ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25oct127

The Inter-Role of Cybersecurity, AI and Blockchain in Preventing Money Laundering and Terrorism Financing

Abayomi Oluwaseun Japinye[1*]

[1]Compliance Department, Central Bank of Nigeria, Lagos, Nigeria

Corresponding Author: Abayomi Oluwaseun Japinye[1*]

Publication Date: 2025/10/09

Abstract: This study investigates the integration of cybersecurity, artificial intelligence (AI), and blockchain technologies in mitigating money laundering and terrorism financing risks. An online survey was conducted via Google Forms, targeting 400 LinkedIn users with certifications or job roles in cybersecurity, compliance, anti-money laundering (AML), or counter-terrorist financing (CTF). Convenience sampling was employed to select participants, striking a balance between statistical power and practicality, with a sample size sufficient to capture diverse perspectives within the target population. The survey assessed integration levels and perceived effectiveness of cybersecurity, AI, and blockchain technologies, using a multiple-choice Likert scale to ensure uniform responses. Pearson's correlation coefficient was used to assess relationships between integration levels and perceived effectiveness for each technology. Multivariate regression analysis explored interactions between these technologies and their impact on integration levels. The Pearson correlation analysis showed weak but statistically significant relationships between integration levels and perceived effectiveness for cybersecurity (-0.068), AI (0.032), and blockchain (0.041). Regression analysis indicated that perceived effectiveness of cybersecurity and blockchain significantly predicts integration levels, while AI does not. This study highlights the complexities and stakeholder expectations involved in integrating these technologies, suggesting areas for improvement and future research to enhance their effectiveness in combating financial crimes. Ethical considerations, including informed consent and anonymity, were strictly adhered to throughout the research process.

Keywords: *Cybersecurity, Artificial Intelligence, Blockchain, Integration, Perceived Effectiveness, Money Laundering, Terrorism Financing.*

How to Cite: Abayomi Oluwaseun Japinye (2025) The Inter-Role of Cybersecurity, AI and Blockchain in Preventing Money Laundering and Terrorism Financing. *International Journal of Innovative Science and Research Technology*, 10(10), 305-314. https://doi.org/10.38124/ijisrt/25oct127

I. INTRODUCTION

The convergence of finance and technology has led to the emergence of blockchain technology as a significant development. Initially conceived as the backbone for cryptocurrencies, blockchain has since evolved into a versatile tool with wide-ranging implications, especially in the field of anti-money laundering and countering the financing of terrorism (Maboe, 2018). The pressing need for effective anti-money laundering (AML) and countering the financing of terrorism (CFT) measures has been emphasised by the increasingly sophisticated methods employed by illicit actors to launder money and fund terrorist activities. Traditional approaches to combating these threats have often fallen short in the face of rapidly evolving financial ecosystems (Akartuna et al, 2022).

Blockchain technology offers a promising avenue for bolstering these efforts through its intrinsic features of transparency, immutability, and decentralisation (Kalam & Mssassi, 2024). This inherent transparency holds the potential to revolutionise the way financial activities are monitored and regulated, providing regulators and law enforcement agencies with unprecedented visibility into the flow of funds. However, while the incorporation of blockchain technology into anti-money laundering (AML) and countering the financing of terrorism (CFT) efforts offers significant advantages, it is not devoid of challenges (Schwarz et al., 2021). Through a comprehensive examination of foundational concepts, current challenges, technological limitations, case studies, and future trends, this research offers valuable insights into the opportunities and challenges associated with the integration of blockchain technology into AML/CFT efforts.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25oct127

The study aims to explore the effectiveness of integrating cybersecurity measures, artificial intelligence (AI), and blockchain technology to mitigate the risks of money laundering and terrorism financing. The first objective of the study is to assess the relationship between the integration level of cybersecurity measures and their perceived effectiveness in reducing the risks associated with money laundering and terrorism financing. The second objective focuses on the integration of artificial intelligence. The study aims to determine the relationship between the level at which AI is integrated into financial systems and its perceived effectiveness in preventing money laundering and terrorism financing. The third objective examines the correlation between the integration level of blockchain technology and its perceived effectiveness in mitigating money laundering and terrorism financing risks. Finally, the fourth objective explores the interaction between the effectiveness of cybersecurity, AI, and blockchain technologies and their integration levels.

II. LITERATURE REVIEW

The conceptual framework provides a structured approach to understanding the relationship between blockchain technology and anti-money laundering (AML) as well as countering the financing of terrorism (CFT) strategies. The components of this framework are discussed below.

- *Foundational Concepts of Blockchain Technology*

The foundational concepts of blockchain technology represent the bedrock upon which its transformative potential is built. Understanding these concepts is crucial for grasping the intricacies of blockchain's applications in various domains, including its role in enhancing anti-money laundering (AML) and countering the financing of terrorism (CFT) efforts. At its core, blockchain is a decentralised and distributed ledger technology that enables the secure recording and verification of transactions across a network of nodes (Schwarz et al., 2021). The decentralised nature of blockchain means that it operates without a central authority, as no single entity has control over the entire system, preventing a single point of failure (Drescher, 2017). This decentralisation imbues blockchain with resilience against tampering, censorship, and unauthorised alterations, thereby fostering trust among network participants.

However, despite its revolutionary potential, blockchain technology is not without its challenges and limitations. Scalability remains a significant concern, as the processing capacity of blockchain networks may be insufficient to handle the volume of transactions required for widespread adoption (Toufaily et al., 2021). Additionally, interoperability issues and regulatory uncertainties pose obstacles to the seamless integration of blockchain into existing financial systems (Upadhyay, 2020). Addressing scalability, interoperability, and regulatory challenges, therefore, will be crucial in realising the full benefits of blockchain technology in the fight against financial crime and terrorism financing.

- *Blockchain Solutions in AML and CFT*

One of the primary advantages of blockchain technology in AML/CFT lies in its ability to create an immutable and transparent ledger of transactions (Antunes & Cabral, 2019). Blockchain can record every transaction in a decentralised and distributed ledger, thereby enabling real-time visibility into the flow of funds and facilitating the detection of suspicious activities and the tracing of illicit funds back to their source. The transparency inherent in blockchain also enhances auditability and accountability, as every transaction is verifiable by all participants in the network, reducing the risk of fraud and manipulation.

In addition, blockchain solutions offer novel approaches to identity verification and authentication, addressing key challenges in AML/CFT compliance. Through the use of cryptographic techniques and digital signatures and Know Your Customer (KYC) requirements, blockchain-based identity management systems can securely store and verify customer identities, reducing the risk of identity theft, impersonation, and fraudulent transactions (Yang & Chan, 2021). Smart contracts, which offer automated and programmable solutions to enforce compliance rules and monitor suspicious activities, are another innovative application of blockchain technology in AML/CFT (Antunes & Cabral, 2019). Smart contracts can be programmed to execute predefined actions based on predefined triggers or conditions, such as flagging transactions above a certain threshold or blocking transactions involving sanctioned entities (Sharif, 2023).

- *Current Challenges in AML and CFT Efforts*

The current landscape of anti-money laundering (AML) and countering the financing of terrorism (CFT) efforts presents several challenges that impede effective detection, prevention, and mitigation of illicit financial activities. One of the foremost challenges facing AML/CFT efforts is the globalised nature of financial markets. This poses significant challenges to AML/CFT efforts, as illicit funds can easily traverse international borders through complex networks of shell companies, offshore accounts, and illicit financial intermediaries. Another significant challenge is the increasing sophistication of money laundering techniques employed by transnational criminal organisations, terrorist groups, and individuals (Rose-Ackerman & Palifka, 2018). These actors exploit emerging technologies, such as encryption, anonymisation services, and decentralised platforms, to obfuscate their illicit activities and evade detection by authorities (Sartori et al., 2023). The convergence of cybercrime and financial crime poses novel challenges, as cybercriminals leverage hacking, ransomware, and money muling schemes to launder illicit proceeds and fund terrorist activities (Gundur et al., 2021).

However, by leveraging advanced analytics, artificial intelligence, blockchain technology, and international cooperation mechanisms, stakeholders can enhance the effectiveness, efficiency, and resilience of AML/CFT frameworks and mitigate the risks posed by illicit financial activities on a global scale (Pavlidis, 2023). It is worth noting that addressing regulatory, technological, and operational

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25oct127

challenges will require concerted efforts and sustained commitment from policymakers, regulators, financial institutions, and law enforcement agencies to safeguard the integrity of the global financial system and protect against threats to security and stability.

- *Future Trends and Implications*

Exploring future trends and implications in the integration of blockchain technology into anti-money laundering (AML) and countering the financing of terrorism (CFT) efforts reveals both exciting possibilities and critical considerations for stakeholders in the financial industry and regulatory bodies alike. For instance, the reliance on blockchain technology for regulatory technology (RegTech) solutions introduces challenges related to data privacy, security, and regulatory compliance (Li, Maiti and Fei, 2023). RegTech solutions leverage blockchain for automating compliance processes, enhancing transparency, and streamlining regulatory reporting, thereby reducing the administrative burden on financial institutions and improving regulatory oversight (Yıldırım, 2023). Furthermore, the emergence of decentralised finance (DeFi) and non-fungible tokens (NFTs) presents both opportunities and challenges for AML/CFT efforts. DeFi platforms, which leverage blockchain technology to enable peer-to-peer lending, trading, and other financial activities without intermediaries, offer new avenues for financial inclusion but also pose risks of money laundering and terrorist financing due to their decentralised and pseudonymous nature. Similarly, NFTs, which represent unique digital assets on the blockchain, have been associated with AML/CFT concerns, particularly in the context of their use in online marketplaces for illicit goods and services (Granadeiro, 2023).

While these future trends hold promise for advancing AML/CFT efforts, they also raise critical considerations and potential risks that must be addressed. For example, according to Cheng et al. (2021), the proliferation of privacy-enhancing technologies, such as zero-knowledge proofs and confidential transactions, may enable illicit actors to obscure their activities and evade detection by authorities. Regulators and industry stakeholders, therefore, must stay abreast of these developments and adapt their AML/CFT strategies accordingly to address the evolving risks posed by DeFi and NFTs.

III. METHODOLOGY

To achieve the objectives of this study, we employed an online survey hosted on Google Forms, which allowed for the anonymous collection of quantitative data from 400 participants. These participants were selected based on their LinkedIn profiles, specifically targeting those with certifications or job roles related to cybersecurity, compliance, anti-money laundering (AML), or counter-terrorist financing (CTF). We adopted a positivist research philosophy, which emphasises objective data collection and analysis, aligning well with our focus on measurable outcomes (Saunders et al., 2019). Although we considered interpretivism, which focuses on understanding subjective meanings, it was less suitable for our strictly quantitative approach. Pragmatism, which combines both positivist and interpretivist methods, was also deemed inappropriate as it does not align closely with our emphasis on quantitative data.

The survey-based approach was chosen for its efficiency in reaching a large number of participants and collecting quantitative data (Coffey & Elliott, 2023). While qualitative research could provide deeper insights into subjective experiences, it was not appropriate for our focus on quantitative data. Furthermore, convenience sampling was used to identify participants on LinkedIn with relevant certifications or job roles. Despite the potential for bias, we minimised it through careful selection criteria (Rueda et al., 2022). We determined a sample size of 400 participants to balance statistical power and practicality. This sample size was deemed sufficient to capture a diverse range of perspectives and experiences within the target population, ensuring the reliability and generalizability of our findings (Memon et al., 2020). Our comprehensive questionnaire covered various aspects of the integration of cybersecurity, AI, and blockchain technologies in preventing money laundering and terrorism financing. The questions were clear and concise, with multiple-choice Likert scale answers to ensure uniformity in responses. The questionnaire began with demographic information, including age, gender, education level, and employment status, to provide context and allow for analysis based on different demographic variables.

For the first objective, we assessed the relationship between the integration level of cybersecurity measures and their perceived effectiveness in mitigating money laundering and terrorism financing risks. We used Pearson's correlation coefficient to measure the strength and direction of this relationship. The second objective involved assessing the relationship between the integration level of AI and its perceived effectiveness in addressing these risks. Again, Pearson's correlation coefficient was used for analysis. For the third objective, we examined the relationship between the integration level of blockchain technology and its perceived effectiveness in preventing money laundering and terrorism financing, using the same correlation analysis method. The fourth objective examined the interaction between the effectiveness of cybersecurity measures, AI, and blockchain technologies, as well as their impact on the integration levels in preventing money laundering and terrorism financing. We used multivariate regression analysis, such as multiple linear regression or MANOVA, to analyse the relationships between these variables.

Ethical considerations were paramount throughout the research process. Informed consent was obtained from all participants, who were informed about the study's purpose, their rights, and the confidentiality measures in place to protect their data. Participants were assured of their anonymity, and no personally identifiable data was collected. Participation was voluntary, and participants could withdraw at any time. Several limitations are hereby acknowledged, including potential sampling bias and self-reporting bias, which are common in survey-related studies. Efforts were made to mitigate these biases through careful selection criteria and questionnaire design.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25oct127

IV. RESULTS

A. *Descriptive Statistics*

Table 1 presents the demographic information of the participants for this study.

Table 1 Participants' Socio-Demographic Characteristics

Socio-Demographic Characteristics	Frequency	Percentage
Age **Mean (S/D)**	39.23 (8.828)	
Gender		
Male	276	69.0
Female	124	31.0
Educational Qualification		
Bachelor's Degree	226	56.5
Master's Degree	140	35.0
Ph. D.	28	7.0
Others	6	1.5
Employment Status		
Employed	264	66.0
Unemployed	72	18.0
Student	56	14.0
Others	8	2.0

The demographic characteristics of the study participants provide a robust foundation for the research. The mature age profile, high educational qualifications, and significant employment in relevant sectors suggest that the data collected will be rich in practical insights and technical expertise. This demographic makeup is to enhance the validity and reliability of the findings, as the participants are well-equipped to provide informed opinions on the integration and effectiveness of cybersecurity measures, AI, and blockchain technologies. However, the gender imbalance is a factor that must be acknowledged, as it could introduce a bias in the perspectives shared. Future research could aim for a more balanced gender representation to ensure diverse viewpoints are considered. In addition, while the sample includes unemployed individuals and students, their perspectives can provide valuable contrast and highlight different stages of engagement with the technologies in question.

Table 2 below provides a detailed statistical analysis of various items related to the integration levels and perceived effectiveness of cybersecurity, AI, and blockchain technologies in mitigating money laundering and terrorism financing risks. Key metrics such as mean, standard deviation, residual variance, item-total correlation, Cronbach's alpha, internal consistency, and convergent validity are included to assess the reliability and validity of the items.

Table 2 Summary Analysis with Reliability Tests

Items	Mean	Standard Deviation	Residual Variance	Item-Total Correlation	Cronbach Alpha	Internal Consistency	Convergent Validity
Integration Level of Cybersecurity							
INC1	2.25	1.133	1.283	0.436	0.711	0.712	0.747
INC2	2.32	1.148	1.317				
INC3	2.65	1.164	1.355				
Perceived Effectiveness of Cybersecurity							
PEC1	2.31	1.123	1.262	0.513	0.883	0.878	0.792
PEC2	2.34	1.035	1.071				
PEC3	2.24	1.024	1.048				
Integration Level of AI							
INA4	2.32	1.042	1.085	0.410	0.789	0.762	0.634
INA5	2.48	1.157	1.338				
INA6	2.65	1.196	1.430				
Perceived Effectiveness of AI							
PEA1	2.47	1.216	1.478	0.654	0.709	0.708	0.712
PEA2	2.81	1.220	1.489				
PEA3	2.35	1.081	1.169				
Integration Level of Blockchain							
ILB1	2.31	1.093	1.194	0.448	0.754	0.735	0.776

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25oct127

1LB2	2.51	1.210	1.464				
ILB3	1.91	0.849	0.721				
Perceived Effectiveness of Blockchain							
PEB1	2.35	1.060	1.125	0.691	0.836	0.835	0.822
PEB2	2.27	1.073	1.151				
PEB3	2.40	1.111	1.234				

The Cronbach's alpha values across the items indicate that the survey is generally reliable, with most constructs showing acceptable to high reliability. The high item-total correlations for many items further confirm this reliability. The high standard deviations and residual variances suggest significant variability in respondents' perceptions of integration levels and effectiveness. This variability could be due to different organisational contexts, levels of exposure to these technologies, or differing levels of implementation and maturity in cybersecurity, AI, and blockchain adoption.

The mean scores for integration levels of cybersecurity, AI, and blockchain are moderate, indicating that while these technologies are being integrated to some extent, there is room for improvement. This highlights a potential area for organisations to focus on enhancing the integration of these technologies. The perceived effectiveness scores are also moderate, suggesting that respondents see some benefits of these technologies in mitigating money laundering and terrorism financing, but may also recognise limitations or areas where effectiveness could be improved.

The lower integration levels and perceived effectiveness of blockchain compared to cybersecurity and AI suggest that blockchain technology might be less mature or less widely adopted in the context of AML and CTF. This could be a focal point for future initiatives aiming to enhance the use of blockchain in these areas. The combination of items measuring both integration levels and perceived effectiveness allows for a comprehensive assessment of how well these technologies are being utilised and their impact. This dual focus can provide actionable insights for organisations looking to improve their AML and CTF strategies through better integration and use of technology.

B. Inferential Statistics

- *Objective 1: Assess the Relationship between Integration Level (INC) and the Perceived Effectiveness of Cybersecurity (PEC) Measures in Mitigating Money Laundering and Terrorism Financing Risks.*

To assess the relationship between the integration level of cybersecurity measures (INC) and the perceived effectiveness of these measures (PEC), a Pearson correlation analysis was conducted. The results are presented in Table 3.

Table 3 Correlations Between INC and PEC

		INC	**PEC**
INC	Pearson Correlation	1	-.068
	Sig. (2-tailed)		.013
	N	400	400
PEC	Pearson Correlation	-.068	1
	Sig. (2-tailed)	.013	
	N	400	400

The Pearson correlation coefficient between INC and PEC is -0.068 with a p-value of 0.013, indicating a weak negative correlation that is statistically significant. This result suggests that as the integration level of cybersecurity measures increases, the perceived effectiveness of these measures tends to decrease slightly. This counterintuitive finding may reflect complexities in implementation or differing expectations among stakeholders regarding the effectiveness of integrated cybersecurity measures.

- *Objective 2: Assess the Relationship Between Integration Level (INA) and the Perceived Effectiveness of AI (PEA) in Mitigating Money Laundering and Terrorism Financing Risks.*

The relationship between the integration level of AI (INA) and its perceived effectiveness (PEA) was also analysed using Pearson correlation. The results are displayed in Table 4.

Table 4 Correlations Between INA and PEA

		INA	**PEA**
INA	Pearson Correlation	1	.032
	Sig. (2-tailed)		.024
	N	400	400
PEA	Pearson Correlation	.032	1
	Sig. (2-tailed)	.024	
	N	400	400

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25oct127

The Pearson correlation coefficient between INA and PEA is 0.032 with a p-value of 0.024, indicating a very weak positive correlation that is statistically significant. This positive correlation suggests that as the integration level of AI increases, the perceived effectiveness of AI measures also increases slightly. This indicates a slight tendency for stakeholders to view AI integration positively concerning its effectiveness in mitigating financial crimes.

- *Objective 3: Assess the relationship between integration level (INB) and the perceived effectiveness of Blockchain (PEB) in mitigating money laundering and terrorism financing risks.*

The relationship between the integration level of blockchain (INB) and its perceived effectiveness (PEB) was examined through Pearson correlation analysis. The results are summarised in Table 5.

Table 5 Correlations Between INB and PEB

		INB	PEB
INB	Pearson Correlation	1	.041
	Sig. (2-tailed)		.011
	N	400	400
PEB	Pearson Correlation	.041	1
	Sig. (2-tailed)	.011	
	N	400	400

The Pearson correlation coefficient between INB and PEB is 0.041 with a p-value of 0.011, indicating a very weak positive correlation that is statistically significant. This positive correlation implies that as the integration level of blockchain increases, the perceived effectiveness of these measures also increases slightly. Stakeholders seem to view the integration of blockchain technologies as slightly beneficial for improving measures against money laundering and terrorism financing.

- *Objective 4: Explore the Interaction Between the Effectiveness of Cybersecurity Measures, AI, and Blockchain Technologies and the Resulting Impact on their Integration levels in Preventing Money Laundering and Terrorism Financing.*

To explore the interaction between the perceived effectiveness of cybersecurity (PEC), AI (PEA), and blockchain (PEB) on the integration levels of these technologies, a multiple regression analysis was conducted. The model summary is provided in Table 6.

Table 6 Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.452[a]	.323	.316	.70952

a. Predictors: (Constant), PEB, PEC, PEA

The R value of 0.452 indicates a moderate positive correlation between the integration level of these technologies and their perceived effectiveness. The R-Squared value of 0.323 implies that the perceived effectiveness of cybersecurity, AI, and blockchain technologies can explain 32.3% of the variation in the integration level.

The ANOVA results are presented in Table 7, which shows the overall significance of the model.

Table 7 ANOVAa

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	4.718	3	1.573	3.124	.026[b]
	Residual	199.353	396	.503		
	Total	204.071	399			

a. Dependent Variable: INC
b. Predictors: (Constant), PEB, PEC, PEA

The F-statistic of 3.124 with a p-value of 0.026 indicates that the overall model is statistically significant, meaning that the combined perceived effectiveness of cybersecurity, AI, and blockchain significantly predicts the integration level of these technologies. The regression coefficients are detailed in Table 8.

Table 8 Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	2.620	.254		10.298	.000
	PEC	.254	.058	.047	4.379	.000
	PEA	.082	.050	.083	1.637	.102
	PEB	.127	.061	.103	2.071	.039

a. Dependent Variable: INC

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25oct127

The regression analysis reveals several significant findings. The coefficient for the perceived effectiveness of cybersecurity (PEC) is positive and statistically significant (B = 0.254, p < 0.001), indicating that higher perceived effectiveness of cybersecurity measures significantly enhances the integration level. Conversely, the coefficient for the perceived effectiveness of AI (PEA) is not statistically significant (B = 0.082, p > 0.05), suggesting that stakeholders' perceptions of AI effectiveness do not significantly impact the integration level. The coefficient for the perceived effectiveness of blockchain (PEB) is positive and statistically significant (B = 0.127, p < 0.05), highlighting the importance of stakeholders' confidence in blockchain technologies for their integration.

V. CRITICAL DISCUSSION

The Pearson correlation analysis reveals a weak negative correlation (r = -0.068, p = 0.013) between the integration level of cybersecurity measures (INC) and the perceived effectiveness of these measures (PEC). This statistically significant result, despite its weak magnitude, suggests a slightly inverse relationship wherein higher integration levels correlate with marginally lower perceived effectiveness of cybersecurity measures. This finding contrasts with the theoretical expectation that enhanced integration of cybersecurity measures should yield higher perceived effectiveness, as suggested by classical cybersecurity frameworks. Renaud and Coles-Kemp (2022) note the multifaceted challenges inherent in cybersecurity implementations, highlighting that sophisticated and highly integrated systems often introduce complexities that can lead to operational inefficiencies and user dissatisfaction. This complexity can diminish stakeholder confidence in the effectiveness of these measures, particularly in the initial stages of implementation.

Shaikh and Siponen (2023) explored the discrepancy between cybersecurity investments and stakeholder expectations, emphasising that stakeholders often harbour unrealistic expectations about the immediate benefits of integrated cybersecurity solutions. The mismatch between anticipated and actual outcomes can lead to disillusionment, adversely impacting perceived effectiveness. Furthermore, Gligorea et al. (2023) discussed the learning curves and system adaptation processes associated with new technological integrations. These transitional periods, characterised by initial inefficiencies, can negatively affect perceptions of effectiveness. The initial adaptation phase often involves overcoming operational disruptions and refining processes, which may temporarily reduce the perceived efficacy of cybersecurity measures.

The Pearson correlation analysis reveals a very weak positive correlation (r = 0.032, p = 0.024) between the integration level of AI (INA) and its perceived effectiveness (PEA). This suggests that as the integration of AI in financial crime prevention measures increases, there is a slight but statistically significant improvement in stakeholders' perceptions of its effectiveness. This finding indicates a modest level of growing confidence in AI capabilities among stakeholders. The observed positive correlation aligns with existing research highlighting the positive impact of AI integration on the effectiveness of financial crime prevention. For instance, Kumar et al. (2022) emphasised that AI technologies can significantly enhance the detection and prevention of money laundering and terrorism financing activities by providing advanced data analysis and pattern recognition capabilities. However, the weak strength of the correlation might be indicative of lingering initial scepticism surrounding AI implementation, as discussed by Yampolskiy (2021). The author noted that while AI offers substantial benefits, the early stages of adoption often involve overcoming scepticism and demonstrating tangible outcomes to build trust and confidence.

The Pearson correlation analysis reveals a very weak positive correlation (r = 0.041, p = 0.011) between the integration level of blockchain technologies (INB) and their perceived effectiveness (PEB). This slight yet statistically significant increase in perceived effectiveness with higher integration levels of blockchain technologies indicates a growing recognition of blockchain's potential benefits among stakeholders. This finding aligns with the existing literature that underscores blockchain's potential to enhance transparency and security in financial transactions. Rijanto (2024) highlighted the foundational advantages of blockchain technology, including immutable records and decentralised control, which can significantly bolster security measures against financial crimes like money laundering and terrorism financing.

However, the weak strength of the correlation also reflects challenges noted in the literature concerning the initial integration of blockchain technologies. Sobolewski and Allessie (2021) discussed these initial integration challenges, emphasising the need for comprehensive stakeholder education to bridge knowledge gaps and align expectations with technological capabilities. The weak correlation observed in this study suggests that while stakeholders are beginning to appreciate blockchain's benefits, significant hurdles remain in the early stages of integration.

The multiple regression analysis conducted to explore the interaction between the perceived effectiveness of cybersecurity (PEC), AI (PEA), and blockchain (PEB) on the integration levels of these technologies revealed significant predictors of integration levels. Specifically, the combined perceived effectiveness of these technologies explains 32.3% of the variation in integration levels, highlighting the substantial influence that stakeholder perceptions have on the integration process. The findings align with existing literature that underscores the combined impact of multiple technologies in enhancing financial crime prevention measures. Kshetri (2018), for example, discussed the complementary roles these technologies play in providing comprehensive security solutions, where cybersecurity ensures the protection of data, AI enhances predictive analytics, and blockchain ensures transparency and immutability.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25oct127

VI. CONCLUSION

This study aimed to assess the relationship between the integration levels of various advanced technologies, cybersecurity, AI, and blockchain, and their perceived effectiveness in mitigating money laundering and terrorism financing risks. Through Pearson correlation and multiple regression analyses, several key findings emerged. The Pearson correlation analysis revealed a weak negative correlation between the integration level of cybersecurity measures (INC) and their perceived effectiveness (PEC). This suggests that as the integration level of cybersecurity measures increases, the perceived effectiveness tends to decrease slightly, likely due to implementation complexities and misalignment between stakeholder expectations and practical outcomes. For AI, the analysis showed a very weak positive correlation between the integration level (INA) and perceived effectiveness (PEA), indicating a slight increase in perceived effectiveness with higher integration levels. This reflects a growing confidence in AI's capabilities, although initial scepticism persists.

Similarly, a very weak positive correlation was found between the integration level of blockchain technologies (INB) and their perceived effectiveness (PEB). This finding suggests that stakeholders recognise the benefits of blockchain integration, though initial challenges and education gaps may influence perceptions. The multiple regression analysis indicated that the perceived effectiveness of cybersecurity and blockchain had significant positive impacts on integration levels, while AI did not show a significant impact, pointing to ongoing scepticism or a lack of understanding about AI's potential benefits.

- *Based on these Findings, Several Actionable Recommendations are Proposed:*

- Strategic Communication and Expectation Management: Organisations should implement effective communication strategies to align stakeholder expectations with the realities of technology integration. Transparent communication about the expected challenges and benefits can help manage expectations and reduce initial disappointment.
- Enhanced Training and Support: Comprehensive training and support during the integration phase are crucial to mitigate initial inefficiencies and improve user confidence in new systems. Equipping stakeholders with the necessary skills and knowledge can enhance the perceived effectiveness of cybersecurity measures.
- Transparency in AI Processes: To address AI perception issues, organisations should invest in educating stakeholders about AI's capabilities and real-world applications. Providing clear examples of successful AI implementations and highlighting its complementary role alongside other technologies can build greater confidence.
- Proactive Addressing of Integration Challenges: Organisations should emphasise the unique benefits of blockchain in training and communication with stakeholders. Addressing integration challenges proactively can improve perceptions and facilitate smoother technology integration.

Based on the findings of this study, several areas for future research can be identified to explore further and address the complexities and dynamics of integrating advanced technologies in mitigating money laundering and terrorism financing risks. The study reveals a weak negative correlation between cybersecurity integration and perceived effectiveness, indicating underlying complexities and misalignment of expectations. Future research should focus on case studies and stakeholder perceptions to understand these challenges. AI integration shows a very weak positive correlation with perceived effectiveness, suggesting initial scepticism. Research should explore factors like transparency and trust, and conduct longitudinal studies on evolving perceptions. Blockchain integration also shows a very weak positive correlation, highlighting the need for educational programs and best practices.

REFERENCES

[1]. Adebayo, T. A. (2025a). The relationship between financial development and economic growth in Nigeria. *Review of Business and Economics Studies*, *13*(1), 24–42. https://doi.org/10.26794/2308-944x-2025-13-1-24-42

[2]. Akartuna, E.A., Johnson, S. & Thornton, A. (2022). Preventing the Money Laundering and Terrorist Financing Risks of Emerging technologies: an International Policy Delphi Study. *Technological Forecasting and Social Change*, 179, p.121632. Doi: https://doi.org/10.1016/j.techfore.2022.121632.

[3]. Antunes, S. & Cabral, S. (2019). *The Impact of Blockchain Technology on Anti-Money Laundering and Counter-Terrorism Financing Management by Financial Institutions*. [online] Available at: https://repositorio.iscte-iul.pt/bitstream/10071/19391/4/master_sofia_silva_cabral.pdf.

[4]. Cheng, H.K., Hu, D., Puschmann, T. & Zhao, J.L. (2021). The Landscape of Blockchain Research: Impacts and Opportunities. *Information Systems and e-Business Management*. Doi:https://doi.org/10.1007/s10257-021-00544-1.

[5]. Coffey, S.M. & Elliott, M.R. (2023). Optimising Data Collection Interventions to Balance Cost and Quality in a Sequential Multimode Survey. *Journal of survey statistics and methodology*. doi:https://doi.org/10.1093/jssam/smad007.

[6]. Drescher, D. (2017). *Blockchain Basics*. Berkeley, CA: Apress. doi:https://doi.org/10.1007/978-1-4842-2604-9.

[7]. Gligorea, I., Cioca, M., Oancea, R., Gorski, A.-T., Gorski, H. & Tudorache, P. (2023). Adaptive Learning Using Artificial Intelligence in e-Learning: A Literature Review. *Education Sciences*, 13(12), pp.1216–1216. doi:https://doi.org/10.3390/educsci13121216.

[8]. Granadeiro, C. (2023). Decoding the Future of Artistic Creations: the Legal Challenges and Possible

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25oct127

Solutions for the Regulation of Non-Fungible Tokens (NFTs). *Business Law Review*, [online] 44(6). Available at: https://kluwerlawonline.com/journalarticle/Business+Law+Review/44.6/BULA2023025 [Accessed 3 Mar. 2024].

[9]. Gundur, R.V., Levi, M., Topalli, V., Ouellet, M., Stolyarova, M., Chang, L.-C. & Domínguez Mejía, D. (2021). *Evaluating Criminal Transactional Methods in Cyberspace as Understood in an International Context*. [online] *Research @ Flinders*. CrimRxiv. Available at: https://researchnow.flinders.edu.au/en/publications/evaluating-criminal-transactional-methods-in-cyberspace-as-unders.

[10]. Kalam, A.A.E. & Mssassi, S. (2024). Leveraging Blockchain for Enhanced Traceability and Transparency in Sustainable Development. *Lecture Notes in Networks and Systems*, pp.162–177. doi:https://doi.org/10.1007/978-3-031-54318-0_14.

[11]. Kshetri, N. (2018). Blockchain's Roles in Meeting Key Supply Chain Management Objectives. *International Journal of Information Management*, [online] 39(39), pp.80–89. doi: https://doi.org/10.1016/j.ijinfomgt.2017.12.005.

[12]. Kumar, P., Murphy, A., Werner, S. & Christophe Rougeaux (2022). *The fight against money laundering: Machine learning is a game changer*. [online] McKinsey & Company. Available at: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-fight-against-money-laundering-machine-learning-is-a-game-changer [Accessed 3 Jun. 2024].

[13]. Li, J., Maiti, A. & Fei, J. (2023). Features and Scope of Regulatory Technologies: Challenges and Opportunities with Industrial Internet of Things. *Future Internet*, [online] 15(8), p.256. doi: https://doi.org/10.3390/fi15080256.

[14]. Maboe, R. (2018). *An Overview of Blockchain Technology in the South African Financial Industry*. [online] Available at: https://wiredspace.wits.ac.za/server/api/core/bitstreams/afbd275a-494a-4018-b43a-510f86d7db7b/content.

[15]. Memon, M.A., Ting, H., Cheah, J.-H., Thurasamy, R., Chuah, F. & Cham, T.H. (2020). Sample Size for Survey Research: Review and Recommendations. *Journal of Applied Structural Equation Modeling*, [online] 4(2). doi: https://doi.org/10.47263/jasem.4(2)01.

[16]. Pavlidis, G. (2023). Deploying Artificial Intelligence for Anti-Money Laundering and Asset Recovery: The Dawn of a New Era. *Deploying Artificial Intelligence for Anti-Money Laundering and Asset Recovery: The Dawn of a New Era*, 26(7), pp.155–166. doi: https://doi.org/10.1108/jmlc-03-2023-0050.

[17]. Renaud, K. & Coles-Kemp, L. (2022). Accessible and Inclusive Cyber Security: A Nuanced and Complex Challenge. *SN Computer Science*, 3(5). doi: https://doi.org/10.1007/s42979-022-01239-1.

[18]. Rijanto, A. (2024). Blockchain Technology Roles to Overcome accounting, Accountability and Assurance Barriers in Supply Chain Finance. *Asian Review of Accounting*. doi: https://doi.org/10.1108/ara-03-2023-0090.

[19]. Rocha-Salazar, J.-J., Segovia-Vargas, M.-J. and Camacho-Miñano, M.-M. (2021). Money Laundering and Terrorism Financing Detection Using Neural Networks and an Abnormality Indicator. *Expert Systems with Applications*, [online] 169, p.114470. doi: https://doi.org/10.1016/j.eswa.2020.114470.

[20]. Rose-Ackerman, S. & Palifka, B.J. (2018). Corruption, Organized Crime, and Money Laundering. *Institutions, Governance and the Control of Corruption*, [online] pp.75–111. doi: https://doi.org/10.1007/978-3-319-65684-7_4.

[21]. Rueda, M. del M., Martínez-Puertas, S. & Castro-Martín, L. (2022). Methods to Counter Self-Selection Bias in Estimations of the Distribution Function and Quantiles. *Mathematics*, [online] 10(24), p.4726. doi: https://doi.org/10.3390/math10244726.

[22]. Sartori, M., Seher, I. & Prasad, C. (2023). The Illicit Use of Cryptocurrency on the Darknet by Cyber Criminals to Evade Authorities. *Lecture notes in electrical engineering*, pp.449–459. doi: https://doi.org/10.1007/978-3-031-29078-7_39.

[23]. Saunders, M., Lewis, P. & Thornhill, A. (2019). *Research Methods for Business Students*. 8th ed. United Kingdom: Pearson.

[24]. Schwarz, N., Chen, M.K., Poh, M.K., Jackson, M.G., Kao, K., Fernando, M.F. & Markevych, M. (2021). *Virtual Assets and Anti-Money Laundering and Combating the Financing of Terrorism (1): Some Legal and Practical Considerations*. [online] *Google Books*. International Monetary Fund. Available at: https://books.google.com.ng/books?hl=en&lr=&id=WxVNEAAAQBAJ&oi=fnd&pg=PP6&dq=However [Accessed 3 Mar. 2024].

[25]. Shaikh, F.A. & Siponen, M. (2023). Organisational Learning from Cybersecurity Performance: Effects on Cybersecurity Investment Decisions. *Inf Syst Front*, 26. doi: https://doi.org/10.1007/s10796-023-10404-7.

[26]. Sharif, M.R. (2023). Exploring the Potential: Smart Contracts and the Fight against Trade-Based Money Laundering in International Trade. *Social Science Research Network*. [online] doi: https://doi.org/10.2139/ssrn.4616946.

[27]. Sobolewski, M. and Allessie, D. (2021). Blockchain Applications in the Public Sector: Investigating Seven Real-Life Blockchain Deployments and Their Benefits. *Public Administration and Information Technology*, pp.97–126. doi: https://doi.org/10.1007/978-3-030-55746-1_5.

[28]. Toufaily, E., Zalan, T. & Dhaou, S.B. (2021). A Framework of Blockchain Technology Adoption: an Investigation of Challenges and Expected Value. *Information & Management*, 58(3), p.103444. doi: https://doi.org/10.1016/j.im.2021.103444.

[29]. Upadhyay, N. (2020). Demystifying Blockchain: A Critical Analysis of Challenges, Applications, and Opportunities. *International Journal of Information*

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25oct127

Management, 54. doi: https://doi.org/10.1016/j.ijinfomgt.2020.102120.
[30]. Yampolskiy, R.V. (2021). *AI Risk Scepticism*. [online] arXiv.org. doi: https://doi.org/10.48550/arXiv.2105.02704.
[31]. Yang, X. and Chan, J. (2021). Blockchain and Identity Management. *Springer eBooks*, pp.192–204. doi: https://doi.org/10.1007/978-3-030-93179-7_15.
[32]. Yıldırım, U. (2023). Exploring the Trends, Challenges, and Opportunities of Regulatory Technology (RegTech) in the Financial Industry: A Systematic Literature Review. *Cankaya.edu.tr*. [online] doi: http://hdl.handle.net/20.500.12416/7165.