medium enterprises. Sustainability 2021, 13, 8158.
10. Knirsch, F., Unterweger, A., and Engel, D. (2019). Implementing a Blockchain from Scratch: Why, How, and What We Learned. *EURASIP Journal on Information Security*, 2019(2):1–14.
11. Norberg, ‘‘Unblocking the bottlenecks and making the global supply chain transparent: How blockchain technology can update global trade,’’ School Public Policy Publications, vol. 12, no. 9, pp. 1–24, Mar. 2019.
12. Resnick and R. Zeckhauser, ‘‘Trust among strangers in internet transactions: Empirical analysis of eBay’s reputation system,’’ in The Economics of the Internet and E-Commerce (Advances in Applied Microeconomics). Bingley, U.K.: Emerald (MCB UP), vol. 11. Oct. 2002.
13. Sarda, S.; Sharma, S.; Pal, R. Consumer Protection Regulation in Light of E-Commerce and Product Liability. Issue 2 Indian JL Leg. Rsch. 2022, 4, 1.

14. Tschorsch, F. and Scheuermann, B. (2016). Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies. *IEEE Communications Surveys n& Tutorials*, 18(3):2084–2123.

15. Viriyasitavat, W., Xu, L. D., Bi, Z., and Sapsomboon, A. (2019). New Blockchain-Based Architecture for Service Interoperations in Internet of Things. In *IEEE Transactions on Computational Social Systems*, volume 6, pages 1–10. IEEE.

16. Wang, C., Yanli, F., ―Model Based Security Policy Assessment for E-Business Environment‖, Proceedings of the Second Symposium International Computer Science and Computational Technology(ISCSCT ’09) Huangshan, P. R. China, 26-28, Dec. 2009, pp. 088-*093.*

17. Whitten, A., and Tygar, J.D. Why Johnny can’t encrypt: A usability evaluation of PGP 5.0. Working paper, School of Computer Science, CMU (2002).

18. Yakubov, A., Shbair, W. M., Wallbom, A., Sanda, D., and State, R. (2018b). A Blockchain-Based PKI Management Framework. In *The First IEEE/IFIP International Workshop on Managing and Managed by Blockchain (Man2Block) colocated with IEEE/IFIP NOMS*, pages 1–6, Tapei, Tawain. IEEE.

19. Yu, J. and Ryan, M. (2017). Evaluating web PKIs. In *Software Architecture for Big Data and the Cloud*, chapter 7, pages 105–126. Elsevier.

Résumé

Dans le domaine du commerce électronique, la technologie joue un rôle important. Ainsi, la croissance rapide du commerce électronique actuel a nécessité le développement de robustes mécanismes d'authentification électronique (EA) pour assurer des transactions sécurisées, valables et fiables. Par conséquent, la recherche actuelle vise à examiner attentivement l'intégration de la technologie blockchain et de l'infrastructure de gestion clé (IGC) en tant que solutions pivotales exceptionnelles pour améliorer l'authentification électronique dans le e-commerce, dans une étude comparative. Worthy a noté que Blockchain, avec son registre décentralisé, offre une sécurité, la transparence et la traçabilité inégalées, ce qui en fait un moyen idéal pour sécuriser les transactions de commerce électronique. Par rapport à IGC, ce dernier fournit des services essentiels pour la génération, le stockage, la distribution, ainsi que la gestion des clés cryptographiques, qui sont extrêmement essentielles pour sécuriser la communication et la protection des données. Par conséquent, ce travail modeste souligne attentivement la synergie entre la blockchain et IGC, démontrant comment leur utilisation copieuse peut renforcer les processus d'authentification électronique. La méthode de recherche adoptée par le chercheur est une analyse complète de ces technologies; cette recherche vise à présenter un cadre de haute qualité qui aborde les défis actuels de la sécurité du commerce électronique, contribuant finalement au

développement de plates-formes commerciales en ligne plus résilientes et fiables.

Mots clés: Blockchain, IGC, E-Commerce, Recherche comparative.