Electronic Journal of Business and Management
ICDBSE Special Issue, 2024 pp. 1-19
e-ISSN:2550-1380-ISSN

Effectiveness of Blockchain Technology in Preventing Financial Fraud: A Study Among Public Listed Companies in Malaysia.

Anusha Ramesh
Asia Pacific University of Technology and Innovation

Meera Eeswaran
Asia Pacific University of Technology and Innovation
meera_ees@apu.edu.my

Faros Faizdnor Roslan
Asia Pacific University of Technology and Innovation

Dhamayanthi Arumugam
Asia Pacific University of Technology and Innovation

Abstract

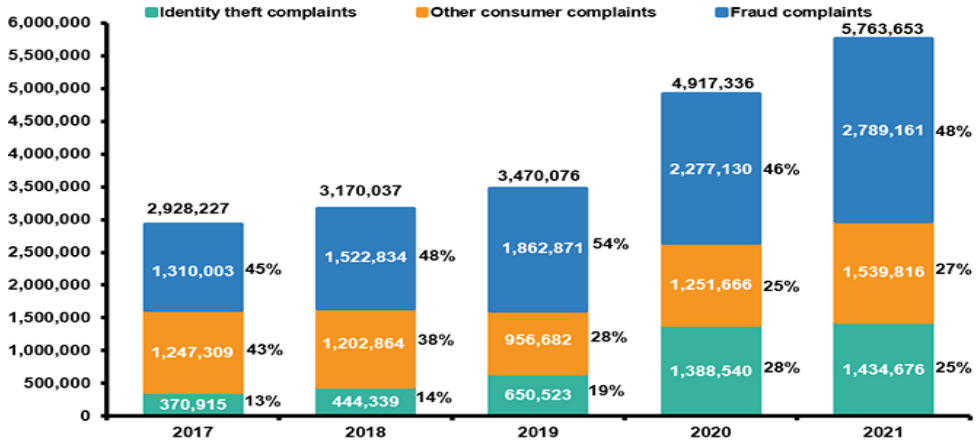
The main goal of this research is to examine how well blockchain technology functions to prevent financial fraud. The purpose of this study is to determine whether blockchain technology can effectively combat financial fraud, a type of white-collar crime that is dramatically increasing throughout the world. With this concern, this project aimed to identify the effectiveness of blockchain technology in preventing financial fraud among public listed companies in Malaysia. Since there are only a few studies have analysed various factors that influence financial fraud, this study intends to achieve the aim of the study which is to figure out the level of influence that the factors identified as independent variables on the dependent variable, financial fraud. The primary method is used by the researcher to acquire the data. The three factors examined in this study—immutability, consensus method, and distributed ledger technology—all have a major impact on financial fraud. The data was acquired from staff of public listed companies in Malaysia. Statistical Package of the Social Sciences (SPSS) is used to analyze the correlations between the three factors and all of the factors were shown to have a substantial link with financial fraud in Malaysian public listed companies. This study's findings suggest that individuals and businesses should be aware of the threats of financial theft that exist all around them and the value of having key tools that are resistant to phishing scams. The investigation raises awareness of the application of blockchain technology among customers as well as companies to prevent financial fraud.

Key Words: *Financial Fraud, Immutability, Consensus Algorithm, Distributed Ledger Technology.*

1.0 Introduction

Financial fraud is defined widely as a purposeful act of dishonesty involving financial transactions for financial benefit. 'White-collar criminals,' such as business experts with specialized skills and criminal intent, are often involved in complicated financial fraud. Financial fraud can occur in a variety of settings, including businesses, financial institutions, and government organizations. It can cause significant financial losses to individuals and businesses, and can also have broader economic consequences such as reduced investor confidence and market disruption (Chen, 2022). In addition to that, there is evidence of an increase in identity theft and fraud reports in the United States between 2017 and 2021. Exhibit 1.1 shows an excerpt from the statistics.

Exhibit 1.1: Extract of Index Score of Identify Theft, by Country, in United States



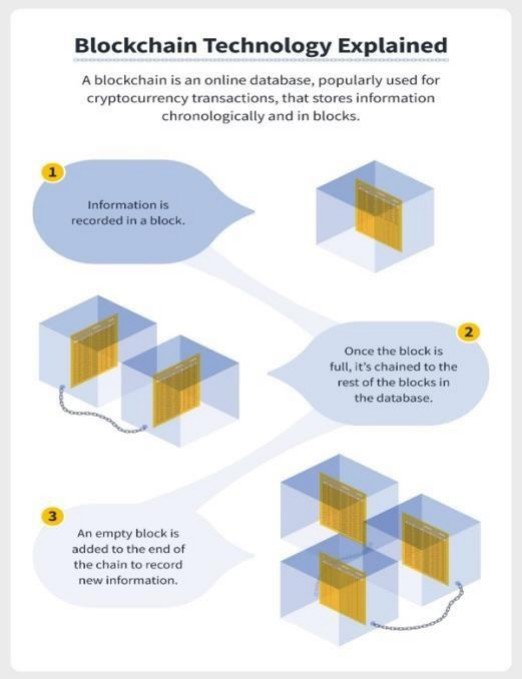
Source: (THE INSTITUTES, 2022)

Financial fraud impacts companies and economies. Fraud costs more than money. Fraud costs businesses millions. According to the government, fraud hinders services and aims. Needy people lose money and receive unsafe services. Fraud undermines national security. (Commonwealth of Australia, n.d.). The Fraud Act 2006 criminalizes financial fraud. Under the Fraud Act 2006, offenders face up to 10 years in prison, while financial fraud suspects riskup to 14 years (David & Phillips, 2015).

Further, according to the World Economic Forum in 2018, financial institutions spend morethan $8.2 billion on online crime and fraud, making them a trillion-dollar industry. Numerousfactors, including the degree of vulnerability against these crimes that are inherent inautomation and digitization, higher volume of transactions, and integration within countriesand internationally on the use of financial systems, create opportunities for such crimes to occur(Ngo-Lam, 2019). Fraud and attacks are attracting more attention than ever in the majority of financial institutions. With the development of digitization and the automation of financialinstitutions, crimes have risen more than ever due to extremely sophisticated technologies.

Correspondingly, in Malaysia, about 10,722 frauds occurred in 2020, representing a 23 percent increase over 2018. The majority of online fraud fell under the category of financial crime, such as funding loans. To take up arms this, Deputy Prime Minister Datuk Seri Wan Azizah decided to develop a project dubbed the Cyber Security Modular Professional, which is like Industry 4.0 (Bernama Malaysia, 2022).

Exhibit 1.2: Illustration of How Blockchain Works



As a matter of course, blockchain, a revolutionary database technology, is crucial for a corporation's long-term viability and problem-solving capabilities. It can help manage Bitcoin's volatility and complexity. Blockchain's features like distributed copies, verifiability, transparency, anonymity, and authentication make it ideal. It consists of interconnected blocksthat store unchangeable transaction data, offering security against hacking (Xu, Chen, & Kou,2019). Satoshi Nakamoto introduced the concept in 2008, leading to the development of blockchain and Bitcoin. Various industries, including supply chain management, tourism, healthcare, and e-commerce, have successfully adopted blockchain (Bayramova, J.Edwards, & Roberts, 2021). Blockchain is an uneditable digital information system that forms the basis of immutable ledgers. It's a type of distributed ledger technology (DLT) that decentralizes security and trust (Hayes, 2022). It ensures fraud-free transactions with digital signatures that can't be falsified or altered. Unlike traditional systems relying on regulatory bodies, blockchain relies on user consensus for smoother, safer, and faster transactions.

Before blockchain gained widespread attention, distributed ledger technology (DLT) was developed to create decentralized and secure transaction recording and verification systems. DLT distributes a database across a network of computers instead of storing it centrally. Eachnetwork node holds a copy of the ledger, and consensus among nodes is required to validate transactions, ensuring a tamper-resistant system for securely storing and transferring digital assets (BlockstreetHQ Team, 2018).

Blockchain, a subset of DLT, uses cryptography to secure ledger transactions. Transactions are grouped into blocks, and each block is linked to the previous one, forming a chain of blocks. This creates an immutable transaction record distributed across the network, preventingmanipulation by any single party (BlockstreetHQ Team, 2018). Ripple is an example of a DLTsystem that facilitates cross-border payments between financial institutions. In Ripple, the sender initiates a payment by creating a ledger entry, which is validated by a network of Ripplenodes before updating the ledger with the new account balances for both parties (BOTSPedia,2022).

CIMB Group of Malaysia, a major financial institution in the ASEAN region, has partnered with Ripple, a global payments technology company. Ripple's technology, particularly xCurrent and xRapid products, is gaining popularity for its ability to facilitate almost instant international money transfers through RippleNet (Raza, 2021). Ripple utilizes XRP as a "bridgecurrency" to enable fast, cost-effective transactions between different currencies and paymentsystems. It employs the Ripple Protocol Consensus Algorithm (RPCA) for transaction verification, allowing real-time execution and making it one of the fastest blockchain networks.Ripple eliminates intermediaries, reducing the cost of international money transfers.

CIMB plans to incorporate Ripple technology, specifically xCurrent, into its SpeedSend platform, expanding Ripple's presence in Malaysia (FRANKENFIELD, 2022). Traditional financial institutions are increasingly interested in blockchain technology due to its efficiency and cost-effectiveness. CIMB, with its vast network of 800 locations across 15 countries in the ASEANregion, will further strengthen its position by adopting Ripple's blockchain (Raza, 2021). CIMBhas also developed Trade Connect, a blockchain-based platform for trade finance, enabling digital document management, smart contracts, and automated trade finance processes. The bank plans to invest around RM1.2 billion (approximately US$263.65 million) in 2022 to enhance its digital transformation and technological infrastructure (Banking Frontiers, 2023).

2.0 Literature Review

This chapter assesses the previous research and works of literature on factors influencing financial fraud. It will cover the perception of financial fraud and its determinants, immutability, consensus algorithm, and distributed ledger technology. This section will applya diversity of existing reliable journals to evaluate both dependent and independent variables and the literature gaps will be identified to give a direction to this thesis. Besides, theories arealso discussed in this chapter.

2.1 Financial Fraud

In a study by (Hashim & Salleh, 2020), the focus was on fraud risk and its drivers in state- controlled firms. The research utilized case studies from four such enterprises and employed the fraud triangle hypothesis. Interviews with top executives revealed a significant increase infraud cases due to inadequate internal controls and a lack of fraud detection skills. The report emphasized the risk of fraud in state-controlled firms involving suppliers, governments, customers, and shareholders, driven by opportunities, incentives, and rationalizations. It stressed the importance of establishing robust internal controls and fraud detection mechanisms to reduce fraud likelihood. (Akomea-Frimpong & Andoh, 2020) examined fraud cases, factors, and control methods in Ghanaian pharmacies, surveying 412 industry stakeholders.

Results identified various fraud cases, including pharmaceutical thefts, cash fraud, forged checks, andquestionable accounting practices. The study recommended the use of products, fraud policies, software, and internal procedures to mitigate these issues. (Repousis & LOIS, 2019) investigated fraud risks and schemes in Greek companies through questionnaires distributed tobranch staff in five firms. Their research highlighted forgeries, bribery, and money launderingas common fraud risks, with inactive accounts and check usage as prevalent schemes. The study emphasized the importance of all financial institution employees being aware of these threats. (Strelcenia & Prakoonwit, 2023) discussed the link between technology and the rise infinancial fraud, emphasizing how online transactions facilitated cybercriminal activities.

They underscored the necessity for robust security systems to protect financial data in online transactions. (Katterbauer & Syed, 2022) examined the impact of financial fraud on the banking industry, focusing on ransomware's negative effects and proposing a multidisciplinary approach involving intelligence, law enforcement, and third-party organizations. They emphasized crime-mitigating techniques, such as enhancing security measures and information sharing, to combat financial fraud. The study underscored the importance of strong security measures and information dissemination for preventing financial fraud and safeguarding financial transactions' integrity.

2.2 Immutability

In (Friis, 2017) study, the potential of blockchain technology in combating financial fraud is explored. Blockchain's key feature, its immutable transaction log, is highlighted as a powerfultool for tracing and preventing fraud. When transactions are recorded in a blockchain, they become permanent and unalterable, enabling swift detection and investigation of fraudulent activities. Blockchain's decentralized nature, which involves multiple parties in transaction verification and validation, enhances security and transparency while reducing the risk of a single point of failure. This attribute further minimizes the possibility of fraud and data corruption. (Patil & Kadam, 2021) study focuses on blockchain's role in protecting forensic evidence, particularly in cases of financial fraud in the healthcare industry. They emphasize that blockchain's cryptographic hashing and immutability make it an ideal technology for securing and maintaining the integrity of digital forensic evidence.

The use of Ethereum, a blockchain platform, enhances traceability and transparency in the chain of custody for digital data. Once evidence is recorded on the blockchain, it cannot be altered or removed, ensuring consistent and tamper-proof information accessible to all stakeholders. This promotes transparency and trust, especially for victims of financial fraud and identity theft. (Haque & Rahman, 2020) survey delves into the security challenges and benefits of blockchain in addressing financial fraud. They highlight the immutability of blockchain as a crucial aspect, which prevents unauthorized alterations and provides accurate information, particularly in tax-related disputes. Blockchain's decentralized nature and cryptographic hashing make it difficultto tamper with data, ensuring the accuracy of tax claims and reducing tax-related fraud.

In conclusion, these studies collectively underscore the potential of blockchain technology, with its immutable ledger and decentralized structure, in combating financial fraud and safeguardingdigital forensic evidence. Blockchain's transparency, integrity, and security features make it a promising tool for enhancing fraud prevention and detection in various sectors, ultimately benefiting both organizations and individuals in their pursuit of financial security and justice.

> H_{A1}: There is a relationship between immutability and financial fraud among public listed companies in Malaysia.

2.3 Consensus Algorithm

Litke & Anagnostopoulos (2019) argue that the implementation of blockchain technology in supply chains is highly beneficial. By creating a chain of nodes that tracks products from production to consumption, blockchain increases transparency and trust among stakeholders. Including trusted third parties in the blockchain's custody chain can facilitate rapid digital transactions, improving efficiency. The partnership between Walmart and IBM serves as a case study of blockchain's application in the supply chain. Walmart developed a blockchain- based system to trace the distribution of leafy greens, enhancing food safety. This technologyenabled real-time monitoring of product movement from farm to store, ensuring proper handling and compliance with quality standards. It also facilitated the rapid identification andremoval of contaminated products, reducing the risk of disease outbreaks.

Blockchain's consensus algorithms ensure that all network nodes share the same transaction information, enhancing security and preventing financial fraud, failures, and errors. (NICHOLLS & KUPPA, 2021) suggest that algorithms are effective in preventing financial fraud. Their studyfound that Support Vector Machines (SVMs) were used in only about 23% of financial fraud prevention cases, while algorithms were used in the remaining 77%. Consensus algorithms play a crucial role in maintaining blockchain integrity and preventing fraudulent financial activities. By storing and verifying credit card transactions on the blockchain, fraudulent transactions can be quickly detected and prevented. For instance, unusual card activity, like transactions from foreign countries when the cardholder has never made such purchases before, can be flagged and prevented through algorithms. The consensus algorithm ensures the legitimacy of transactions on the blockchain, making it harder to commit financial fraud through system manipulation.

Al-Khater (2020) explores various forms of financial fraudand their impact on individuals' privacy and security. The author proposes blockchain technology, with its unique algorithms, as a solution to this issue. Algorithms are particularly effective in industries that handle numerous transactions daily, such as banking. They can analyze transaction data to detect and prevent fraudulent behavior, improving the security of financial transactions. Data analytics tools using algorithms have been shown to significantly reduce fraud losses in businesses. Algorithms can also check the timing of data input to prevent manipulation. Overall, algorithms are highlighted as a valuable tool in preventing and detecting financial fraud, enhancing the security and integrity of financial transactions.

> H_{A2}: There is a relationship between consensus algorithm and financial fraud among public listed companies in Malaysia.

2.4 Distributed Ledger Technology

Roszkowska (2021) conducted a study that focused on the foundations of financial scandals, using case studies of Enron and Arthur Andersen as examples. The research suggests that blockchain technology can offer solutions to various financial fraud and audit issues, enhancethe accuracy of financial statements, and transform overall business operations. (Car &Campara, 2020) examined the application of Distributed Ledger Technology (DLT) in the maritime industry. DLT was found to streamline the shipping process by collecting data on optimal discharge locations and eliminating the need for extensive paperwork. This environmentally friendly approach simplifies operations and ensures efficient data transmission among stakeholders. DLT also enhances security by controlling data access and preventing fraud and theft, particularly in the regulation of wastewater discharges.

Sirohi (2020) discussed the relevance of blockchain technology in the banking sector to combat financial fraud. Blockchain's distributed ledger technology enhances security by connecting transactions and data to all users and servers. The transparency of individual transactions and the inherent security features of blockchain contribute to a reduced crime rate in the financial sector. Many banking institutions are integrating blockchain technology into their operations, particularly in mobile banking and multi-currency cards, to enhance security. Tarr (2018) proposed a study focusing on the impact of distributed ledger technology in the insurance market. Insurance fraud, costing billions annually, can be mitigated through DLT's validation of consumers, policies, and transactions using statistical data. DLT minimizes delays and errorsby automating repetitive claims and identifying suspicious parties involved in fraudulent activities. It also ensures the integrity of policy records and transaction details, aiding in the detection of trends and patterns related to insurance fraud.

These studies collectively highlightthe potential of blockchain and Distributed Ledger Technology (DLT) in addressing various issues, including financial fraud prevention, supply chain efficiency, and environmental sustainability. Blockchain's transparency, security, and automation capabilities make it a valuable tool across multiple industries, offering innovative solutions to complex challenges.

> H_{A3}: There is a relationship between distributed ledger and financial fraud among public listed companies in Malaysia.

2.5 Underpinning Theory

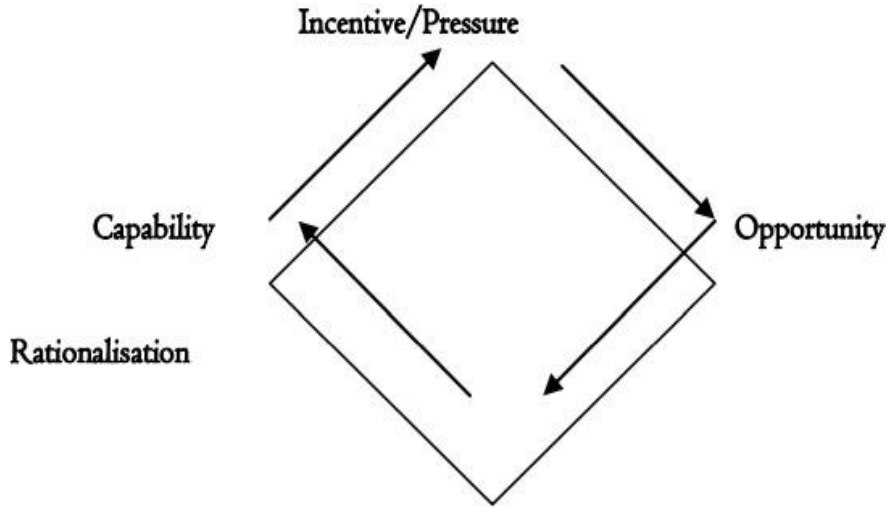
A large number of the world's leading organizations have met massive financial fraud activitiesthat have had a negative impact on a country's economy. It is critical to have a deeper grasp ofthe main motivations behind scams. This study examines a basic fraud theory known as frauddiamond theory from the inside out. It is critical to have a thorough understanding of the theoryin order to prevent fraud, particularly financial fraud among public listed companies (Mansor & Abdullahi, 2017).

2.5.1Fraud Diamond Theory

Fraud theory is a philosophy that explains why a company commits corporate fraud. The Fraud Diamond Theory is the theoretical framework that underpins this research (Christian & Basri,2019). Wolf and Hermanson proposed the idea to replace Cressy's Fraud Triangle Theory, andit is based on four assumptions about why corporations commit fraud. Pressure, opportunity, rationalization, and capability are all factors to consider (Abdulrahman, 2019). The first assumption, pressure, suggests that an individual has a need that cannot be conveyed to peoplewho, from a more focused perspective, would have likely supported the issue's resolution. It istypically associated with the home, the workplace, or the outside world, and it may be a monetary or non-monetary (Abdulrahman, 2019).

According to Mansor & Abdullahi (2017), a person's major motivation for committing fraud in an organization may be financial pressure.Approximately 95% of fraudulent acts have been committed due to the perpetrator's financial difficulties. Next, opportunity. An opportunity arose for a person to commit fraud, which violates the individual's position of financial trust inside his company. Fraud can be perpetratedin the workplace if there is insufficient management and oversight. The third assumption is thatthe fraudster justifies his fraudulent conduct by applauding himself (Abdulrahman, 2019).

EXHIBIT 2.1: FRAUD DIAMOND THEORY



Sources: (Abdulrahman, 2019)

Finally, capability. Capability signifies that the misrepresentation perpetrator has the necessary essential features, abilities, or positional power to carry out his deception. This concept improves the grasp of the aspects of falsification as most crimes and forgeries would not haveoccurred if the ideal individual with the precise skills to commit the fraud had not been identified (Abdulrahman, 2019).

2.6 Literature Gap

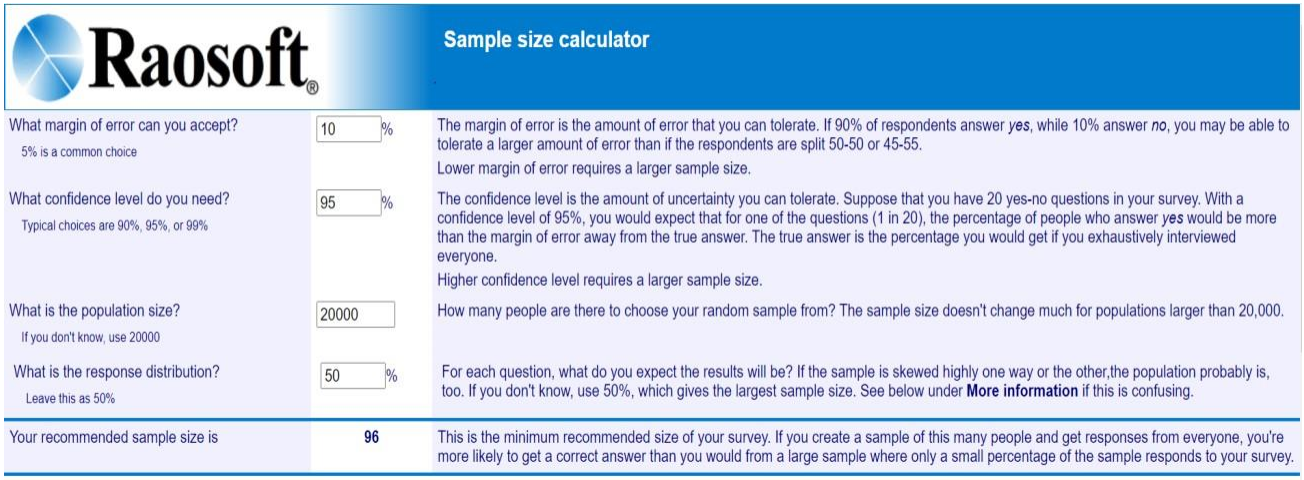
Even though various studies have been done and are being done on financial fraud, the scope of this research needs to be expanded on a regular basis based on secondary data collecting. This is mostly down to the fact that financial fraud is impacted by more than just the independent variables investigated in this study. As a result, the discussion of the independentfactors used for this study was limited, resulting in a literature gap that future researchers shouldaddress. Furthermore, there was a gap in the literature because the literature on financial fraudhas been determined to be limited throughout time. The research context, sample size, kind ofmethodology, and research methods used by previous researchers all differ across the literaturefound for this study, resulting in literature gaps. For example, according to previous studies, the use of quantitative and qualitative methodologies such as surveys and interviews, previousliterature, and blockchain fans varied. As a result, more research on the factors of financial fraud among Malaysia's listed companies is required.

3.0 Methodology

This research employs the positivism philosophy as the basic foundation for this study.The approach of this research is deductive. Using the deductive approach, the hypotheses and theory were developed. This study uses a survey strategy to obtain relevant data fromrespondents to test the hypotheses. Furthermore, this research implements the mono method which is a quantitative study as this research involves collecting and assessing numerical data.Cross-sectional research will be employed to gather primary data by constructing a self- administered questionnaire (SAQ).

The SAQ will be created via Google Forms and distributed through links and emails to the respondents. Lastly, data collection will be conducted among public listed companies staff and examples of public listed companies that are chosen in this study are Sunway Berhad, Affins Holding Berhad, Nestle Malaysia Berhad, Top Glove, and others. Based on the Roasoft sample size calculator, with a margin error of 10%, a confidencelevel of 95%, and a population size of 20,000, this study estimates 96 respondents to respond to the questionnaire. Relevant data analysis will be implemented by using various statistical techniques such as descriptive analysis, Cronbach Alpha, Pearson’s Correlation Coefficient andMultiple Regression Model to analyze the numerical data.

Exhibit 3.1: Raosoft Sample Size Calculator



Source: (Raosoft Inc, 2004)

4.0 Results, Findings and Discussions

The findings of the hypothesis test between the dependent and independent variables will be explained in great depth. Additionally, the Reliability Test, Pearson's Correlation Coefficient, and Multiple Linear Regression results will be analyzed below.

Table 1: Reliability Test

Variables	Number of Items	Likert Scale	Cronbach's Alpha
Dependent Variables:			
- *Financial Fraud*	6	1 - 5	0.745
Independent Variables:			
- *Distributed Ledger*	8	1 - 5	0.879
- *Immutability*	8	1 - 5	0.926
- *Consensus Algorithm*	8	1 - 5	0.943
Overall Cronbach's Alpha			0.962

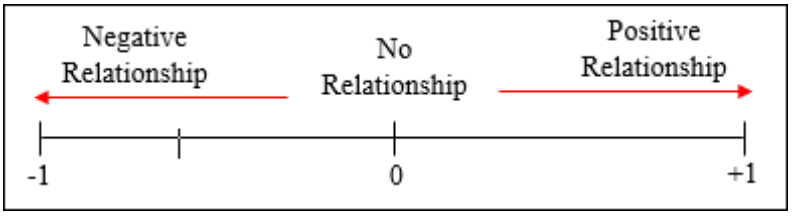
Source: Primary Data

Based on Table 1, depicts the Alpha's 0.962 output. Financial fraud is the dependent variable, and immutability, consensus algorithms, and distributed ledgers technology, are the independent variables, adding up to a total of 30 questions in the questionnaire, which is represented by the number N of items. Therefore, based on the findings, it can be deduced thatthe reliability score is greater than 0.9, demonstrating that the overall questionnaire is excellentfor use in the analysis of research evaluating the efficacy of blockchain technology inpreventing financial fraud.

4.1 Pearson's Correlation Coefficient

Pearson's Correlation Coefficient is used in the SPSS software for the hypothesis testing in Chapter 3. The correlation coefficients (r), according to Higgins (The Correlation Coefficient,2005), range from -1 to 1. A correlation coefficient of -1 indicates that there is a negative relationship between the two variables, which means that when one variable's value increases,the other variable's value decreases. When the correlation coefficient is 1, the two variables aresaid to be positively correlated, which means that when one variable rises, the other follows similarly. If the correlation coefficient is zero, there is absolutely no relationship at all betweenthe two variables. In this study, the importance of a 2-tailed correlation coefficient is evaluated.The p-value, or level of significance, must be less than or equal to 0.05 (p-value 0.05) in orderfor H_0 to be rejected and H_A to be approved. The p-value is used since there is no statisticalsignificance despite the high correlation.

Exhibit 4.1: Range of Correlation Coefficient



Source: Researcher Own Source

Table 2: Result of Correlation Between Dependent and Independent Variables

Correlations					
		Financial Fraud	Immutability	Consensus Algorithm	Distributed Ledger Technology
Financial Fraud	Pearson Correlation	1	.771**	.666**	.662**
	Sig. (2-tailed)		<.001	<.001	<.001
	N	130	130	130	130
Immutability	Pearson Correlation	.771**	1	.696**	.668**
	Sig. (2-tailed)	<.001		<.001	<.001
	N	130	130	130	130
Consensus Algorithm	Pearson Correlation	.666**	.696**	1	.863**
	Sig. (2-tailed)	<.001	<.001		<.001
	N	130	130	130	130
Distributed Ledger Technology	Pearson Correlation	.662**	.668**	.863**	1
	Sig. (2-tailed)	<.001	<.001	<.001	
	N	130	130	130	130

Source: Primary source

The outcomes for Pearson correlation had been proven, as shown in Table 2 above. Immutability (IV1) has shown the greatest relationship with financial fraud (DV) through observation, with a value of 0.771. While the positive sign of the correlation coefficient indicated that the variables were positively associated, the strength of the relationship betweenthese variables was regarded as being excellent. Immutability and financial fraud were significantly correlated, with a sig. value of 0.001 since the association is significant at the 0.01level.

Followed by the second strongest relationship discovered is between financial fraud (DV) andthe consensus algorithm (IV2), with a correlation coefficient of 0.666. The strength of the relationship was deemed to be strong, as indicated by a positive correlation coefficient. This coefficient demonstrated that the variables were positively and directly related. The correlationbetween the consensus algorithm (IV2) and financial fraud (DV) has been determined to be significant at the 0.01 level. This indicates that there is a significant relationship between thesetwo variables, as evidenced by the sig value of 0.001.

Finally, the third independent variable, distributed ledger technology (IV3), likewise shows a strong relationship with financial fraud (DV). The correlation coefficient resulted in a value of0.662, indicating that the significance of this relationship was equivalent to that of other independent variables. The positive sign of the correlation coefficient signifies these two variables are positively or directly related. The correlation between distributed ledger technology (IV3) and financial fraud (DV) has been demonstrated to be significant at the 0.01level. This significance is supported by the sig. value of 0.001, as shown in the table above.

4.2 Multiple Linear Regression

Based on Table 3, it is apparent that the R-value, also referred to as the coefficient correlation,is what serves to define the range between the dependent and independent variables in terms of a strong positive link (shown by +1) and a strong negative relationship (represented by -1).The research shows that there is a positive correlation between financial fraud and all of the other independent variables, with an R-value of 0.797. In addition, the value of R2 iscomparable to 0.636, which can also be converted into 63.6%, and this plays to estimate the model's ability to explain variations in the dependent variable through variations in the independent variables (Zach, 2022). By this, it can be concluded that immutability, consensusalgorithms, and distributed ledger technologies have a high association with financial fraud. The remaining 36.4% of financial fraud may be impacted by many factors.

Table 3: Model Summary[B] of Multiple Linear Regression

Model	R	R^2	Adjusted R^2	Standard Error of the Estimate	Change Statistics				
					R^2 Change	F Change	df1	df2	Significant F Change
1	.797[a]	.636	.627	.23235	.636	73.271	3	126	.001

a. Dependent Variable: Financial Fraud

b. Predictors: (Constant), Distributed Ledger Technology, Immutability, Consensus Algorithm

Table 4: Analysis of Variance (Anova[A])

ANOVA[a]						
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	11.867	3	3.956	73.271	<.001[b]
	Residual	6.802	126	.054		
	Total	18.669	129			

Source: Primary Data

a. Dependent Variable: Financial Fraud
b. Predictors: (Constant), Distributed Ledger Technology, Immutability, ConsensusAlgorithm

Analysis of Variance (ANOVA) is a statistical technique used to assess the significance of estimated results in research Field (Multiple Regression, 2008). It is particularly useful for comparing samples with numerically dependent variables (O'Donoghue, 2013). ANOVA calculates the Regression Sum of Squares, which represents the variability explained by the regression model, by subtracting the Residual Sum of Squares from the Total Sum of Squares Field (How to Read the Output From Simple Linear Regression Analyses, 2012). Degrees of freedom (df) in ANOVA are determined by subtracting 1 from the number of variables (df = n-1) (Statistic How To, 2018). The F ratio is employed to describe the differences between variables. In hypothesis testing, the p-value for ANOVA should be less than or equal to 0.05 to reject the null hypothesis, indicating a significant correlation between variables (Minitab Inc, 2016).

In Table 4, it's noted that there are 3 degrees of freedom (df = 4-1 = 3) for financial fraud, immutability, consensus algorithms, and distributed ledger technology. The residual degrees of freedom, accounting for the sample size, are 130, resulting in an overall degree of freedom of 129. This demonstrates that as the sample size increases, the degrees of freedom also increase. The F value is calculated by dividing the regression mean square by the residualmean square. It is used to assess how well the regression model fits the data. The table shows a significant p-value of 0.001. The equation F (3, 126) = 73.271, p (0.001) < 0.05 indicates thatthe regression model accurately fits the data, establishing a significant linear relationship between the dependent and independent variables. ANOVA is employed to determine the significance of results in research, with degrees of freedom and the F ratio playing critical roles. In the presented analysis, the model effectively fits the data, indicating a significant relationshipbetween variables, paving the way for hypothesis testing.

TABLE 5: RESULTS OF HYPOTHESIS TEST

H1	H_{01}	There is no relationship between immutability and the effectiveness of blockchain technology in preventing financial fraud.	**Rejected**
	H_{A1}	There is a relationship between immutability and the effectiveness of blockchain technology in preventing financial fraud.	**Accepted**
H2	H_{02}	There is no relationship between consensus algorithm and the effectiveness of blockchain technology in preventing financial fraud.	**Rejected**
	H_{A2}	There is a relationship between consensus algorithm and the effectiveness of blockchain technology in preventing financial fraud.	**Accepted**
H3	H_{03}	There is no relationship between distributed ledger technology and the effectiveness of blockchain technology in preventing financial fraud.	**Rejected**
	H_{A3}	There is a relationship between distributed ledger technology and the effectiveness of blockchain technology in preventing financial fraud.	**Accepted**

Source: Primary Source

According to Table 4.8, all the connections between the dependent variable and independent variables are valid and capable of influencing one another. Significant associations are the consequence of the strategies employed to test the hypothesis.

5.0 Conclusion, Limitations and Recommendations

Understanding financial fraud is crucial for individuals, companies, and industries. By puttingin place an effective system with strong firewalls and practical tools, financial fraud can be prevented. As blockchain technology advances, it becomes a potent and essential tool for reducing, avoiding, and safeguarding against financial fraud. Numerous studies have revealeda positive relationship between the factors influencing blockchain technology and financial fraud. Financial fraud can be made more publicly known by using blockchain technology, anduser and business data can be securely kept with strong tools to strengthen defenses against fraudsters. This study focuses on three aspects of blockchain technology to improve knowledgeamong organizations.

The study investigates the implications of financial fraud on several features of blockchain technology, including immutability, consensus algorithm and distributed ledger. The findings demonstrate that each of the three independent variables has a favourableand significant influence on financial fraud. It insists that financial fraud will increase in frequency as the benefits of blockchain technology increase. Notably, immutability has a significant relationship with financial fraud, but consumers and companies should take into account the other factors' major impacts as well.

5.1 Limitations

Few limitations can be addressed in this study to enhance future research. The first limitation of this study is the duration of the research. The research is being conducted in a short duration.This period restricts the researcher to gather adequate information and examining more detail on this study. Thus, an extended timeframe is ideal for a better research outcome. Furthermore, the researcher finds difficulties in finding relevant journals and previous research regarding theframework of this study. The lack of information in journals affects the researcher to conduct the study efficiently. Additionally, the constraint of time arrangement for journals is from 2015to 2021 to be chosen for the literature review. However, many old journals are relevant and fitto be used in this study.

5.2 Recommendations

Blockchain technology has gained widespread popularity in today's technologically advanced society, offering a digital alternative to traditional paper-based transaction processing. It enables users to securely preserve and exchange information, resulting in a 2.8% global increase in its adoption (Tuwiner, 2022). However, along with its benefits, blockchain technology presents significant drawbacks, notably its high energy consumption, which drivesup operational costs for many companies (Ghosh & Das, 2020). The energy-intensive nature of blockchain technology is primarily due to the proof-of-work algorithm used, which relies ontrial and error to determine hash values. For instance, Bitcoin miners create new blocks approximately every 10 minutes, which has improved efficiency but comes at a substantial energy cost (Ghosh & Das, 2020).

To address the energy consumption issue, analysts have proposed several solutions. One approach is the utilization of renewable energy sources, such as solar and wind power, to provide electricity for blockchain operations. Mongolia's use of coal power for blockchain technology serves as a cautionary example of the environmental impact of non-renewable energy sources. Companies like IBM and Intel are advocating for green blockchains that promote sustainability and decentralization of authority in power generation. This involves thecreation of microgrids, where excess power can be seamlessly transferred to those in need (Ghosh & Das, 2020).

Another solution is the implementation of the Lightning Network technology. Introduced by Thaddeus Dryja and Joseph Poon in 2015, this system allows transactions to be logged only after the channels between users are closed, significantly reducing energy consumption. Transactions are managed without the involvement of external parties, and data is no longer stored once a channel is closed, ensuring privacy and efficiency. This approach consumes lessenergy as fewer transactions require high energy levels (SHARMA, 2022).

Despite the initial appearance of high energy consumption in blockchain technology, it is essential to consider that its carbon emissions are lower than many everyday activities, such astraditional banking, which is predicted to consume 263.72 TWh of energy annually by 2021 (Galaxy Digital prediction). This perspective underscores the importance of exploring sustainable energy solutions and innovative technologies like the Lightning Network tomitigate the environmental impact of blockchain technology while harnessing its transformative potential (SHARMA, 2022).

References

1. Abdulrahman, S. (2019). Forensic Accounting and Fraud Prevention in Nigerian PublicSector: A Conceptual Paper. *International Journal of Accounting & Finance Review*, 13-21.
2. Akomea-Frimpong, I., & Andoh, C. (2020). Understanding and controlling financial fraud in the drug industry. *Journal of Financial Crime*, 337.
3. AL-KHATER, W. A. (2020). Comprehensive Review of Cybercrime Detection Techniques. *IEEE Access*.
4. Bayramova, A., J.Edwards, D., & Roberts, C. (2021). The Role of BlockchainTechnology in Augmenting SupplyChain Resilience to Cybercrime. 1-19.
5. Bernama Malaysia. (2022, February 28). *Ministry of Commuications and Multimedia Malaysia*. Retrieved from 2020: https://www.kkmm.gov.my/index.php/en/privacy-policy/233-kpkk-news/16471-bernama-11-feb-2020-gov-t-actively-addressing-cyber- threats-crimes-dpmhttps://www.kkmm.gov.my/index.php/en/privacy-policy/233-kpkk-news/16471-bernama-11-feb-2020-gov-t-actively-addres
6. Car, M., & Campara, L. (2020). Distributed Ledger Technology as a Tool for Environment Sustainability in the Shipping Industry. *Journal of Marine Science and Engineering*, 1-16.
7. Chen, J. (2022, July 24). *What Is Fraud?* Retrieved from Investopedia: https://www.investopedia.com/terms/f/fraud.asp
8. Christian, N., & Basri, Y. Z. (2019). ANALYSIS OF FRAUD PENTAGON TO DETECTING CORPORATE FRAUD IN INDONESIA. *International Journal of Economics, Business and Management Research*, 1-13.
9. Commonwealth of Australia. (n.d.). *The total impacts of fraud*. Retrieved from Commonwealth Fraud Prevention Centre: https://www.counterfraud.gov.au/total- impacts-fraud
10. Dallal, G. E. (2012). *How to Read the Output From Simple Linear Regression Analyses*.Retrieved February 15, 2018, from http://www.jerrydallal.com/lhsp/slrout.htm
11. David, & Phillips. (2015, May 16). *Implications of Financial Crime and Fraud*.Retrieved from DPP Law: https://www.dpp-law.com/services/corporate-financial- crime/financial-fraud/
12. Field, A. (2008). Multiple Regression. *Research Methods in Psychology*, 1-11.
13. Friis, G. (2017). A Blockchain-Based Approach Towards Overcoming Financial Fraudin Public Sector Services . *Business & Information Systems Engineering*, 442.
14. Gates, M. (2021, April 19). *The Global Fraud Landscape*. Retrieved from https://www.asisonline.org/security-management-magazine/articles/2021/05/the- global-fraud-landscape/
15. Ghosh, E., & Das, B. (2020). A study on the issue of blockchain's energy consumption.1-15.

16. Haque, A. B., & Rahman, M. (2020). Blockchain Technology: Methodology, Application and Security Issues. *International Journal of Computer Science andNetwork Security*, 21-22.
17. Hashim, H. A., & Salleh, Z. (2020). The risk of financial fraud: a management perspective. *Journal of Financial Crime*, 1143 - 1144.
18. Hayes, A. (2022, May 16). *How Does a Blockchain Work?* Retrieved fromInvestopedia: https://www.investopedia.com/terms/b/blockchain.asp
19. Higgins, J. (2005). The Correlation Coefficient. In *The Radical Statistician* (p. 11). California: The Management Advantage, Inc.
20. Katterbauer, K., & Syed, H. (2022). Financial cybercrime in the Islamic Finance Metaverse. *Metaverse*, 56 - 59.
21. Litke, A., & Anagnostopoulos, D. (2019). Blockchains for Supply Chain Management: Architectural Elements and Challenges Towards a Global Scale Deployment. *Electrical and Computer Engineering*, 1-3.
22. Mansor, N., & Abdullahi, R. (2017). Fraud Triangle Theory and Fraud Diamond Theory. Understanding the Convergent and Divergent For Future Research. *nternational Journal of Academic Research in Accounting, Finance and Management Sciences*, 38–45.
23. Minitab Inc. (2016). *Interpret the key results for One-Way ANOVA*. Retrieved February15, 2018, from http://support.minitab.com/en-us/minitab-express/1/help-and-how- to/modeling-statistics/anova/how-to/one-way-anova/interpret-the-results/key-results/
24. Ngo-Lam, V. (2019, December 24). *Cyber Crime: Types, Examples, and What Your Business Can Do*. Retrieved from Exabeam: https://www.exabeam.com/information- security/cyber-crime/
25. NICHOLLS, J., & KUPPA, A. (2021). Financial Cybercrime: A Comprehensive Surveyof Deep Learning Approaches to Tackle the Evolving Financial Crime Landscape. *IEEEAccess*.
26. O'Donoghue, P. (2013). *Statistics for Sport and Exercise Studies: An Introduction.* NewYork: Routledge.
27. Patil, S., & Kadam, S. (2021). Security Enhancement of Forensic Evidences Using Blockchain. 263-264.
28. Raosoft Inc. (2004). *Raosoft sample size caolculator*. Retrieved May 22, 2021, from http://www.raosoft.com/samplesize.html
29. Repousis, S., & LOIS, P. (2019). An Investigation of the Fraud Risk and Fraud SchemeMethods in Greek commercial banks . *Journal of Money Laundering Control*, 1 - 2.
30. Roszkowska, P. (2021). Fintech in financial reporting and audit for fraud prevention and safeguarding equity investments. *Journal of Accounting & Organizational Change*,164-167.
31. SHARMA, R. (2022, June 26). *Bitcoin's Lightning Network: 3 Possible Problems*. Retrieved from Investopedia : https://www.investopedia.com/tech/bitcoin-lightning- network-problems/
32. Sirohi, A. (2020). Relevance of Blockchain Technology in The Scenario of Escalating Cybercrime in Banking Sector in the UK.
33. Statistic How To. (2018). *Degrees of Freedom: What are they?* Retrieved February 16,2018, from http://www.statisticshowto.com/degrees-of-freedom/
34. Strelcenia, E., & Prakoonwit, S. (2023). Improving Classification Performance inCredit Card Fraud Detection by Using New Data Augmentation. *AI*, 172 - 175.
35. Tarr, J.-A. (2018). Distributed ledger technology, blockchain and insurance:Opportunities, risks and challenges. *Insurance Law Journal*.

36. THE INSTITUTES. (2022, May 13). *Facts + Statistics: Identity theft and cybercrime*.Retrieved from Insurance Information Institute : https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime
37. Tuwiner, J. (2022, July 15). *79+ Blockchain Statistics, Facts, and Trends*. Retrieved from Buy Bitcoin Worldwide: https://www.buybitcoinworldwide.com/blockchain- statistics/
38. Xu, M., Chen, X., & Kou, G. (2019). A systematic review of blockchain. *Springer Open*, 1-14.
39. Zach. (2022, March 24). *How to Interpret Adjusted R-Squared (With Examples)*. Retrieved from Statology: https://www.statology.org/adjusted-r-squared-interpretation/

Authors Profile:

[A]Anusha Ramesh

Research Scholar, Asia Pacific University, Malaysia.

[B]Meera Eeswaran

Senior Lecturer, Asia Pacific University, Malaysia.

[C]Faros Faizdnor Roslan

Lecturer, Asia Pacific University, Malaysia

[D]Dr Dhamayanthi Arumugam

Senior Lecturer, Asia Pacific University, Malaysia

For instructions on how to order reprints of this article, please visit our website: https://ejbm.apu.edu.my/ ©Asia Pacific University of Technology and Innovation