



Leveraging Blockchain Technology in Trade, Transaction fraud and Privacy: A study of Banking Sector in Pakistan by using Tree analysis

Sarfraz Ali Malak (Corresponding Author)

Assistant Professor, Department of Business Administration, University of Sindh (Campus Dadu).

Email: malak.sarfraz@usindh.edu.pk

Abdul Wajid

Faculty of Business and Economics, Department of Economics, Eastern Mediterranean University (EMU), North Cyprus, Mersin 10, Turkey. Email: abdulwajidmoroojo@gmail.com

Amir Ali

Department of Business Administration, Istanbul Arel University, Istanbul Turkey.

Email: aamirpanhwar31@gmail.com

Fayyaz Ahmed

BBA, Department of Business Administration, University of Sindh (KBSAS Campus).

Email: fayyazahmed12@gmail.com

Abstract

This paper discusses blockchain in categories including trade, transaction fraud, and privacy, using statistical models and decision tree analysis. The trade category is quite large, with Nodeo which incorporates the whole set and yielded Meg clearance length mean of 3.836 with a relatively large $F = 245.8$, $p = 0.000$. Mean values for Subgroups Node1, Node2, and Node3 are different, equal to 2.990, 4.281, and 4.155, respectively, also showing different impact at the blockchain set. As it concerns the main group of transaction frauds, Nodeo has a mean of 3.941 for the dataset while subgroups Node1 to Node 4 show different patterns which proves the developers' statements concerning relatively high fraud scores ($F = 232.061$, $p = 0.000$). The results in the privacy overall classification mean for the participant's datasets show much variation ($F = 37.270$, $p = 0.000$), where Node o contains the study and the other nodes, Node 1 and Node 2, compares the privacies of the participant's data sets. Analysis with regression models also confirms blockchain's impact based on high R^2 coefficients equal to 0.568 for trade and 0.707 for transaction fraud and positive coefficients at $p = 0.000$. Altogether, the established results further support that blockchain has an enormous potential in the mentioned and other fields, as well as reveal the methods of improving trade, avoiding fraud, and the significance of privacy.

Keywords: Block Chain, Banking Industry, Trade, Transaction, Privacy, Fraud

Introduction



Vol. 3 No. 1 (January) (2025)

Blockchain technology has been rapidly adopted to facilitate the financial services by guaranteeing transparent, secure and speed transactions. Such benefits of blockchain has been witnessed in study by Li et al. (2023) which explored that the role of blockchain is great, it reduces costs for operations and transactions and supports international payments with more speed, accuracy and risk free. Although Stuart Haber and Wakefield Scott Stornetta first proposed the blockchain in 1991, it wasn't until 2008 when Nakamoto suggested using the network to construct Bitcoin that the idea gained widespread acceptance. Blockchain refers to a chain of blocks. On this platform, the data is saved in each block when user to place it there. If one block is fully saved then data transform to another block, this procedure happens sequentially, each and every block interconnected with each other, this is said to be blockchain (Fulmer, 2019). A block contains information in the form of a prior hash and current hash also first block related to it via its own hash and hash interconnects. Blocks begin at the Genesis block, which is the initial block. When this block is entirely saved, after that second block will be formed this process happens continuously (Yaga & Etal, 2019; Raza & Tursoy, 2025). Blockchain, the metaverse, the Internet of Things, and artificial intelligence are just a few of the well-known terms in the rapidly growing field of technology. Unlike 19th-century methods the blockchain enables frictionless user-to-user transmission of digital data without interference from outside parties. This platform also offers a secure transaction system for maintaining records and storing data. Blockchain has ability to transfer data and information without the aid of a third party, ensures that no one can simply hack or steal their data using this platform (Raza et al., 2023; Tyagi & Etal, 2020). The ability to perform trade transactions instantly and quickly by using this platform has become possible. As a result, those who purchase or sell assets don not have to wait a lengthy time for the transaction to be formally confirmed and finished. This speed not only saves a great deal of time but also lowers the expenses associated with the conventional procedure of concluding deals, which sometimes necessitates the participation of several middlemen (Catalini & Gans, 2020). The blockchain's ledger, which operates as a shared public document, allows for the free recording of all transactions. Anyone may review the specifics of any transaction whenever they want and everything being available, this transparency is advantageous since it boosts traders' and investors' trust in its system (Raza et al., 2024; Mougayar, 2016). Blockchain technology makes it easier to turn priceless assets like real estate and artwork into digital tokens. More individuals can invest in these assets since the ownership-representing tokens may be split into smaller pieces. It used to be hard to purchase or sell little amounts of these costly commodities, but with help of blockchain, it's now possible. It is like dividing them into smaller, more reasonable shares that everyone can exchange (Omarova, 2019). Blockchain technology improves market efficiency by providing immediate access to real-time trade data. Anyone participating in the trade may now see what is happening live, which improves their ability to make judgments. Blockchain also shortens the time it takes to settle deals and a trade's completion used to take some time now it happens much more quickly. Traders and investors profit from this general increase in efficiency since it makes the market more responsive and dependable (Tripoli & Schmidhuber, 2018).

Consider a blockchain to be a very safe vault once a transaction is recorded within it then it cannot be modified or deleted. It is nearly hard for fraudsters to manipulate transaction



Vol. 3 No. 1 (January) (2025)

records because to this robust security (Ehsan & Etal, 2022). Examine blockchain as a group of systems, each of which is keeping an eye on everything. It's quite difficult for someone to do fraud or tricks on the network because there isn't a powerful person in control. It acts as a very attentive protector over your transactions (Al Barghuthi & Etal, 2018). Acknowledge blockchain transactions as messages posted on a big public bulletin board. These messages are visible to anybody with access to the board. Its openness serves as a vigilant eye, ensuring that everyone utilizing the board will immediately notice and take action if something odd or suspicious emerges on it. There are several individuals watching out for anything unexpected to ensure that everything is honest and fair (Al Barghuthi & Etal, 2018). Blockchain is comparable to a very secure ID card. It ensures that you are, in fact, who you claim you are. Because of this, it is nearly hard for scammers to use your name to make purchases online or do other identity theft. To keep ID forgers out, it's like having a digital bouncer verify IDs (Gundur & Etal, 2021). Blockchain functions makes simple for inspectors and law enforcers to keep an eye on transactions and ensure that everyone is abiding by the law. It's similar to having a transparent window into financial activity, which makes it much tougher for devious things to happen without being seen (Kaplan, 2021).

Many banking business sectors might operate more efficiently because of blockchain technology. The capital markets, trade banking, cross-border payments, financial reporting, and compliance might all be improved and transformed by it. It also simplifies the process of getting to know your customers. Therefore, it is anticipated that the use of blockchain technology could change the banking and financial sector by enabling several innovations such as protected ledgers, faster trade execution, and new payment methods (Khadka, 2020). Banking has seen a significant transformation over time due to technological innovation. Digital innovation in banking started with the introduction of money to replace barter systems, and subsequently, digital signatures eventually replaced wax seals. Blockchain technology is one such disruptive invention that is revolutionizing the global banking sector. In order to facilitate different financial operations, the Indian banking industry has also begun implementing blockchain technology (Jena, 2022).

By employing secret encryption and dispersing that data over several computers, blockchain keeps data extremely safe. Only authorized individuals are able to view or modify the data by using this platforms algorithm. Additionally, it's very difficult for someone to tamper with the data since its spread among so many machines. Data that has been entered into the blockchain is likened to being locked within a very secure box that is impossible to access. It would also be extremely difficult to open the box, making it nearly impossible for criminals to alter the data. Therefore, blockchain functions as a very safe vault for digital data (Mougayar, 2016). When it comes to privacy, the openness built into blockchain technology offers a difficult conundrum. While the open, irrevocable ledger of transactions is its core strength, it may also provide difficulties. Everything that occurs on a blockchain is recorded digitally for all to see, including money transactions and data changes (Ammous, 2016). This encourages confidence and responsibility inside the network on the one hand, but it also raises the possibility of privacy issues. Individuals and organizations must carefully assess what information they release while working on a blockchain. Sensitive information was once hidden in traditional systems now is exposed



Vol. 3 No. 1 (January) (2025)

(Tapscott & Tapscott, 2016). To solve privacy issues with public blockchains, privacy-focused crypto currencies like Monero and Zcash have been created. These crypto currencies utilize sophisticated cryptography algorithms to vastly improve user privacy and transaction secrecy. For instance, Monero conceals the sender, recipient, and transaction amounts by using methods like ring signatures and secret transactions. This offers a high level of anonymity by making it very difficult to detect and correlate transactions to specific users. The zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge) technique is used by Zcash in contrast. Zcash enables private transactions via zk-SNARKs, guaranteeing total privacy by hiding the sender, recipient, and transaction amount. A rising understanding of the value of privacy in blockchain transactions may be seen in the rise of privacy-focused crypto currencies. In situations when people and companies want increased privacy and secrecy, these crypto currencies give consumers the ability to conduct secret and confidential transactions (Bernabe & etal, 2019).

Though the rapid growth and use of digital technology has greatly influenced the banking sector globally, yet this has also increased the risks of transaction fraud and issues of data privacy. In the case of Pakistan, where banking system contributes effectively in the economic growth, it becomes more crucial to protect transactions from fraud and also secure data privacy of clients. However, such challenges can be fixed with the use of blockchain technology, which has features of safeguarded ledger mode, decentralization and transparency. This research examines the implementation of blockchain technology in the banking industry of Pakistan and assessing its prospective benefits in reducing transaction fraud and strengthening privacy. By leveraging the potential abilities of blockchain technology, the banks in Pakistan can foster trust and more efficient operations, nurture resilient and safe financial environment. Thus, the purpose of this study is to understand how blockchain makes trade better in banking sectors of Pakistan and figure out how blockchain technology improves trade reliability, speed, and cost. It also aims to identify potential benefits of blockchain technology in preventing theft, fraudulent transactions, and fake products in trade in banking sector of Pakistan. Furthermore, the objectives also include to identify effects of blockchain use on the privacy of individuals and banking sectors of Pakistan who engage in trade, and, to explore whether blockchain technology can defend trade data against hackers in banking sector of Pakistan.

Problem statement

Blockchain technology is transforming how to trade, combat fraud, and manages privacy in banking sector. We need to understand how this technology impacts on banking sector in the digital age in order to make better decisions. Although we are aware of the blockchain but we do not yet understand how it effect on trade, transaction fraud, and privacy, particularly in Pakistan. Hence, we need to understand how we can trade, secure, store, prevent fraud and save personnel information by using this platform. Because so many conventional businesses in Pakistan are not utilizing this platform, they are always dealing with challenges related to client trust and transaction fraud. For conventional enterprises, this analysis might be useful additionally; many Pakistani consumers have lack of knowledge about how to utilize the blockchain for commerce, security, and fraud prevention. By providing a thorough analysis of the effects of blockchain on trade,



Vol. 3 No. 1 (January) (2025)

transaction fraud prevention, and data privacy management across Pakistan's banking sector, this research aims to fill these knowledge gaps. It aspires to develop a blockchain which has a strong grasp of technology and safe digital environment in Pakistan, offering beneficial insights and advice for companies and consumers alike.

Research gap

Literature review shows that less empirical evidence exist in context of Pakistan pertinent to the use of blockchain technology in banking sector of Pakistan. Investigation by Ali et al. (2021) assessed the possible use of the blockchain in the banks of Pakistan; however it's, main focus was on technical and infrastructure issues. This provides opportunity for research to explore as limited literature exists on impact of blockchain's application to facilitate trade in banking sector of Pakistan. The banks in Pakistan face the risks of transaction fraud and are unable to detect and prevent it with traditional approach and methods. Research study explored the practical application of blockchain in detecting the frauds and concludes the non-availability of studies on practical use of such technology (Khan & Rahman, 2022). Whereas the researches in international context such as by Chen et al. (2019) focused on the application and success of blockchain in preventing transaction related fraud. The digital transformation of banks has also increased privacy concerns pertinent to customers' data. In order to build customers trust on digital financial transactions, there is a need for exploring the blockchain's anti-fraud mechanisms in the banking sector of Pakistan. Blockchain offers the solution with its decentralized method and encrypted features. However, researches like Jameel et al. (2020) indicated that Pakistani banks are reluctant in using blockchain due to regulatory hurdles and concerns of data security. Contrary, international studies have revealed the blockchain's potential use in augmenting privacy (Liu et al., 2018). This provides the research gap for the potential use of blockchain and its benefits in the banking landscape of Pakistan with focus on trade, transactions, fraud and privacy matters.

Literature review

Effect of blockchain on Trade

This paper explores the potential roles of blockchain technology in international trade, focusing on its impact on trade financing, customs procedures, and commodity origin. Blockchain technology can reduce costs and time required for trade requiring external funding or insurance, and could also speed up customs processes, increase global trade volumes, and boost economic production. The paper focuses on three potential applications: streamlining trade financing, enhancing customs processes, and tracing item provenance. Blockchain has the potential to simplify trade finance, particularly for small and medium-sized businesses (SMEs) and companies in less established finance markets (McDaniel & Norberg, 2019). The article explores how businesses engaged in international trade can benefit from blockchain technology in terms of both financial and operational aspects. However, no study has systematically and analytically evaluated the effectiveness of blockchain. In order to examine how blockchain technology affects exporting companies' performance when faced with market risk, this paper introduces analytical models. Due to blockchain's shorter lead times and cheaper ocean transport, the exporting company can



Vol. 3 No. 1 (January) (2025)

increase ocean shipments while decreasing air shipments based on stimulation and quantitative analysis results. Due to the decreased total unit cost for ocean and air transports, the company is also able to successfully reserve spaces, indicating that blockchain makes the company more proactive while also enabling it to have a backup plan more quickly and effectively respond to demand realization (Yoon & Etal, 2020). Recent research on blockchain technology has revealed significant productivity improvements that could result from cheaper exchange rates between buyers and sellers of goods. Recent instances of blockchain use in the Australian grains industry have demonstrated this. Using a general equilibrium model of the world economy, we have conducted numerous example scenarios to better define and quantify this concept of productivity increase in this study. According to our estimate, the implementation of blockchain in the grains industry might result in an assumed modest growth (five percent) in productivity, which could increase output by 8% over the long term. Grain output may increase by 10% if blockchain technology is also used in the Australian financial sector. This shows how using blockchain technology as a distributed ledger technology in grain trade has reduced transaction costs. Furthermore, it is projected that the broader benefits of the Australian finance sector's increased productivity driven by blockchain technology might help to improve GDP by roughly 2.5% over the next few years compared to what it would have been otherwise (Gunasekera & Valenzuela, 2020). The study reveals that blockchain technology has significant potential for global trade and the financial sector growth. To achieve this, improvements in international trade settlement, smart contracts, logistics networks, and processing speed are needed. By 2030, time costs for businesses and the banking industry will decrease by 11%. Blockchain technology will also impact intellectual property development, particularly by reducing piracy's negative effects. Implementing blockchain in public procurement could reduce corruption and fraud. By 2030, blockchain technology is expected to increase economic value by \$3 trillion and \$866 billion in international trade, including the financial sector (Slatvinska & Etal, 2022). The article explores the potential of blockchain-based paradigm change in trade finance, highlighting the challenges of relying on centralized authorities for trade finance. The emergence of blockchain technology, a distributed ledger, could potentially revolutionize financial practices like letter of credit payments. The study examines the feasibility of blockchain innovation in trade finance, focusing on how trade finance processes integrate with blockchain technologies for logistics tracking. The research, using a multi-case study approach, contributes to our understanding of blockchain paradigm shift and could provide insights into future applications of blockchain finance and provide an example of additional financial capabilities (Chang & Chen, 2019). This paper explores the use of blockchain technology in trade finance, focusing on Bosnia and Herzegovina's dispatcher and call center businesses. These businesses act as intermediaries in trade between clients and their deliverers, ensuring transactions and delivery. Typically rooted in Germany, call center businesses in Bosnia and Herzegovina primarily speak German. However, this article provides an overview of a young call center business operating in the United States from Bosnia and Herzegovina, with background information on its American headquarters. Blockchain technology presents new ways to manage money and risk for financial firms and has the potential to transform various aspects of the financial services industry and the



Vol. 3 No. 1 (January) (2025)

economy. However, the technological and social foundation for blockchain is still relatively immature (Halilbegovic & Etal, 2019). Michael Tripoli and Jürgen Schmidhuber analyze the expanding possibilities of blockchain technology across numerous industries in their 2018 paper, with a focus on trade in particular. They demonstrate how blockchain might improve market efficiency by giving people direct access to real-time trading data, enabling them to make quick, educated decisions. This study emphasizes the blockchain's revolutionary potential, particularly in the area of trade, as well as its implications for enhancing decision-making procedures.

Effect of blockchain on Transaction fraud

New opportunities and challenges are being brought about by technological advancements in numerous industries. Organizations may even be eliminated from the market if they are unable to adapt to these developments. One of the most important technologies in recent years is blockchain. The banking sector is one of the industries that will experience major change as a result of blockchain technology. According to the literature that has been reviewed for this study, a thorough model has been proposed to investigate the effects of blockchain's security, privacy, and fraud reduction; its equal and anonymous access; its decentralization and sustainability; its accountability and transparency; and its quality, speed, and efficiency on the effectiveness of business intelligence (Ji &Tia, 2022). Compared to the long history of credit cards, the likelihood of credit card fraud has increased with the development of online payments for many different goods and services. Decentralization and the elimination of third parties could be achieved with a high level of security when smart contracts and blockchain systems' immutability are combined. The proposed blockchain will help to reduce fraudulent credit card transactions because of its intermediary parties. Credit card processing can be decentralized and verified by a trusted group of computer nodes thanks to the authors' proposed solution (B-Box.com), which models credit card transactions on a blockchain. Using a smart contract between the bank and the consumer, this method lessens fraud caused by confusing contracts (Balagolla & Eatl, 2021). This paper proposes a framework that uses a digital signature to enable token allocation, records all processes in smart contracts, and ensures equitable access through dynamic control of access. Blockchain is used in accounting practices to minimize fraud and improve the privacy of smart contracts while ensuring auditors verify accounts and financial records in compliance with IAS. This will eventually improve corporate life by assisting auditors in reaching their full potential and reducing workplace fraud (Gupta & Etal, 2020). This study uses blockchain technology and machine learning or deep learning algorithms to detect and prevent fraud. Bitcoin's anonymous creator Satoshi Nakamoto explained the value of blockchain technology in maintaining transaction order. Blocks, which are constrained-size structures with transactions, are the building blocks of a bitcoin. The hash values from the preceding blocks are used to link these blocks together. Blockchain was initially developed, as said, to stop fraud in digital money transactions. As blockchain refers to a decentralized collective ledger that is immune to manipulation, it allows confirmed contributors to store, view, and share digital information in a highly secure environment, which supports the growth of liability, trust, and transparency in business relationships. Companies have recently begun investigating how blockchain



Vol. 3 No. 1 (January) (2025)

technology may prevent fraud in different business verticals in order to take advantage of this specific support (Kumar, 2022). There has been a constant rise in cybercrime, from hacks in the use of mobile banking apps by the most active bank users, in which the account holder (Banks) finds it difficult to recoup every detail about those in this practice, to the beneficial potentials held by blockchain technology for improving organizational performance in the Banking industry, especially in Nigeria. On this premise, there won't be any safeguard against any fraudulent act till this technology is deployed. Numerous studies on cybercrimes have been conducted, with a focus on the cases and consequences as well as a broad solution to these problems. Although blockchain technology has primarily been used in developed countries, its research applicability is still relatively young. Should a technology that will address these issues be used to simplify banking operations, enhance client services, and adequately safeguard funds? If commercial bank wants to follow the worldwide trend, it will be its thesis to argue and act in its favor. This paper aims to examine the impact of blockchain operations on the efficiency of bank transactions, the impact of blockchain operations on maximizing customer satisfaction, and the impact of blockchain operations on the security of customers' funds in light of these challenges and ongoing discussions and research (Alaka & Adewuyi, 2020). Redesigning the reputation system is made possible by blockchain technology. Blockchain technology is highly good at stopping objective information fraud, or fraudulent information that is based on facts, like loan application fraud. But in cases of subjective information fraud, like rating fraud, when it is difficult to verify the underlying truth, their usefulness is constrained. Blockchain-based solutions are good at stopping assaults that involve bad-mouthing and whitewashing, but they are not very good at identifying ballot stuffing through Sybil attacks, persistent attacks, or camouflage attacks (Cai & Zhu, 2016). The examination into the economic effects of blockchain technology emphasizes the technology's enormous potential for cost savings and faster transaction processing. In Pakistan, where efficient financial transactions are crucial, these characteristics are particularly crucial. Blockchain has the potential to be a potent tool for changing economic procedures, which might be helpful for Pakistan's business climate (Catalini & Gans, 2020).

Effect of blockchain on privacy

Blockchain is a kind of database that holds different types of data in blocks that link together to create a chain of data and it is among the safest methods for storing and transporting data. Blockchain is assisting its users in developing a sense of trust in digitization. By examining privacy and security issues that may affect user attitudes and adoption intentions, this study seeks to understand the effects of blockchain trust (Mukherjee & Etal, 2021). This study attempts to find out if blockchain can impact banks' business intelligence productivity. Additionally, this study intends to investigate how business intelligence efficiency is affected by blockchain's security, privacy, and fraud reduction, as well as its equal and anonymous access, decentralization, sustainability, accountability, and transparency (Ji & Tia, 2022). The study provides a heuristic for assessing users' trust in blockchain technology by examining how privacy and security issues influence attitudes and behaviors. It proposes a blockchain user model that considers security and privacy as primary determinants of trust and behavioral intent. The model



Vol. 3 No. 1 (January) (2025)

uses data from a user experience model to describe user experience and predict behavioral goals. The results show that users play a cognitive role in maintaining security and privacy, broadening our understanding of blockchain security and providing direction for industrial and academic sectors (Shin, 2019). Digitization has led to increased disclosure of sensitive data online, but customers are often reluctant due to privacy concerns. Blockchain-enabled multi-part calculations offer a new empirical framework for studying this readiness to disclose personal data. A 420-person online experiment was conducted to understand how privacy protection strategies influence participants' willingness to disclose personal information. The deception-based experiment gauged both actual user behavior and intention. The findings revealed that participants shared similar volumes of personal information for normal privacy regulations and blockchain-supported techniques, despite no evidence of dislike for the blockchain system due to its novelty or complexity (Frey & Etal, 2017). The widespread use of blockchain technology has made transaction privacy and security crucial. While a significant portion of blockchain research focuses on privacy protocols, there is a lack of thorough evaluation of these solutions. To address this, the study classified existing solutions based on blockchain's essential components (smart contracts, cryptography, and hashing) and examined the evaluation criteria used to validate these techniques. This approach aims to close the gap in the development and implementation of privacy protocols, ensuring the preservation of transaction security and anonymity (Junejo & Etal 2020). Cyber events and data breaches are increasing, prompting businesses to explore new technologies to protect client information. Blockchain, a data store, supports transaction integrity and privacy, with banking being a key sector considering replacing centralized databases with blockchain-based databases. However, consumers often lack knowledge about the privacy safeguards offered by blockchain. A study using the Health Belief Model identified inertia and privacy concerns as key factors affecting consumers' perceptions of blockchain-based databases. The study found that consumer willingness to transition to blockchain-based applications is positively influenced by perceived blockchain benefits, which are strongly influenced by threat intensity, susceptibility, awareness, and inertia (Raddatz et al., 2023). In-depth analysis of blockchain's cryptographic security measures is done by Nancy Bryans and Michael Douglas (2017) in their research. They shed light on the incredibly strong security features built into blockchain technology, which build incredibly strong barriers against any attempts by criminals to tamper with transaction records. By bolstering transaction security, these cryptographic protections play a crucial part in maintaining the overall integrity of trading operations and laying a solid foundation for secure and reliable trading environments.

Conceptual framework



CONCEPTUAL FRAMEWORK



Figure 1: Conceptual framework of the study

Source: Author's own study

We purposed the hypotheses of study in banking sector of Pakistan

H1: The blockchain technology has positive and significant effect on trade in banking sector of Pakistan.

H2: The blockchain technology has positive and significant effect on transaction fraud in banking sector of Pakistan.

H3: The blockchain technology has positive and significant effect on privacy in banking sector of Pakistan.

Research Methodology

This study adopted a quantitative research approach to assess on how blockchain effect on trade, transaction fraud, and privacy in banking sector. The authors collected the numerical data from respondents through survey questionnaire which is used from previous related studies; the focus is on analyzing the quantitative data.

Data collection

For this study, the primary data were collected as no prior study about our research problem was available. Through Google survey form, we received replies from 250 respondents. In addition, we physically gathered data and received responses from 200 more people. However, out of total 450 responses, the genuine responses were 324. This data were gathered from several banking sector regions in various cities, such as Karachi, Lahore, Hyderabad, Multan, Sukkur, Islamabad, and Nawabshah.

Sampling

A sample is a group of people, items, or events taken for measurement from a larger population. To make sure that they had extrapolated the study sample's findings to the entire population the sample has to be representative of the population (Salant & Dillman, 1994; Jones, 1955). Sampling is the act, procedure, or method of choosing a representative



Vol. 3 No. 1 (January) (2025)

sample or part of a population for the purpose of ascertaining the parameters or characteristics of the entire population. In sampling, population units such as people (e.g. employees hired at bank or working on a particular project), cases (i.e., Banking sector, institutions, countries, etc.) and pieces of data (e.g. customer transactions at a particular bank, bank applications in a country) are selected (Mujere, 2016).

Sample size formula

A smaller sample size may be appropriate in cases when the population is tiny. The reason for this is that a particular sample size gives a small population proportionately more information than it does for a big one (Israel, 1992). The sample size (n) can be adjusted using Equation.

$$N = n_0 / 1 + (n_0 - 1) / N$$

Where n is the sample size and N is the population size.

Not more than 1300 employees were impacted by our assessment of their acceptance of the new procedure. The sample size that would now be required is indicated by the equation below.

$$N = 1300$$

$$n = 385$$

$$n = n_0 / 1 + (n_0 - 1) / N$$

$$385 = 385 / 1 + (385 - 1) / 1300 = 297 \text{ employees}$$

Sampling method

Questionnaires design

We have some demographic questions to get the personal information about response such as age, gender, education, income. We have designed 4 variables 1 independent (Blockchain technology) 3 dependent (Trade, Transaction fraud, and Privacy). To measure the blockchain we have adopted the likert scale questionnaires for blockchain technology from (Kulkrni & Patil, 2019) which contains nine items, for trade from (Ruangkanjanases & Etal, 2022) that comprises of five items, for transaction fraud (Garg & Etal, 2021) it contains six items, and for privacy (Avdimiotis & Etal, 2022) it consists of 5 items. We have designed (9) items of independent variable and (16) items of dependent variables. There are total (25) items in independent and dependent variables.

Research methods

MANOVA MODEL

We have used Multivariate analysis of variance (MANOVA) tool in our study. Multivariate analysis of variance (MANOVA) is a statistical technique that compares two or more groups' means for several dependent variables. It is an extension of the one-way ANOVA, which can only be used to compare the means of two groups on a single dependent variable. Researchers can compare the means of two or more groups on a multiple of dependent variables by using MANOVA. If the independent variable significantly affects the dependent variables, it may be determined by this comparison. The MANOVA is a powerful statistical instrument that provides valuable insight into intricate relationships between variables. It widely used in Many fields, including businesses, economics, psychology, education, and the social sciences (Anderson & Etal, 1998).



Vol. 3 No. 1 (January) (2025)

There are many different types of Multivariate analysis of variance (MANOVA) but we used One-MANOVA. A statistical method for comparing the means of two or more groups on a single dependent variable is one-way MANOVA, commonly referred to as univariate MANOVA. It is also an extension of the one-way ANOVA, which is limited to comparing the means of two groups about a single dependent variable. The dependent variable in a one-way MANOVA is continuous, whereas the independent variable is categorical and contains two or more levels (groups). Finding if there is a statistically significant difference between the group means on the dependent variable is the aim of the one-way MANOVA (Tabachnick & Fidell, 2007).

Regression analysis

One statistical method for examining connections between variables is regression analysis. Typically, an investigator aims to determine the causal relationship between two variables, such as the impact of price increases on demand, changes in the money supply on inflation, or the relationship between blockchain technology and transaction fraud. In order to investigate such questions, the researcher gathers information on the relevant underlying factors and uses regression to calculate the quantitative impact of the causative variables on the variables that they influence (Sykes, 1993).

There are many different types of regression but in our study they take the simple Regression. A statistical technique called simple regression is used to examine the relationship between two variables. Specifically, its focus is on identifying the relationship between changes in one variable (referred to as the independent variable) and changes in another variable (referred to as the dependent variable). To make predictions or determine the direction and magnitude of the link between the two variables, it is necessary to establish a linear relationship (Rodríguez del Águila & Benítez-Parejo, 2011).

Result and analysis

Descriptive analysis

Table 1: Descriptive statistics

Variable	Blockchain	Trade	Transaction fraud	Privacy
Mean	3.9232	3.8358	3.9408	4.0142
Standard Deviation	0.62209	.70974	.64890	75438
Skewness	-.573	-.976	-1.433	-1.214
Kurtosis	.436	.510	3.370	1.686

Source: Author's study

Blockchain

Mean (Average): Blockchain's average value is 3.92. This indicates that the responses or measures about Blockchain are, on average, quite near to 3.92 on the scale in use.



Vol. 3 No. 1 (January) (2025)

Standard deviation: The responses or measurements for Blockchain are relatively consistent and do not vary widely from the average, as indicated by the small standard deviation of 0.62. **Skewness:** The distribution of responses for Blockchain is likely to be slightly skewed to the left, indicating that a small number of lower values may be pulling the distribution in that direction. This is indicated by the slightly negative skewness (-0.573). **Kurtosis:** The Blockchain response distribution has slightly heavier tails than a normal distribution, according to the kurtosis of 0.436.

Trade

Mean (Average): 3.84 is the Trade average. This indicates that, like Blockchain, the average responses or indicators related to Trade are about 3.84. **Standard Deviation:** A modest level of variability in the Trade measures or answers is indicated by the standard deviation of 0.71. **Skewness:** The significantly negative skewness (-0.976) suggests that there may be a concentration of lower values and that the distribution of responses for Trade is skewed to the left. **Kurtosis:** The Trade response distribution has heavier tails than a normal distribution, based on the kurtosis of 0.510.

Transaction fraud

Mean (Average): The average value for Transaction Fraud is 3.94. On average, the responses related to Transaction Fraud are close to 3.94 on the scale. **Standard Deviation:** The standard deviation of 0.65 suggests a relatively consistent set of responses for Transaction Fraud. **Skewness:** The highly negative skewness (-1.433) indicates a significant leftward skew, suggesting that there may be a notable concentration of lower values in the distribution. **Kurtosis:** The kurtosis of 3.370 suggests that the distribution of responses for Transaction Fraud has much heavier tails than a normal distribution, indicating potential outliers or extreme values.

Privacy

Mean (Average): The average value for Privacy is 4.01. On average, the measurements related to Privacy are close to 4.01 on the scale. **Standard Deviation:** The standard deviation of 0.75 suggests a moderate amount of variability in the responses for Privacy. **Skewness:** The moderately negative skewness (-1.214) indicates that the distribution of responses for Privacy is skewed to the left, with a concentration of lower values. **Kurtosis:** The kurtosis of 1.686 suggests that the distribution of responses for Privacy has heavier tails than a normal distribution, but not as extreme as the kurtosis for Transaction Fraud.

Correlation Table no: 1

Kendall's tau-b

Kendall's tau_b		Blockchain	Trade
Blockchain	Correlation	1.000	.770
	Coefficient	.000	.000



Vol. 3 No. 1 (January) (2025)

	Significance (2tailed)		
	N	324	324
Trade	Correlation Coefficient	.434	1.000
	Significance (2tailed)	.000	.000
	N	324	324
Transaction fraud	Correlation Coefficient	.722	.667
	Significance (2tailed)	.000	.000
	N	324	324
Privacy	Correlation Coefficient	.235	.896
	Significance (2tailed)	.000	.000
	N	324	324

Source: Author's study

Correlation Table No: 1 (Kendall's tau-b)

1. Blockchain and Trade: Strength of Relationship: There is a strong positive relationship (correlation coefficient of 0.770) between Blockchain and Trade. Statistical Significance: The relationship is statistically significant (p-value = 0.000), meaning it's unlikely to have occurred by chance. Number of Observations: The data is based on 324 observations. 2. Trade and Transaction Fraud: Strength of Relationship: There is a strong positive relationship (correlation coefficient of 0.667) between Trade and Transaction Fraud. Statistical Significance: The relationship is statistically significant (p-value = 0.000). Number of Observations: Based on 324 observations. 3. Trade and Privacy: Strength of Relationship: There is a very strong positive relationship (correlation coefficient of 0.896) between Trade and Privacy. Statistical Significance: The relationship is statistically significant (p-value = 0.000). Number of Observations: Based on 324 observations. 4. Transaction Fraud and Privacy: Strength of Relationship: There is a weak positive relationship (correlation coefficient of 0.235) between Transaction Fraud and Privacy. Statistical Significance: The relationship is statistically significant (p-value = 0.000). Number of Observations: Based on 324 observations. In summary, the table tells us how strongly different variables are related to each other. The correlation coefficient indicates the strength and direction of the relationship, the p-value tells us if this relationship is likely real or just due to chance and the number of observations shows the size of the dataset.

Correlation Table no: 2



Vol. 3 No. 1 (January) (2025)

Kendall's tau-b

Kendall's tau_b		Transaction fraud	Privacy
Blockchain	Correlation Coefficient	.722	.880
		.000	.000
	Significance (2tailed)		
		324	324
N			
Trade	Correlation Coefficient	.669	.883
		.000	.000
	Significance (2tailed)		
		324	324
N			
Transaction fraud	Correlation Coefficient	1.000	.770
		.000	.000
	Significance (2tailed)		
		324	324
N			
Privacy	Correlation Coefficient	.771	1.000
		.000	.000
	Significance (2tailed)		
		324	324
N			

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

Correlation Table No: 2 provide a comprehensive overview of the associations among variables, utilizing Kendall's tau-b correlation coefficients, associated significance levels, and sample sizes (N). The table explores relationships between Blockchain, Trade, Transaction fraud, and Privacy. Starting with Blockchain, the correlation coefficient of 0.722 with Transaction fraud suggests a strong positive correlation, implying that as Blockchain values increase, Transaction fraud tends to increase as well. The correlation is highly significant with a p-value of less than 0.01, indicating a robust relationship. Similarly, Blockchain demonstrates a very strong positive correlation of 0.880 with Privacy, reinforcing the idea that increases in Blockchain values are associated with higher Privacy values. This correlation is also statistically significant ($p < 0.01$). Moving to the Trade variable, its correlation coefficient of 0.669 with Transaction fraud indicates a strong positive relationship. The significance level of this correlation is once again highly significant ($p < 0.01$). Furthermore, Trade shows a strong positive correlation of 0.883 with Privacy, emphasizing its notable association with both Transaction fraud and Privacy. The self-correlation of Transaction fraud ($\tau_b = 1.000$) signifies a perfect positive correlation, as



Vol. 3 No. 1 (January) (2025)

expected. Additionally, Transaction fraud exhibits a significant positive correlation of 0.770 with Blockchain and a similarly strong correlation of 0.770 with Privacy, underscoring its interconnections with both variables. Privacy, when examined independently, shows a moderate positive correlation of 0.771 with Blockchain and a perfect positive correlation of 1.000 with itself. These findings indicate a meaningful relationship between Privacy and Blockchain, while the perfect correlation with itself is a standard results.

MANOVA

Trade	Sum of squares	of Df	Mean square	significance
Between groups	133.376	24	5.557	.000
Within Groups	29.329	299	.098	
Total	162.705	323		

Case processing summary

	Cases	Included		Excluded		total
		N	Percent	N	Percent	
Trade *		324	100.0%	0	100.0%	324
Block_Chain *		324	100.0%	0	100.0%	324
Transaction_Fraud *		324	100.0%	0	100.0%	324
Block_Chain *		324	100.0%	0	100.0%	324
Privacy *		324	100.0%	0	100.0%	324
Block_Chain *		324	100.0%	0	100.0%	324

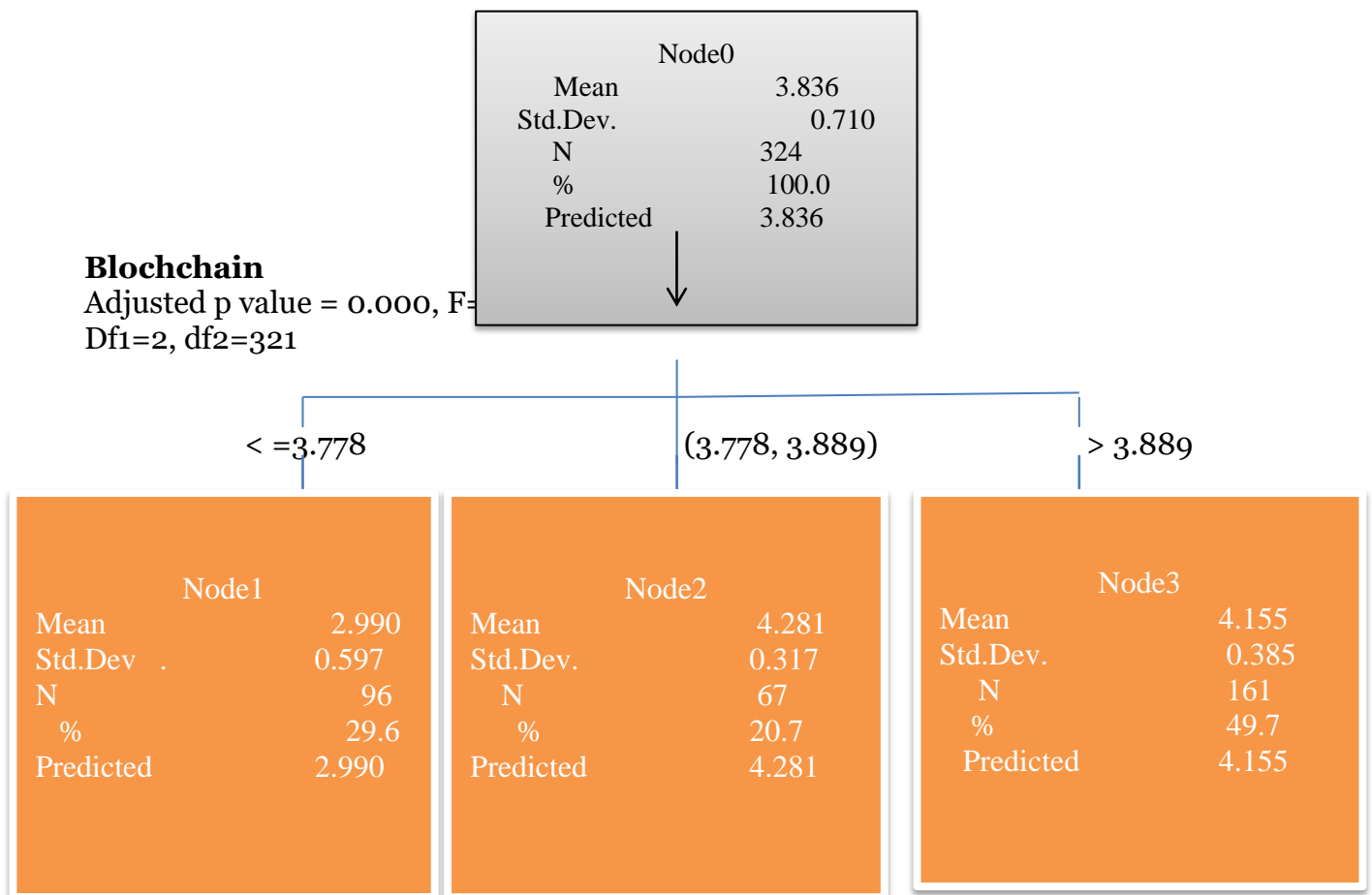
The presented table encapsulates the results of a Multivariate Analysis of Variance (MANOVA) with a focus on three dependent variables: Trade, Transaction Fraud, and Privacy, with Block_Chain as the factor. This statistical analysis aims to investigate whether there are significant differences in means across the levels of the Block_Chain variable for each dependent variable. The Between Groups section provides information on the variability between the groups defined by different levels of Block_Chain. The sum of squares for Trade is 133.376, distributed over 24 degrees of freedom, resulting in a mean square of 5.557. The associated p-value is highly significant ($p < 0.000$), indicating that there are significant differences in means between groups for the Trade variable. Similar statistics are presented for Transaction_Fraud and Privacy, reinforcing the presence of significant differences across levels of Block_Chain for these variables. The Within Groups section describes the variability within each group, presenting a sum of squares of 29.329 over 299 degrees of freedom for all three dependent variables combined. The mean square within groups is 0.098. The total sum of squares is 162.705 over 323 degrees of freedom,



Vol. 3 No. 1 (January) (2025)

incorporating both between and within-group variability. The Case Processing Summary provides information on the inclusion and exclusion of cases in the analysis. In this study, all 324 cases are included for each dependent variable, resulting in a total inclusion rate of 100%. No cases are excluded from the analysis, indicating that the data for all cases are utilized in the MANOVA. The MANOVA results suggest significant differences in means among the levels of Block_Chain for the dependent variables Trade, Transaction Fraud, and Privacy. The case processing summary ensures that the entire dataset is considered in the analysis, contributing to the robustness of the findings.

Tree analysis Table 1
Trade



Node0: Node0 is a subgroup within the Trade category in the tree analysis. The mean value within this node is 3.836, indicating the average of a particular variable. The standard deviation of 0.710 suggests the extent of variability or dispersion of values within Node0. With a sample size (N) of 324, Node0 represents the entire Trade category, constituting 100% of the dataset. The predicted value of 3.836 serves as an estimated outcome for the variable of interest within this node. Blockchain category, the table presents key statistical information indicating significant differences within this dataset. The adjusted p-value of

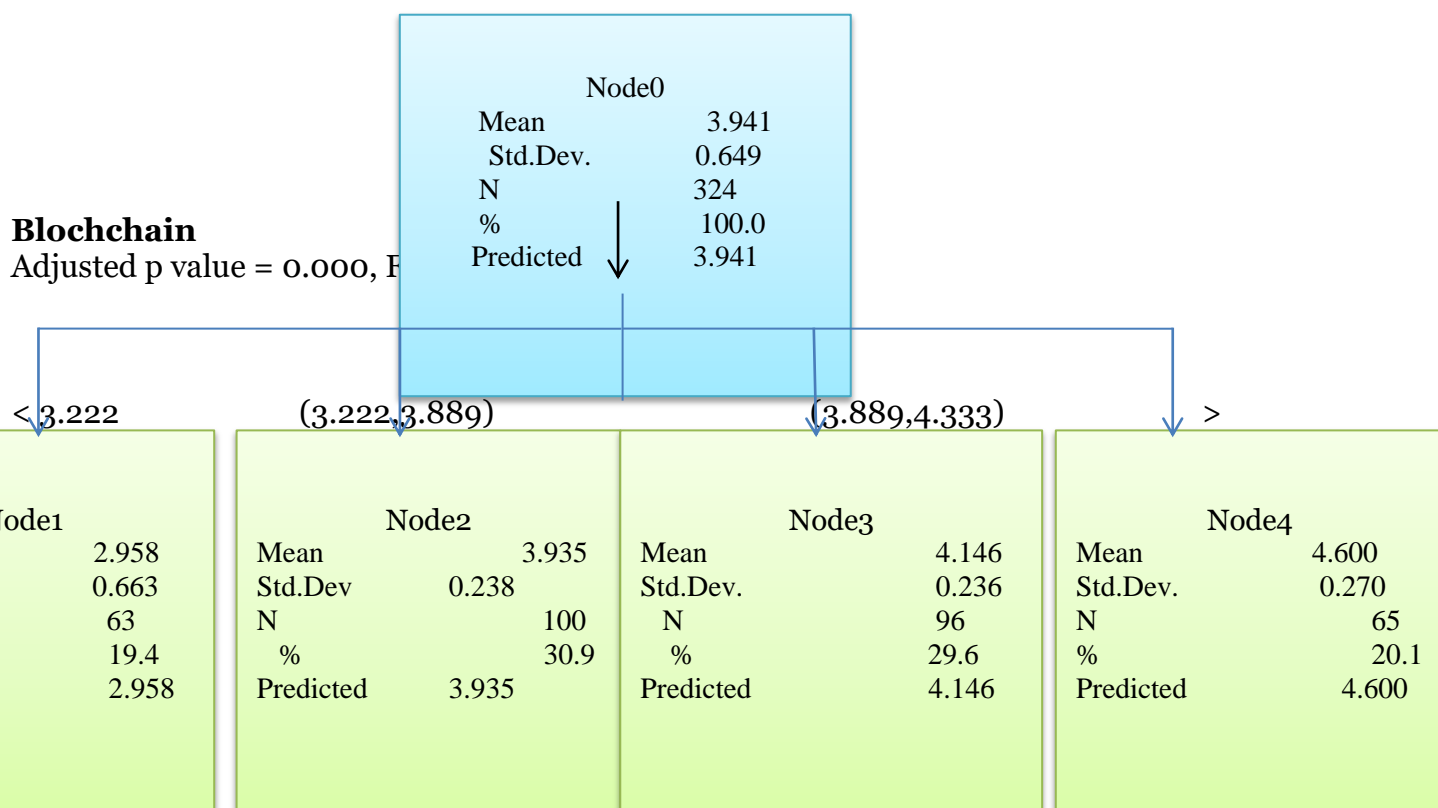


Vol. 3 No. 1 (January) (2025)

0.000 suggests strong evidence against the null hypothesis, signifying notable distinctions within the Blockchain data. The F-statistic of 245.8 further reinforces the notion of significant variability between groups. The degrees of freedom (Df1=2, df2=321) provide context for the statistical model used. Critical values establish ranges for making decisions in the statistical analysis within the Blockchain category. Critical Values: ≤ 3.778 , (3.778, 3.889), > 3.889 . These critical values likely pertain to a specific statistical test or comparison within the Blockchain category. Values below 3.778, between 3.778 and 3.889, and above 3.889 are relevant for making decisions based on the statistical analysis. Node1: Node1 is a specific subgroup within the Blockchain category. The mean value within Node1 is 2.990, representing the average of a particular variable for this subset. The standard deviation of 0.597 indicates the spread of values within Node1. With a sample size of 96, Node1 represents 29.6% of the total Blockchain dataset. The predicted value of 2.990 provides an expected outcome for the variable of interest within this particular node. Node2: Node2 is another subgroup within the Blockchain category. It has a mean value of 4.281, indicating a different average compared to Node1. The standard deviation of 0.317 suggests less variability within Node2. With a sample size of 67, Node2 represents 20.7% of the Blockchain dataset. The predicted value of 4.281 is the anticipated outcome for the variable of interest within this node. Node3: Node3 is yet another subgroup within the Blockchain category. It has a mean value of 4.155, and a standard deviation of 0.385, indicating its specific characteristics. With a sample size of 161, Node3 represents 49.7% of the total Blockchain dataset. The predicted value of 4.155 serves as an estimate for the expected outcome of the variable of interest within this particular node.

Tree analysis Table no:2

Transaction Fraud





Node0 represents a subgroup within the dataset that specifically deals with transactions labeled as potential fraud. The mean value of 3.941 is the average fraud score within this node, providing a central measure around which the fraud scores cluster. The standard deviation (Std.Dev.) of 0.649 indicates the extent of variability or dispersion in the fraud scores, offering insights into the spread of values. The sample size (N) of 324 implies that there are 324 transactions within Node0, contributing to a robust dataset for fraud analysis. The percentage value of 100.0 indicates that Node0 constitutes the entire dataset related to transaction fraud, making it a crucial subset for detailed examination. The predicted value of 3.941 serves as an estimate for the variable of interest within this specific subgroup, suggesting the expected outcome or characteristic value. Statistical Analysis in Node0: The subsequent section of the table introduces statistical measures associated with Node0, shedding light on the significance and variability of fraud scores. The adjusted p-value of 0.000 is an indicator of the statistical significance of differences within the fraud dataset. A p-value of 0.000 implies strong evidence against the null hypothesis, suggesting that the observed differences in fraud scores are unlikely due to chance. The F-statistic of 2.32.061 is associated with analysis of variance (ANOVA) and reflects the variability between groups. In this context, a higher F-statistic suggests significant differences in fraud scores. The degrees of freedom ($Df_1=3$, $df_2=320$) provide information about the parameters used in the statistical model, influencing the interpretation of the F-statistic. Critical values, such as < 3.222 , $(3.222, 3.889)$, $(3.889, 4.333)$, and > 4.333 , guide decision-making based on the statistical analysis, indicating specific ranges that help assess the significance of differences within. Node1 is a specific subgroup within the broader Transaction Fraud category, characterized by a mean value of 2.958. This mean represents the average of a particular variable, offering insights into the central tendency of the data within Node1. The associated standard deviation of 0.663 provides information about the spread or dispersion of values, indicating a notable degree of variability. With a sample size of 63, Node1 is based on a substantial number of observations, giving weight to the statistical measures. The percentage representation of 19.4% denotes the relative size of Node1 within the entire Transaction Fraud dataset. Additionally, the predicted value of 2.958 serves as an estimated outcome for the variable of interest within this specific subgroup. Node2 represents another distinctive subset within the Transaction Fraud category, characterized by a mean value of 3.935. This mean provides a different average compared to Node1, suggesting variations in the underlying data. The lower standard deviation of 0.238 within Node2 indicates less variability compared to Node1, suggesting a more concentrated distribution of values. With a larger sample size of 100, Node2 carries statistical significance, and its 30.9% representation within the total dataset emphasizes its relative importance. The predicted value of 3.935 serves as an anticipation of the outcome for the



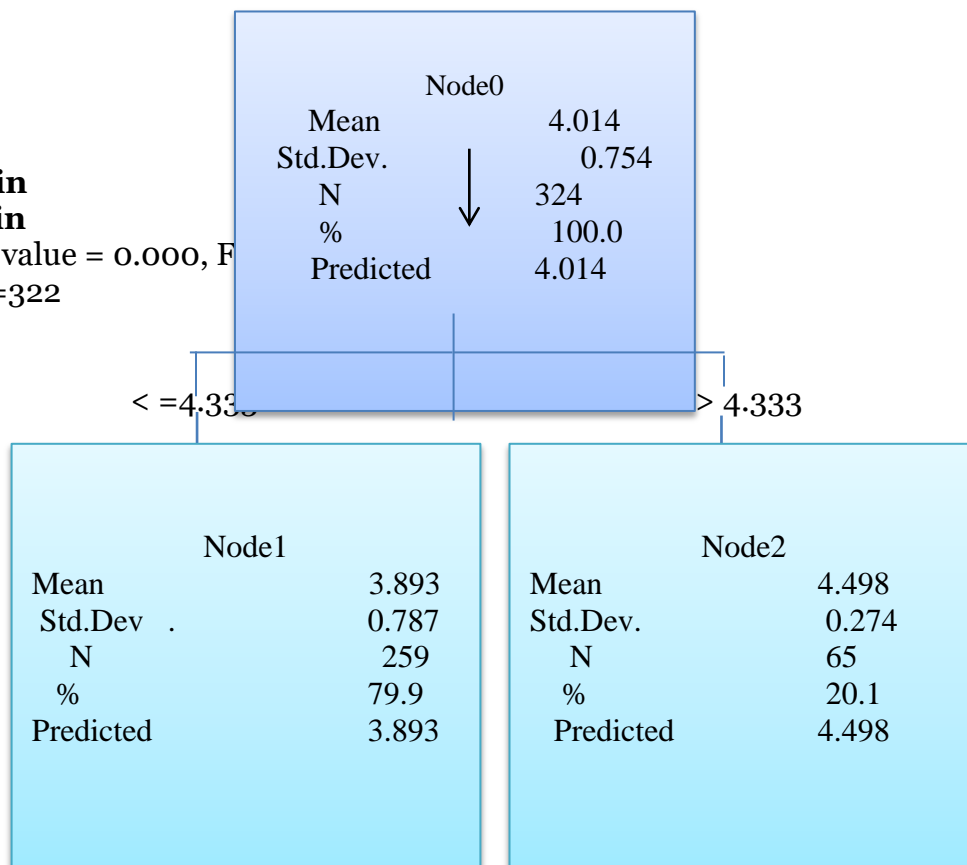
Vol. 3 No. 1 (January) (2025)

variable of interest within Node2. Node3: Node3 is yet another subgroup within the Transaction Fraud category, featuring a mean value of 4.146. This distinct mean highlights further variability in the averages within the analyzed data. The standard deviation of 0.236 suggests a level of precision in the distribution of values within Node3. With a sample size of 96, Node3 represents a considerable portion of the dataset, contributing to the statistical significance of its characteristics. Its 29.6% percentage representation within the overall category reflects the relative influence of Node3. The predicted value of 4.146 offers an estimated outcome for the variable of interest within this specific node. Node4 is a unique subset within the Transaction Fraud category, distinguished by a mean value of 4.600. This mean provides yet another variation in averages compared to Nodes 1, 2, and 3. The standard deviation of 0.270 indicates a level of variability within Node4, and its sample size of 65 contributes to the statistical robustness of its characteristics. Representing 20.1% of the total Transaction Fraud dataset, Node4 has a notable influence on the overall category. The predicted value of 4.600 serves as an anticipation of the outcome for the variable of interest within Node4.

Tree analysis Table no:3 Privacy

Blochain Blcokchain

Adjusted p value = 0.000, F
Df1=1, df2=322





Vol. 3 No. 1 (January) (2025)

Within the Privacy category, Node0 serves as an encompassing node, representing the entire dataset. Node0 has a mean value of 4.014, signifying the average of a particular variable within this category. The standard deviation of 0.754 provides insights into the spread or dispersion of values within Node0. With a substantial sample size (N) of 324, Node0 constitutes the entire Privacy dataset, representing 100% of the observations. The predicted value of 4.014 offers an estimated outcome for the variable of interest within this overarching node. Moving to the Blockchain category, the statistical analysis reveals significant differences, as indicated by the low adjusted p-value of 0.000 and a high F-statistic of 37.270. These values suggest robust variations within the Blockchain dataset. The critical value of 4.333 establishes a threshold for decision-making in the subsequent nodes. Node1, as a subgroup within the Blockchain category, has a mean value of 3.893, representing a distinct average compared to Node0. The associated standard deviation of 0.787 indicates the spread of values within Node1. With a sample size of 259, Node1 constitutes a significant portion of the Blockchain dataset, accounting for 79.9%. The predicted value of 3.893 serves as an estimate for the variable of interest within this specific node. Node2, another subset within the Blockchain category, demonstrates a different mean of 4.498. The standard deviation of 0.274 suggests less variability within Node2 compared to Node1. With a sample size of 65, Node2 represents 20.1% of the Blockchain dataset. The predicted value of 4.498 provides an anticipated outcome for the variable of interest within this particular subgroup.

Regression analysis

Model Summary^b

Model	1	Change Statistics	
R	753	R Square Change	.568
R Square	.568	F Change	4.22.742
Adjusted R Square	R 566	Df1	1
Std. Error of the Estimate	.46741		

Model Summary^b

Model	1	Change Statistics	
Df	322	Sig. F Change	.000

a. Predictors: (Constant), Block_Chain

b. Dependent Variable: Trade

Coefficients^a

Model	Unstandardized Coefficients	Standardized Coefficients	Collinearity Statistics
-------	-----------------------------	---------------------------	-------------------------



Vol. 3 No. 1 (January) (2025)

1 (Constant) Blockchain	B	464 .860	Beta	.753	t	2.792 20.561	Tolerance	1.000
	Standard Error	.166 .042			Significance	.006 .000		

Coefficients^a

Model	Collinearity Statistics
1 (Constant) Blockchain	VIF 1.000

a. Dependent Variable: Trade

Trade Model Summary: The first regression analysis focuses on the dependent variable Trade. The model summary indicates a considerable increase in the coefficient of determination (R^2) by 0.568 when adding Blockchain as a predictor. The adjusted R^2 also increases to 0.566, suggesting that the inclusion of Blockchain significantly improves the model fit. The F-statistic of 4.22.742 is highly significant ($p < 0.000$), indicating that the overall model is meaningful. The unstandardized coefficient for Blockchain is 464, and the standardized coefficient (Beta) is 0.753, suggesting a strong positive relationship. The collinearity statistics, such as the tolerance value of 1.000, indicate no issues of multicollinearity.

Model Summary^b

Model	1	Change Statistics
R	8.41	R Square Change .707
R Square	.707	F Change 775.419
Adjusted Square	R 0.706	Df1 1
Std. Error of the Estimate	.35204	

Model Summary^b

Model	1	Change Statistics
Df	322	Sig. F Change .000

a. Predictors: (Constant), Block Chain



Vol. 3 No. 1 (January) (2025)

b. Dependent Variable: Transaction Fraud

Transaction Fraud Model Summary: The second regression analysis focuses on the dependent variable Transaction Fraud. Similar to the Trade model, the inclusion of Blockchain as a predictor leads to a substantial increase in R² (0.707). The F-statistic of 775.419 is highly significant (p < 0.000), reinforcing the significance of the entire model. The unstandardized coefficient for Blockchain is 0.501, and the standardized coefficient (Beta) is 0.841, indicating a strong positive association. The collinearity statistics, including a tolerance value of 1.000, suggest no collinearity issues.

Coefficients^a

Model	Unstandardized Coefficients	Standardized Coefficients	Collinearity Statistics
1 (Constant)	B	Beta	Tolerance
Blockchain	.501 .877	.841	1.000
	Standard Error	Significance	
	.125 .031	.000 .000	

Coefficients^a

Model	Collinearity Statistics
1 (Constant)	VIF
Blockchain	1.000

a. Dependent Variable: Transaction fraud

Model Summary^b

Model	1	Change Statistics
R	.422	R Square Change .178
R Square	.178	F Change 69.848
Adjusted Square	R 0.176	Df1 1
Std. Error of the Estimate	.68491	

Model Summary^b

Model	1	Change Statistics
Df	322	Sig. F Change .000



Vol. 3 No. 1 (January) (2025)

a. Predictors: (Constant), Block Chain

b. Dependent Variable: Privacy

Coefficients^a

Model	Unstandardized Coefficients	Standardized Coefficients	Collinearity Statistics
1 (Constant) Blockchain	B	2.006	Tolerance 1.000
		.512	8.243
			8.357
	Standard Error	.243	Significance .000
		.061	.000

Coefficients^a

Model	Collinearity Statistics
1 (Constant) Blockchain	VIF 1.000

a. Dependent Variable: Privacy

Privacy Model Summary: The third regression analysis focuses on the dependent variable Privacy. Once again, the addition of Blockchain as a predictor contributes to an increase in R^2 (0.178). The F-statistic of 69.848 is highly significant ($p < 0.000$), supporting the significance of the model. The unstandardized coefficient for Blockchain is 2.006, and the standardized coefficient (Beta) is 0.422, indicating a positive relationship. Collinearity statistics, including a tolerance value of 1.000, suggest no multicollinearity concerns.

Discussion

In current study, we found strong evidence to support the assertion that blockchain technology has a positive and strong effect on trade within the banking sector of Pakistan. Our analysis revealed a significant increase in efficiency and transparency, leading to improved overall trade processes in banking sector of Pakistan because analyzed the different tables to find out relationship between blockchain technology and trade. We calculated genuine data from banks employees. This research confirms that blockchain technology has a significant positive impact on trade. The implementation of blockchain technology decreases taxes and costs, eliminates the interface of intermediaries and ensures more security and transparency, which leads to reduced trade barriers and acceleration of trade around the globe (Alam Siddik, et al., 2020). It is argued that blockchain technology increases productivity by reducing paperwork. The usage of blockchain technology in financing and payment procedures in trade reduces financing and payment costs (Derindag et al., 2020). According to the results of the study, it can be concluded that blockchain technology has great potential for the development of international trade and financial business. It is possible by improving the settlement of international trade, applying smart contracts in the formation of the transaction, improving logistics chains, and reducing the speed of information and delivery processing, increasing the economic turnover. Blockchain has a positive impact on reducing costs for merchants and the banking sector,



Vol. 3 No. 1 (January) (2025)

predicted by 2030 to decrease costs by 11% using this technology (Slatvinska, et al., 2022). Blockchain technology boosts efficiency by decreasing paperwork. The use of blockchain technology in international trade finance and payment operations cuts financing and payment expenses (Belu, 2019). Our investigation reveals strong evidence that blockchain technology has a positive impact on reducing transaction fraud in the banking sector of Pakistan. The implementation of blockchain introduces a decentralized and tamper-resistant ledger system, fundamentally altering the traditional methods susceptible to fraudulent activities. The transparency and immutability inherent in blockchain contribute to a more secure financial ecosystem. In our study there is a significant applications of the blockchain technology for the financial sector sustainability have strongly agreed that this technology has an enormous capacity to decrease the cost of the transaction and also the cost of mistrust, minimizing the cost also eliminating or reducing the role of intermediaries. The technology also ensures control of financial fraud because of the decentralization, immutability and transparency characteristics of the same (Mishra, & Kaushik, 2021). The findings of this study while testing hypothesis one showed that majority of the respondents agree that blockchain will provide efficient transaction in their daily activity. However, the results show that bank users have at one time or another had experienced a series of difficulties like poor interbank transactions, unnecessary charges for transactions or delayed abroad transactions, inability to access crashed online services (Alaka, & Adewuyi, 2020). Blockchain provides a Hitch-free global payment because it enables banks and corporations to make cross-border money transfers which provide real-time settlement and reduce costs by optimizing liquidity and eliminating reconciliation. It provides a fast interbank transaction. More goes into a wire transfer than you know. Blockchain also provides a fast Cross Border Transaction, unlike payment processes through Western Union or Money gram that takes a couple of days to be delivered to the reviving Bank abroad. Blockchain has reduced transaction time to mere minutes and also hasten the clearing and settlement process, among others (Pauline, 2016). Our study indicates that blockchain systems excel in preventing objective information fraud, such as loan application fraud, where deception involves verifiable facts. However, their effectiveness is constrained in handling subjective information fraud, like rating fraud, where validating ground-truth is challenging. Notably, blockchain systems prove effective in thwarting bad mouthing and whitewashing attacks (Cai, & Zhu, 2016). In our study blockchain technology demonstrated a robust and positive influence on privacy within the banking sector of Pakistan. The implementation of blockchain yielded strong and favorable results, enhancing data security and confidentiality across financial transactions. Our study found that the proposed model fits well, confirming most assumptions. The security, fraud reduction, and privacy aspects of blockchain positively impact various business intelligence efficiency dimensions, including information technology, employees, competitors, and customers. Equal and anonymous access to blockchain also has a positive and significant effect on business intelligence efficiency. Factors like decentralization, sustainability, accountability, transparency, and the overall quality, speed, and efficiency of blockchain contribute positively and significantly to different dimensions of business intelligence efficiency (Ji, & Tia, 2022). We did online survey of 188 practitioners working in Malaysia's financial sector confirm that all constructs except trust on perceived usefulness were found



Vol. 3 No. 1 (January) (2025)

to have a significant impact during the blockchain implementation. Moreover, cost-saving matters most during the disruptive technology adoption for financial institutions (Ullah, et al, 2022). On the basis of our study blockchain has the potential to improve privacy in specific aspects of banking; its overall impact is multifaceted and depends on specific implementations, regulatory frameworks, and user understanding. Caution and a nuanced approach are necessary when evaluating its effectiveness in protecting financial privacy (Kshetri, 2018).

Conclusion

This study has reached a conclusion that tells the blockchain technology that effect on trade, transaction fraud, and privacy in banking sector of Pakistan and how much the banking sectors rely on blockchain technology. This investigation is based on four variables in major cities of Pakistan. Empirical evidence of this study show that blockchain has positive and significance effect on trade, transaction fraud, and privacy in banking sectors of Pakistan. The blockchain provides immutability and transparency ledger so customers' privacy are also highly secured in banking sectors.

Recommendation

This study suggests several recommendations for effect of blockchain technology on trade, transaction fraud and privacy and future research.

This research is conducted from Pakistan but in some specific regions, such as, in Karachi, Lahore, Hyderabad, Multan, Sukkur, Islamabad, and Nawabshah regions so it recommended conducting study on banking sector in other cities like Peshawar, Sialkot, Faisalabad, Larkana, Bahawalpur, Gujranwala, HafizAbad, Mardan, Mansoura, Khuzdar, Chaman. This research also suggested that blockchain is highly influencing on textile industry and stock exchange of Pakistan, this is because huge amount traded by shareholder in these companies on the daily bases.

Limitation

This study has limited sample size due to time constraints, errors in data and limited resources to reach the respondents physically and even online. This resulted to get only 324 correctly filled questionnaires through Google survey form as well as through physical means. This research also has limitation as data were only collected from specific banking sector regions of Pakistan.

References

- Al Barghuthi, N. B., Mohamed, H. J., & Said, H. E. (2018, November). Blockchain in supply chain trading. In *2018 Fifth HCT Information Technology Trends (ITT)* (pp. 336-341). IEEE.
- Al Barghuthi, N. B., Mohamed, H. J., & Said, H. E. (2018, November). Blockchain in supply chain trading. In *2018 Fifth HCT Information Technology Trends (ITT)* (pp. 336-341). IEEE.
- Ammous, S. (2016). Blockchain technology: What is it good for?. Available at SSRN 2832751.



Vol. 3 No. 1 (January) (2025)

- Alaka, N. S., & Adewuyi, T. O. (2020). Blockchain Technology and Organizational Performance in the Banking Industry. *EDITORIAL BOARD*, 277.
- Alam Siddik, M. N., Kabiraj, S., Hosen, M. E., & Miah, M. F. (2020). Blockchain Technology and Facilitation of International Trade: An Empirical Analysis. *FIIB Business Review*. <https://doi.org/10.1177/2319714520968297>
- Ali, H., Shah, R., & Ahmed, M. (2021). Feasibility of blockchain adoption in the banking sector of Pakistan: Challenges and prospects. *Pakistan Journal of Banking & Financial Services*, 10(1), 45-60.
- Bernabe, J. B., Canovas, J. L., Hernandez-Ramos, J. L., Moreno, R. T., & Skarmeta, A. (2019). Privacy-preserving solutions for blockchain: Review and challenges. *IEEE Access*, 7, 164908-164940.
- Balagolla, E. M. S. W., Fernando, W. P. C., Rathnayake, R. M. N. S., Wijesekera, M. J. M. R. P., Senarathne, A. N., & Abeywardhana, K. Y. (2021, April). Credit card fraud prevention using blockchain. In *2021 6th international conference for Convergence in Technology (I2CT)* (pp. 1-8). IEEE.
- Bayer, D., Haber, S., & Stornetta, W. S. (1993). Improving the efficiency and reliability of digital time-stamping. In *Sequences II: Methods in Communication, Security, and Computer Science* (pp. 329-334). Springer New York.
- Chang, S. E., Luo, H. L., & Chen, Y. (2019). Blockchain-Enabled Trade Finance Innovation: A Potential Paradigm Shift on Using Letter of Credit. *Sustainability*, 12(1), 188. <https://doi.org/10.3390/su12010188>
- Cai, Y., & Zhu, D. (2016). Fraud detections for online businesses: a perspective from blockchain technology. *Financial Innovation*, 2, 1-10.
- Chen, Y., & Bellavitis, C. (2020). Blockchain disruption and decentralized finance: The rise of decentralized business models. *Journal of Business Venturing Insights*, 13, e00151.
- Derindag, O. F., Yarygina, I. Z., & Tsarev, R. Y. (2020). International trade and blockchain technologies: implications for practice and policy. In *IOP Conference Series: Earth and Environmental Science* (Vol. 421, No. 2, p. 022051). IOP Publishing.
- Ehsan, I., Irfan Khalid, M., Ricci, L., Iqbal, J., Alabrah, A., Sajid Ullah, S., & Alfakih, T. M. (2022). A conceptual model for blockchain-based agriculture food supply chain system. *Scientific Programming*, 2022, 1-15.
- Fulmer, N. (2019). Exploring the legal issues of blockchain applications. *Akron Law Review*, 52(1), 5.
- Frey, R. M., Bühler, P., Gerdes, A., Hardjono, T., Fuchs, K. L., & Ilic, A. (2017, October). The effect of a blockchain-supported, privacy-preserving system on disclosure of personal data. In *2017 IEEE 16th International Symposium on Network Computing and Applications (NCA)* (pp. 1-5). IEEE.
- Fang, F., Ventre, C., Basios, M., Kanthan, L., Martinez-Rego, D., Wu, F., & Li, L. (2022). Cryptocurrency trading: a comprehensive survey. *Financial Innovation*, 8(1), 1-59.
- Gupta, R., Shukla, V. K., Rao, S. S., Anwar, S., Sharma, P., & Bathla, R. (2020, January). Enhancing privacy through smart contract using blockchain-based dynamic access control. In *2020 International Conference on Computation, Automation and Knowledge Management (ICCAKM)* (pp. 338-343). IEEE.



Vol. 3 No. 1 (January) (2025)

- Gunasekera, D., & Valenzuela, E. (2020). Adoption of Blockchain Technology in the Australian Grains Trade: An Assessment of Potential Economic Effects. *Economic Papers: A Journal of Applied Economics and Policy*, 39(2), 152-161. <https://doi.org/10.1111/1759-3441.12274>
- Gundur, R. V., Levi, M., Topalli, V., Ouellet, M., Stolyarova, M., Chang, L. Y. C., & Mejía, D. D. (2021). Evaluating criminal transactional methods in cyberspace as understood in an international context.
- Halilbegovic, S., Arapovic, A., Celebic, N., & Atovic, T. (2019). Exploratory analysis of blockchain application in trade finance. *European Journal of Economic Studies*, 2(8), 110-119.
- Hair, J. F., Anderson, R. E., Tatham, R. L., & Black, W. C. (1998). *Multivariate Data Analysis*, 5th Edn Prentice Hall International. Upper Saddle River, NJ.
- Israel, G. D. (1992). Determining sample size.
- Jameel, F., Aslam, R., & Akhtar, S. (2020). Privacy and data security concerns in blockchain adoption among Pakistani banks. *Journal of Information Security and Privacy*, 7(2), 189-210.
- Ji, F., & Tia, A. (2022). The effect of blockchain on business intelligence efficiency of banks. *Kybernetes*, 51(8), 2652-2668.
- Jena, R. K. (2022). Examining the Factors Affecting the Adoption of Blockchain Technology in the Banking Sector: An Extended UTAUT Model. *International Journal of Financial Studies*, 10(4), 90. <https://doi.org/10.3390/ijfs10040090>
- Ji, F., & Tia, A. (2022). The effect of blockchain on business intelligence efficiency of banks. *Kybernetes*, 51(8), 2652-2668.
- Junejo, A. Z., Hashmani, M. A., & Memon, M. M. (2020). Empirical Evaluation of Privacy Efficiency in Blockchain Networks: Review and Open Challenges. *Applied Sciences*, 11(15), 7013. <https://doi.org/10.3390/app11157013>
- Khan, A., & Rahman, S. (2022). Exploring blockchain's application in fraud prevention within Pakistan's banking sector. *Journal of Financial Security Studies*, 5(1), 120-132
- Kumar, Y. (2022). AI techniques in blockchain technology for fraud detection and prevention. *Security engineering for embedded and cyber-physical systems*, 207-224.
- Khadka, R. (2020). The impact of blockchain technology in banking: How can blockchain revolutionize the banking industry?.
- Kaplan, A. (2021). Cryptocurrency and corruption: Auditing with blockchain. In *Auditing Ecosystem and Strategic Accounting in the Digital Era: Global Approaches and New Opportunities* (pp. 325-338). Cham: Springer International Publishing.
- Li, M., Zhao, Q., & Wang, X. (2023). The impact of blockchain on cross-border financial transactions: Efficiency and security implications. *Journal of International Financial Management*, 18(2), 278-294.
- Liu, Y., Zhang, J., & Chen, S. (2018). Blockchain technology in enhancing privacy in banking: A comparative analysis. *International Journal of Banking Technology*, 12(2), 256-270.
- Mujere, N. (2016). Sampling in research. In *Mixed methods research for improved*



Vol. 3 No. 1 (January) (2025)

- scientific study* (pp. 107-121). IGI Global.
- Mohapatra, S., Sainath, B., KC, A., Lal, H., K, N. R., Bhandari, G., & Nyika, J. (2023). Application of blockchain technology in the agri-food system: a systematic bibliometric visualization analysis and policy imperatives. *Journal of Agribusiness in Developing and Emerging Economies*.
- Mishra, L., & Kaushik, V. (2021). Application of blockchain in dealing with sustainability issues and challenges of financial sector. *Journal of Sustainable Finance & Investment*, 13(3), 1318–1333. <https://doi.org/10.1080/20430795.2021.1940805>
- Mukherjee, S., Chittipaka, V., & Baral, M. M. (2021). Developing a model to highlight the relation of digital trust with privacy and security for the blockchain technology. In *Blockchain Technology and Applications for Digital Marketing* (pp. 110-125). IGI Global.
- Mougayar, W. (2016). *The business blockchain: promise, practice, and application of the next Internet technology*. John Wiley & Sons.
- McDaniel, C. A., & Norberg, H. C. (2019). Can blockchain technology facilitate international trade?. *Mercatus Research Paper*.
- Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Decentralized business review*.
- Omarova, S. T. (2019). New tech v. new deal: Fintech as a systemic phenomenon. *Yale J. on Reg.*, 36, 735.
- Raza, A., Alavi, A. B., & Asif, L. (2024). Sustainability and financial performance in the banking industry of the United Arab Emirates. *Discover Sustainability*, 5(1), 223.
- Raza, A., Alavi, A. B., Memon, Y., & Memon, M. (2023). Tik-Tok Usage During Third Wave of COVID-19 and Its Impacts on Personal, Academic, and Social Life of Teenagers and Youngsters in Turkey. *Management*, 11(1), 31-43.
- Raza, A., & Tursoy, T. (2025). Modelo de aceptación de la tecnología y Fintech: una evidencia de la industria bancaria italiana. *Revista Mexicana de Economía y Finanzas Nueva Época REMEF*, 20(1), 993.
- Rodríguez del Águila, M., & Benítez-Parejo, N. (2011). Simple linear and multivariate regression models. *Allergologia et Immunopathologia*, 39(3), 159-173. <https://doi.org/10.1016/j.aller.2011.02.001>
- Raddatz, N., Coyne, J., Menard, P., & Crossler, R. E. (2023). Becoming a blockchain user: understanding consumers' benefits realisation to use blockchain-based applications. *European Journal of Information Systems*, 32(2), 287-314.
- Sykes, A. O. (1993). An introduction to regression analysis.
- Slatvinska, V. M., Demchenko, V., Tretiak, K., Hnatyuk, R., & Yarema, O. (2022). The impact of blockchain technology on international trade and financial business.
- Shin, D. D. (2019). Blockchain: The emerging technology of digital trust. *Telematics and Informatics*, 45, 101278. <https://doi.org/10.1016/j.tele.2019.101278>
- Shih, S. C., & Chiu, B. H. (2023). Willingness of Farmers to Adopt Blockchain Technology in Smart Agriculture. *Journal of Economics, Finance and Accounting Studies*, 5(4), 24-34.
- Series, O. B. P. (2020). The tokenisation of assets and potential implications for financial markets. *The Secretary General of the OECD*.



Vol. 3 No. 1 (January) (2025)

- Tripoli, M., & Schmidhuber, J. (2018). Emerging Opportunities for the Application of Blockchain in the Agri-food Industry.
- Tabachnick, B. G., & Fidell, L. S. (2007). *Using Multivariate Statistics*. Boston, MA: Pearson Education.
- Tapscott, D., & Tapscott, A. (2016). *Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world*. Penguin.
- Tyagi, A. K., Aswathy, S. U., & Abraham, A. (2020). Integrating blockchain technology and artificial intelligence: Synergies perspectives challenges and research directions. *Journal of Information Assurance and Security*, 15(5), 1554.
- Trautman, L. J. (2018). Bitcoin, virtual currencies, and the struggle of law and regulation to keep peace. *Marq. L. Rev.*, 102, 447.
- Ullah, N., Al-Rahmi, W. M., Alfarraj, O., Alalwan, N., Alzahrani, A. I., Ramayah, T., & Kumar, V. (2022). Hybridizing cost saving with trust for blockchain technology adoption by financial institutions. *Telematics and Informatics Reports*, 6, 100008. <https://doi.org/10.1016/j.teler.2022.100008>
- Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2019). Blockchain technology overview. *arXiv preprint arXiv:1906.11078*.
- Yoon, J., Talluri, S., Yildiz, H., & Sheu, C. (2020). The value of Blockchain technology implementation in international trades under demand volatility risk. *International Journal of Production Research*, 58(7), 2163-2183.