

Enhancing Know Your Customer (KYC) and Anti-Money Laundering (AML) Compliance Using Blockchain: A Business Analysis Approach.

ALLIY BELLO¹, DAVID AMOAH ODURO², EMMANUEL OPOKU³, ADEPEJU DEBORAH BELLO⁴, ADENIJI OMOTAYO LEO⁵, CHIOMA EMMANUELA UKATU⁶, NONSO OKIKA⁷

¹*Project Business Analysis, Northeastern University*

²*Compliance Department, JP Morgan Chase & Co.*

³*Informatics and Networked System, University of South Florida*

⁴*Fraud Department, Barclays Bank,*

⁵*Compliance and Risk, Central Bank of Nigeria,*

⁶*Business Analyst, Sony Interactive Entertainment, U.S. A*

⁷*Network Security Analyst, University of Michigan*

Abstract- This study explored the potential of blockchain technology in improving Know Your Customer (KYC) and Anti-Money Laundering (AML) processes within the financial sector. The study aims to conduct an investigation of the current state of existing literature surrounding the use of blockchain in KYC/AML, as well as the emerging trends in the space, it further aims to clarify the barriers to adoption, and that includes barriers such as regulatory concerns and technical challenges. An organized method that contains thorough literature reviews, well-defined inclusion and exclusion criteria, thematic analysis is used to examine the effectiveness and strategic implications of blockchain technology. Specifically analyzed topics include the improvements as concerns identity verification, advanced fraud detection functionalities and the integration of the blockchain technology within regulatory aspects. This research helps significantly not only in the academic domain but is also very useful for the financial institutions and regulatory bodies striving to utilize blockchain for a more efficient and secure compliance environment..

Indexed Terms- Anti-Money Laundering (AML), Blockchain, Business Analysis, Compliance, Know Your Customer (KYC).

I. INTRODUCTION

KYC (Know Your Customer) & AML (Anti-Money Laundering) is an important procedure for avert financial crimes, obligating that institutions requires the name of customer and anti-money laundering that is compulsory to report a suspicious transaction [1]. Traditional compliance procedures face issues like the operational expense, redundancies and inefficiencies because of duplicate verifying consumer identification over various organizations [2]. Legacy systems are also centralized and thus prevent secure data sharing and regulatory compliance [3]. The problems lead to delay in compliance, fines, and negative feedback from customers due to lengthy onboarding procedures. Above all traditional systems do not have real time monitoring capabilities which prevent for proactive detection of financial frauds [4]. Manual KYC processes are susceptible to errors and fraud, therefore, there is a need for a more efficient and secure solution. Blockchain technology provides a disruptive method by making a decentralized, transparent and secure cryptographically facilitated platform for identity verification and data sharing [5]. By its decentralized nature, it minimizes redundancy, operational expenses, and upholds security in KYC/AML processes [6]. Blockchain's smart contracts automate customer KYC, transaction monitoring and SAR, reducing the scope for human

intervention [7]. However, blockchain adopting still faces limitation of scalability, regulatory ambiguity and integration with existing systems [8]. This paper examines how blockchain technology can improve KYC/AML compliance through a business analysis perspective, investigating the costs and challenges associated as well as the effects it has on financial institutions.

II. RESEARCH AIM AND OBJECTIVES

The primary aim of this study is to examine how blockchain technology can enhance KYC and AML compliance in financial institutions by addressing inefficiencies, reducing costs, and improving fraud detection mechanisms. This research takes a business analysis approach to assess the feasibility and strategic impact of blockchain in compliance frameworks.

The key objectives of this study are:

- 1) To review existing literature on blockchain applications in KYC/AML compliance and assess their effectiveness.
- 2) To identify emerging trends in blockchain-based compliance solutions, including innovations in digital identity verification and automated transaction monitoring.
- 3) To highlight key challenges in blockchain adoption, including regulatory barriers, data privacy concerns, and technical scalability issues.

To propose strategic business recommendations for financial institutions on how to effectively integrate blockchain into their compliance processes.

III. SIGNIFICANCE OF THE STUDY

This research is theoretically and practically relevant, enriching the ongoing academic-practical discussion of blockchain's part in the framework of implementing regulatory compliance. Academics, it expands knowledge of blockchain-based KYC/AML frameworks by demonstrating how DLT promotes a safe, tamper-proof compliance system [9]. It is also in accordance with Regulatory Technology (RegTech) and digital financial security, showing the impact of blockchain on modern financial regulations [4]. Practically, this research contributes to the

financial sector, business analysts and regulatory bodies. Business analysts can leverage its insights to build blockchain-enabled effectiveness models, innovation operational proficiency, & decision-making [3]. Financial services companies can deploy blockchain for cheaper compliance, more data security, faster customer onboarding [5]. Sensors, on the other hand, receive guidance on using blockchain within their existing compliance systems; though assuring security and interoperability [8]. Through examining blockchain's position in the compliance modernization, this research provides strategic advice on creating a transparent, safe and technology-based financial system that can efficiently combat financial crimes.

IV. METHODOLOGY

This study employs a structured approach to systematically review existing literature on the application of blockchain technology in enhancing Know Your Customer (KYC) and Anti-Money Laundering (AML) compliance. The methodology encompasses a comprehensive literature search strategy, clearly defined inclusion and exclusion criteria, and a thematic analysis of the selected studies.

V. LITERATURE SEARCH STRATEGY

The literature search was conducted across multiple reputable databases to ensure a wide-ranging collection of relevant studies. Primary sources included academic journals, industry reports, and case studies accessed through databases such as Google Scholar, Scopus, and Web of Science. The search was performed using specific keywords and phrases to capture the intersection of blockchain technology with KYC and AML compliance. Key search terms included "blockchain and KYC," "AML compliance with blockchain," and "financial technology compliance." These terms were used both individually and in combination to maximize the retrieval of pertinent literature. Additionally, reference lists of selected articles were examined to identify further studies of relevance.

To maintain the relevance and quality of the literature review, specific inclusion and exclusion criteria were

established. Studies were included if they met the following criteria:

a) Inclusion Criteria:

- Peer-reviewed articles published from 2015 onwards, ensuring the inclusion of contemporary research findings.
- Industry reports and case studies that provide practical insights into the implementation of blockchain in KYC and AML processes.
- Publications focusing on the financial sector's application of blockchain technology for compliance purposes.

b) Exclusion Criteria:

- Non-English language publications, to maintain consistency in analysis.
- Studies focusing on non-financial applications of blockchain, as they fall outside the scope of this research.
- Articles lacking empirical data or comprehensive analysis, to ensure the inclusion of substantive and evidence-based studies.

This selection process aimed to curate a collection of high-quality, relevant literature that provides both theoretical and practical insights into the use of blockchain for KYC and AML compliance.

VI. APPROACH TO ANALYSIS

The analysis of the selected literature was conducted using a thematic analysis approach, which allowed for the systematic identification and examination of recurring themes and patterns related to blockchain technology's role in Know Your Customer (KYC) and Anti-Money Laundering (AML) compliance. The thematic approach was chosen for its ability to organize complex information into meaningful categories, facilitating a structured synthesis of key insights from diverse sources.

The literature was categorized based on the following core themes:

- **Identity Verification:** Studies were analyzed to assess how blockchain enhances secure, decentralized, and efficient customer identity verification processes, reducing reliance on traditional centralized databases.
- **Fraud Detection:** Research was examined to understand how blockchain technology

strengthens fraud detection mechanisms by ensuring transaction transparency, immutability, and real-time monitoring.

- **Regulatory Adoption:** Literature addressing the integration of blockchain into existing AML compliance frameworks was reviewed, focusing on challenges, legal considerations, and policy implications.

Each study was evaluated based on its methodology, key findings, and relevance to business analysis. By grouping research into these themes, the study offers a systematic and in-depth exploration of blockchain's transformative role in regulatory compliance. This approach ensures a comprehensive understanding of the potential benefits, limitations, and practical applications of blockchain technology in modern financial institutions.

VII. THEORETICAL BACKGROUND

KYC AND AML COMPLIANCE: AN OVERVIEW
 Know Your Customer (KYC) as well as Anti-Money Laundering (AML) needs are sturdy to financial compliance, created to quit criminal tasks like money laundering, fraudulence, as well as terrorism financing. KYC instructs the financial institutions to verify the identities of their clients, evaluate the associated risks and to monitor the transactions for any suspicious activities. AML increases these measures with the imposition of due diligence, transaction monitoring and reporting requirements [10]. Client compliance is overseen by international regulatory environments. The Financial Action Task Force (FATF) sets AML standards that member countries adopt into their national policies. In the European Union (EU), Anti-Money Laundering Directives (AMLD) set responsibilities of financial institutions, in the United States of America, Financial Crimes Enforcement Network (FinCEN) is responsible for compliance with the Bank Secrecy Act (BSA) [11]. Despite such measures traditional KYC/AML methods are still in-efficient. Excessive identity verification steps drive-up compliance costs, slow onboarding processes and annoy customers and financial institutions [12]. Moreover, centralized identity databases are such risky of security problems, exposure for financial data sensitive to breaches [13]. As compliance regulations become

more intricate, there is a pressing requirement for creative technology-supported options that can boost efficiency and security in financial compliance processes [7].

VIII. BLOCKCHAIN TECHNOLOGY

Blockchain technology provides a disruptive answer to boost the KYC & AML compliance by solving issues in conventional financial surveillance systems. Decentralization reduces dependence on single central authority allowing reduction to risks of data manipulation and improvement in security [14]. Immutability ensures that once record, compliance data cannot be changed, giving tamper-proof and auditable records for the regulators [8]. Besides, transparency enables authorized parties to check compliance-related data in real-time, increasing regulatory oversight and decreasing fraud risks [15]. Smart contracts moreover ease compliance by making certain regulatory workflows are on autopilot; where some degree of manual intervention, fraud and far further is eliminated [7]. Using these features, blockchain reduces fraud by secure identity verification and cryptographic protection [16]. Automated record-keeping allows regulated parties to make timely and accurate regulatory reports, decrease non-compliance penalties [17]. Besides, blockchain enables a safe sharing of data among financial institutions, avoiding duplicate KYC processes and decreasing compliance costs [5]. In the end, blockchain increases compliance efficiency, promotes financial security, and aids world efforts in preventing financial crimes [7].

IX. BUSINESS ANALYSIS IN COMPLIANCE PROCESSES

Business analysis is critical for streamlining of compliance workflow, spot non-optimization and enhance risk assessment on financial institutions. Data driven decisions can enable analysts to scan through KYC and AML systems, point to operational gaps and enable them to come up with exploring alternative for upgrading compliance with regulations [10]. Blockchain business process modeling helps to automate, detects real time fraud and improves due diligence by integrating blockchain to business process model. Blockchain powered identity

verification comes up with a single universal, verifiable customer profile across financial entities which takes away redundant authentication steps and simplifies compliance processes [18]. In addition, the transparent nature of blockchain ensures enhanced probability of calculation of risk, augmenting the cybernetic detective power for risk diagnosis due to the functionality of secured financial transaction history mainly spoiling record tampering capabilities permitting furthermore the seizure identification within various suspicious financial performance marketers in money laundering [19]. Moreover, business analysis also helps to ensure that the AML strategies are aligned with regulatory expectations, to ensure that the institutions meet the evolving global standards [20]. In addition, blockchain integration enables to increase efficiency by automation of transactions monitoring, cost saving in the compliance area, and reduction of regulatory fines [21]. Ultimately, the synergy between business analysis and blockchain increases the financial security, risks management, and the trust of digital transaction [10].

X. DISCUSSIONS

Through a thematic analysis of various studies, it becomes evident that blockchain offers promising solutions for improving KYC and AML processes, but overcoming technical and regulatory hurdles remains essential for widespread adoption.

XI. BLOCKCHAIN APPLICATIONS IN KYC

According to a substantial body of literature converges on the potential of blockchain to revolutionize KYC processes through secure identity management and the automation of customer onboarding. Scholars such as Olawoyin (2024) and Stockburger et al. (2021) propose that blockchain's distributed nature enables the formation of self-sovereign identities where individuals manage personal data. This not only increases the privacy of the individuals but also decreases the risk of data breaches associated with standard centralized systems. Olawoyin (2024) [22] highlights that blockchain's immutable feature significantly protects the integrity of identity data, making it very difficult for tampering or fraud. This is an improvement over

the traditional KYC which is a database that is susceptible to cyberattack. Meanwhile, according to Stockburger et al. (2021) [23] and Jain et al. (2024) [24], blockchain is allowing smart contracts to automate the verification of customer identities, which is decreasing operational costs and making the implementation of onboarding process much faster and efficient. This is particularly relevant for financial institutions, which by tradition has high administrative costs and lengthy periods of time spent verifying the identities of their customers. Blockchain capacity to aid in the establishment of all these methods by avoiding intermediaries and self-identifying identity checks, is seen as a great advantage that could generate more operational efficiency in banks and other financial service firms. In addition, the ability of blockchain to enable interoperability between various financial institutions is another important benefit pointed out by authors such as [25] and [26]. As soon as an identity has been verified on the blockchain, it can safely be shared with other organizations without needing to be verified once again. This is particularly valuable in a globalized economy, where customers typically deal with multiple financial institutions to enhance the experience of the user and to eradicate redundancy. However, [27] agree that even though blockchain has a lot of potential for enhancing KYC procedures, its application is still restricted. The slow run to take up can be explained, however, by several hurdles, such as regulatory booby trapping and a requirement for standardising by authority. Olawoyin (2024) [22] also notes that one of the problems that blockchain is facing with large volume of transactions and data is scalability, and it is likely that, for mass adoption to happen, will need to overcome significant technical hurdles.

XII. BLOCKCHAIN APPLICATIONS IN AML

However, when it comes to Anti-Money Laundering (AML) compliance, the literature is again positively disposed towards blockchain's capacity to revolutionize the sector. It is noted by [24] and [28] that the benefits of blockchain in real-time transaction monitoring and fraud detection can be seen. Blockchain's a transparent, unalterable record enables financial institutions to surface transactions with speed, making it a much harder case for

screening illicit activities, like money laundering. According to [24] this capability greatly improves the effectiveness of AML programmes by allowing for more proactive detection of suspicious activity.

Blockchain also provides special advantages in allowing cross-border compliance. According to [28], the decentralized and transparent character of blockchain allows regulators from various countries to access the same data instantly. This is especially critical for the purpose of anti-money laundering as illicit activities always include cross border transactions. By enabling financial institutions to share data securely and instantly, blockchain has the potential to streamline global AML efforts, reducing the time it takes to detect and respond to suspicious activities.

Furthermore, consensus mechanism embedded in blockchain technology guarantees that all participants in the transaction verify the data and hence adds an extra layer of security. Kokogho, et al (2025) [25] explain that this feature increases the level of transparency and level of trust that exists in the financial transactions, thus defending easy access for money launderers to tamper the monetary system. When creating a detailed, easily auditable record of all transactions, blockchain can enable more effective audits and regulatory reporting, and therefore compliance with AML requirements.

Yet, as stated by [29] and [27], the use of blockchain in AML is not without issues. A scalability of blockchain still remains a big issue, especially when it comes to high volume of financial transactions around the world. Moreover, the linkup between blockchain with existing financial infrastructure and old systems also have a lot of obstacles. As [26] points out, though blockchain has the potential to enhance AML compliance, the slow pace of adoption and the need for the modernization of current systems might hinder its adoption.

XIII. CHALLENGES AND RISKS IN BLOCKCHAIN ADOPTION

Although the advantages of the blockchain in KYC and AML are well known, a consistent thread through the literature is that its use is hampered by

technical and regulatory obstacles. Scholars such as [27] and [22] mention scalability as the chief technical obstacle. Blockchain networks, especially those which are built on top of proof-of-work consensus algorithms, were inaccurate to manage excessive payloads of transactions effectively. Olawoyin (2024) [22] notes that the speed of blockchain networks in processing data, specifically in the case of large-scale applications, is too slow to match the needs of financial institutions. Another crucial issue encountered in the literature is called interoperability, and it is mainly related to the blockchain systems and to financial infrastructure in place. Numerous financial organizations are still running on legacy systems and implementing blockchain to these systems is not an easy job and it needs big investment and technical knowledge. Rusli and Fermay (2024) [28] and Zhuk (2025) [29] note that the lack of standardized protocols across different blockchain platforms further complicates the process of integration. Without clear industry standards, financial institutions may be hesitant to adopt blockchain, fearing compatibility issues and additional costs.

Cybersecurity is another area of concern. While blockchain is often praised for its security features, it is not immune to cyber threats. Scholars such as [25] and [26] highlight that vulnerabilities in smart contracts or flaws in the blockchain's code could be exploited by malicious actors, posing a risk to financial institutions. As [27] argue, ensuring the robustness of blockchain's security framework is critical to its adoption in sensitive sectors like finance and healthcare.

Regulatory challenges also remain a significant barrier. [25] and [26] cite that weaknesses of smart contracts or vulnerabilities in the blockchain code can be manipulated by attackers which could attack the crypto upsets in the financial land. Morar and Popescu (2024) [27] highlight the need to secure the robustness of blockchain's security framework to enable it for adoption in such sensitive industries as finance and healthcare.

However, other challenges, such as getting regulated properly, are also prevalent in this region. In this case, several researchers including [29] and [22]

believe that there lacks certainty in legal cases of blockchain and blockchain applications in many jurisdictions. For instance, problems like data privacy, where the General Data Protection Regulation (GDPR) stands as an example, do make the deployment of blockchain within the financial services quite challenging. The fact that blockchain cannot delete or change stored data clashes with information privacy laws that require a right to be forgotten, leaving a legal ambiguity. In addition, the un-standardized legal provisions across the boards create a problem for global financial companies to deploy blockchain systems.

XIV. IMPLICATIONS FOR BUSINESS ANALYSIS

Blockchain really changes business analysis in the financial services in terms of KYC and AML compliance. In KYC, blockchain removes redundant verification by allowing shared and verified customer identity records that are permanent and accessible across financial institutions, prevented duplication of checks and lower costs [30]. Encryption capabilities of it guarantee a higher level of security through the maintenance of data integrity and privacy and automate customer on-boarding so as to reduce administrative overhead [31]. Blockchain for AML functions facilitate real-time abuse detection by logging transaction collections on a comparative ledger that can fetch on immediately examined for suspect task at any time [32]. This transparency aids in eliminating human mistake and enhancing reporting correctness [26]. Business analysts must assess who blockchain helps streamline processes, reduce risks, and meet regulatory requirements to make financial institutions increase efficiency, reduce security risks, and remain compliant [29].

XV. IMPROVING KYC PROCESSES

Blockchain improves KYC processes by reducing redundant verification, enhancing security, and streamlining customer onboarding. By recording customer identity information on a safe, decentralized log, blockchain as of now empowers various foundations to get to data without the need to re-verify, which lessens the expenses and the time [30]. Blockchain's cryptographic methods give data

integrity, preventing unauthorized changes and protects from identity fraud [26]. Besides, blockchain also automates identity verification with smart contracts. It accelerates user onboarding and enhances user experience [31]. This not only increases operational performance but also ensures conformity to regulatory needs and enables consumers to produce safer and more user-friendly [33].

XVI. STREAMLINING AML COMPLIANCE

Blockchain technology simplifies AML compliance by making it possible for real-time fraud detection, higher reporting accuracy and lower human mistakes. Transactions documented in a blockchain are unaltered and open, permitting financial establishments to identify suspicious activities promptly [32]. Blockchain's distributed characteristics provide data available for real-time compliance monitoring, decreases time spent to detect and report fraud [33]. Additionally smart contracts permit regulatory reporting to be automated, making compliance with the effectiveness that diminishes human oversight and error [26]. This improves overall dynamics of AML processes, resulting in faster, more effective, fraud detection and filing.

XVII. RECOMMENDATIONS FOR FINANCIAL INSTITUTIONS

Several steps need to be taken to ensure that financial organizations are able to successfully implement blockchain for compliance. First, pilot programs should be conducted to determine whether blockchain is effective in KYC/AML [32]. Cost-benefit analysis will help to assess the financial viability and long term savings of blockchain adoption by including costs of implementation and maintenance [34]. Maintaining regulatory cohesion is crucial and institutions need to work with the regulators in order that blockchain based solutions conform to the financial laws and regulations and meet the standard for data protection [29]. Also, promoting partnerships between fintech startups, conventional banks and regulators will make it easier for blockchain to be integrated, promoting innovation with compliance [35].

CONCLUSION

Blockchain technology has been known for good things to come in creating more efficiency and security to the financial compliance processes as it relates to KYC and AML framework. This decentralization saves admin cost and also increases the data accuracy and thus the operational efficiency. In addition, blockchain's cryptographic safety functionalities guarantee that delicate shopper information is safely encrypted and secured from unauthorized entry, lowering dangers of identification theft and fraud. In terms of AML compliance, blockchain's capacity to offer open, genuine and timely transaction observation is crucial to the prevention and reporting of fraud. The decentralized and characteristic immutable property of the blockchain makes financial purchases possible to locate vicarious activities rapidly and share data securely with fortune guardians, timely eliminate an individual blunders and solving blow faithful. These attributes greatly diminish the costs linked to compliance violation and fines and improve regulatory adherence. Blockchain's capacity to enhance customer acceptance procedure, decrease operational costs, as well as improve safeguard has significant impacts on banking institutions. Blockchain not only enhances effectiveness, but also lowers conformity costs by lowering the requirement for hands-on control and replicate verifications. As the financial industry presses on with blockchain adoption, the technology offers up a chance for a more transparent, risk-free, and compliant planet of business practices and ingenuity in career combinations of industries.

REFERENCES

- [1] R. Arasa and L. Ottichilo, "Determinants of Know Your Customer (KYC) compliance among commercial banks in Kenya," *J. Econ. Behav. Stud.*, vol. 7, no. 2, pp. 162–175, 2015.
- [2] E. Esoimeme, *Balancing anti-money laundering measures and financial inclusion: The example of the United Kingdom and Nigeria*. Belmont, CA: Wadsworth, 2020.
- [3] B. Hoffman, J. Okeniyi, and S. Samuel, "Antecedents of compliance with anti-money

- laundering regulations in the banking sector of Ghana," *J. Risk Financ. Manag.*, vol. 17, no. 8, p. 373, 2024. doi: 10.3390/jrfm17080373.
- [4] I. Zavoli and C. King, "The challenges of implementing anti-money laundering regulation: An empirical analysis," *Mod. Law Rev.*, vol. 84, no. 4, pp. 740–771, 2021. doi: 10.1111/1468-2230.12655.
- [5] N. Deepak, J. Patel, L. Jain, M. Srivastava, and H. Jagadish, "A review on Know Your Customer (KYC) system using blockchain technology," *IOSR J. Comput. Eng.*, vol. 25, no. 2, Ser. II, pp. 1–5, 2023. doi: 10.9790/0661-2502020105.
- [6] G. Tripathi, M. A. Ahad, and G. Casalino, "A comprehensive review of blockchain technology: Underlying principles and historical background with future challenges," *Decis. Anal. J.*, vol. 9, p. 100344, 2023. doi: 10.1016/j.daj.2023.100344.
- [7] M. Javaid, A. Haleem, R. P. Singh, S. Khan, and R. Suman, "Blockchain technology applications for Industry 4.0: A literature-based review," *Blockchain: Res. Appl.*, vol. 2, p. 100027, 2021. doi: 10.1016/j.bcr.2021.100027.
- [8] Z. Zheng, S. Xie, H. N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *Int. J. Web Grid Serv.*, vol. 14, no. 4, pp. 352–375, 2018. doi: 10.1504/IJWGS.2018.095647.
- [9] M. Drgon, L. Georgiou, and A. Kiayias, "Robust KYC via distributed ledger technology," unpublished. Available: <https://doi.org/10.6084/m9.figshare.13301363>.
- [10] P. Paul and T. Iyelolu, "Anti-money laundering compliance and financial inclusion: A technical analysis of Sub-Saharan Africa," *GSC Adv. Res. Rev.*, vol. 19, pp. 336–343, 2024. doi: 10.30574/gscarr.2024.19.3.0235.
- [11] B. Abikoye, S. Umeorah, A. Adelaja, O. Ayodele, and Y. Ogunsuji, "Regulatory compliance and efficiency in financial technologies: Challenges and innovations," *World J. Adv. Res. Rev.*, vol. 23, pp. 1830–1844, 2024. doi: 10.30574/wjarr.2024.23.1.2174.
- [12] H. P. Josyula, "Digital identity verification: Transforming KYC processes in banking through advanced technology and enhanced security measures," *Int. Res. J. Modern. Eng. Technol. Sci.*, vol. 5, pp. 128–137, 2023. doi: 10.56726/IRJMETS44476.
- [13] S. K. Mamatha, R. R. Hegde, M. Kamala, and S. Shreevidhya, "KYC verification using blockchain," *Int. J. Novel Res. Dev.*, vol. 8, no. 6, 2023.
- [14] R. Weerawarna, S. J. Miah, and X. Shao, "Emerging advances of blockchain technology in finance: A content analysis," *Pers. Ubiquitous Comput.*, pp. 1–14, 2023. doi: 10.1007/s00779-023-01712-5.
- [15] P. Yeoh, "Regulatory issues in blockchain technology," *J. Financ. Regul. Compliance*, vol. 25, no. 2, pp. 196–208, 2017. doi: 10.1108/JFRC-08-2016-0068.
- [16] A. Thommandru and D. Chakka, "Recalibrating the banking sector with blockchain technology for effective anti-money laundering compliances by banks," *Sustainable Futures*, vol. 5, p. 100107, 2023. <https://doi.org/10.1016/j.sfr.2023.100107>.
- [17] M. Utkina, "Leveraging blockchain technology for enhancing financial monitoring: Main challenges and opportunities," *Eur. J. Interdiscip. Stud.*, vol. 15, no. 2, p. 134, 2024.
- [18] P. Singhal, "Enhancing compliance and KYC processes through AI, OCR, and automation: A cost-effective approach," *Int. J. Comput. Eng. Technol.*, vol. 15, no. 5, pp. 1002–1009, 2024. <https://doi.org/10.5281/zenodo.14000750>.
- [19] P. Maweu, D. Kiragu, and A. Kuria, "Assessment of anti-money laundering practices on financial crime prevention among commercial banks in Kenya," *Int. J. Econ. Bus. Manag. Res.*, vol. 8, no. 8, pp. 309–X, 2024. <https://doi.org/10.51505/IJEBMR.2024.8821>.
- [20] D. M. F. Bello and A. O. Cosmas, "The role of the Economic and Financial Crime Commission (EFCC) in combating corruption in Nigeria," *Musamus J. Public Admin.*, vol. 5, no. 1, 2022.
- [21] A. T. Nicknora, "Anti-money laundering compliance and financial performance of selected commercial banks in South Sudan: A survey of literature on customer due diligence," *J. Financ. Risk Manag.*, vol. 13, no. 2, 2024.

- [22] O. Olawoyin, "Blockchain technology in risk management: Strengthening cybersecurity and financial integrity," *Int. J. Res. Publ. Rev.*, vol. 5, pp. 2336–2348, 2024. <https://doi.org/10.55248/gengpi.5.1024.2829>.
- [23] L. Stockburger, G. Kokosioulis, A. Mukkamala, R. R. Mukkamala, and M. Avital, "Blockchain-enabled decentralized identity management: The case of self-sovereign identity in public transportation," *Blockchain Res. Appl.*, vol. 2, no. 2, p. 100014, 2021. <https://doi.org/10.1016/j.bcra.2021.100014>.
- [24] V. Jain, A. Balakrishnan, P. Chintale, S. Gadiparthi, and M. Najana, "Blockchain empowerment in sanctions and AML compliance: A transparent approach," *Int. J. Comput. Trends Technol.*, vol. 72, no. 5, pp. 11–26, 2024. <https://doi.org/10.14445/22312803/IJCTT-V72I5P102>.
- [25] E. Kokogho, O. Onwuzulike, B. Omowole, C. Ewim, and M. Adeyanju, "Blockchain technology and real-time auditing: Transforming financial transparency and fraud detection in the Fintech industry," *Gulf J. Adv. Bus. Res.*, vol. 3, no. 2, pp. 348–379, 2025. <https://doi.org/10.51594/gjabr.v3i2.88>.
- [26] U. Nweje, "Blockchain technology for secure data integrity and transparent audit trails in cybersecurity," *Int. J. Res. Publ. Rev.*, vol. 5, no. 12, pp. 4902–4916, 2024.
- [27] C. D. Morar and D. E. Popescu, "A survey of blockchain applicability, challenges, and key threats," *Computers*, vol. 13, no. 9, p. 223, 2024. <https://doi.org/10.3390/computers13090223>.
- [28] G. R. Rusli and A. H. Fermay, "Digital financial services effort in enforcing anti-money laundering (AML) through open banking optimization," *AML/CFT J.: J. Anti-Money Laundering Countering Financ. Terror.*, vol. 2, no. 2, pp. 159–174, 2024. <https://doi.org/10.59593/amlcft.2024.v2i2.158>.
- [29] A. Zhuk, "Beyond the blockchain hype: Addressing legal and regulatory challenges," *SN Soc. Sci.*, vol. 5, no. 11, 2025. <https://doi.org/10.1007/s43545-024-01044-y>.
- [30] J. Parra-Moyano, O. Ross, and T. Thoroddsen, "Optimized and dynamic KYC system based on blockchain technology," *Int. J. Blockchains Cryptocurr.*, vol. 1, no. 1, p. 1, 2019. <https://doi.org/10.1504/IJBC.2019.10021398>.
- [31] D. Malhotra, P. Saini, and A. Singh, "How blockchain can automate KYC: Systematic review," *Wireless Pers. Commun.*, vol. 122, pp. 1–13, 2022. <https://doi.org/10.1007/s11277-021-08977-0>.
- [32] A. Thommandru and B. Chakka, "Recalibrating the banking sector with blockchain technology for effective anti-money laundering compliances by banks," *Sustainable Futures*, vol. 5, p. 100107, 2023. <https://doi.org/10.1016/j.sftr.2023.100107>.
- [33] T. Kukman and S. Gričar, "Blockchain for quality: Advancing security, efficiency, and transparency in financial systems," *FinTech*, vol. 4, no. 1, p. 7, 2025. <https://doi.org/10.3390/fintech4010007>.
- [34] R. Jena, "Examining the factors affecting the adoption of blockchain technology in the banking sector: An extended UTAUT model," *Int. J. Financ. Stud.*, vol. 10, no. 4, p. 90, 2022. <https://doi.org/10.3390/ijfs10040090>.
- [35] J. S. Varughese, "Streamlining regulatory processes with blockchain technology: Case studies and best practices," *Int. J. Sci. Res.*, vol. 13, no. 4, 2024. [Online]. Available: <https://www.ijsr.net>.