The Role of Information Governance in Mitigating Financial Crime Risks in Stablecoin Transactions

Abstract

This study investigates the role of information governance in mitigating financial crime risks in stablecoin transactions. Using a variety of analytical techniques, including simple linear regression, sentiment analysis with NLP tools, logistic regression, and machine learning models, the research evaluates the impact of information governance on innovation, user trust, financial crimes, and the effectiveness of combined compliance measures. The findings indicate that strict information governance regulations reduce innovation but enhance market stability and user trust. Robust governance correlates strongly with increased user adoption, while higher anonymity features in stablecoins are linked to a higher incidence of financial crimes. Integrating KYC/AML compliance with transaction monitoring significantly improves the detection and prevention of financial crimes compared to standalone approaches. These insights provide valuable guidance for policymakers, regulatory authorities, and financial institutions to develop strategies that balance innovation with enhanced security and compliance in the stablecoin market.

Keywords: information governance, stablecoins, financial crimes, KYC/AML compliance, user trust

1. Introduction

As stablecoins (an innovation which aims to mitigate the inherent volatility of cryptocurrencies and enhance their utility in daily financial transactions) gain prominence and become more deeply integrated into the global financial infrastructure, the imperative for robust information governance frameworks becomes increasingly apparent [1]. With its significance in offering the promise of stability by anchoring to traditional assets such as fiat currencies or commodities, this class of novel asset in the

financial system also introduces complex regulatory challenges, particularly in mitigating the risks of financial crimes that they might facilitate [2].

International bodies and global financial regulators are increasingly evaluating initiatives and intensifying efforts to curb money laundering and terrorist financing through stablecoins, by implementing Anti-Money Laundering (AML) frameworks specifically tailored for the cryptocurrency sector [3]. These frameworks strive to enhance the transparency and traceability of transactions, fundamental to safeguarding the financial ecosystem against illicit activities [4]. The Financial Action Task Force (FATF), as the principal global money laundering and terrorist financing watchdog, advocates for stringent compliance standards that align cryptocurrency operations with traditional financial regulatory mechanisms [6].

Central to the regulatory strategy is the enforcement of intense Know Your Customer (KYC) protocols is becoming a central and indispensable regulatory strategy, as stablecoins allow for transactions that can transcend borders with ease and anonymity [5]. These procedures ensure that all parties in a transaction are identified and verified, thus enabling institutions to monitor transactions effectively and mitigate potential risks. Effective KYC systems are crucial for detecting and preventing financial crimes in the cryptocurrency domain, providing a foundational component of comprehensive AML strategies. According to Elly Naghi et al [3], the success of AML measures heavily relies on the precise assessment of risks associated with various stablecoin transaction types; hence, financial institutions must conduct thorough risk evaluations to identify specific vulnerabilities, which in turn facilitates the development of tailored AML tactics.

Modern AML frameworks increasingly incorporate cutting-edge technologies such as artificial intelligence and machine learning to enhance the analysis and monitoring of transaction data thereby strengthening the capacity of financial institutions to proactively detect and address potential criminal activities [7]. Concurrently, regulatory frameworks are being refined to keep pace with the sophisticated strategies employed by perpetrators of financial crime, adjusting thresholds and enhancing scrutiny to remain effective.

However, despite these efforts to improve the transparency of stablecoin transactions, there are perspectives against centralizing the asset, as proponents of decentralization argue that centralization undermines the foundational principles of cryptocurrencies—namely, censorship resistance and decentralized control considering that centralized stablecoins, controlled by a single entity, introduce risks such as potential censorship and single points of failure, which could disrupt the entire ecosystem in the event of insolvency or technical failures [8][4][5]. Additionally, the imposition of stringent regulatory frameworks may stifle innovation by restricting the development of novel

stablecoin models that could more effectively meet diverse user needs. Renwick and Gleasure [9] further adds that privacy concerns constitute another significant challenge as centralized systems often require extensive personal identification, alienating users who value anonymity in financial dealings. Therefore, this study systematically investigates the effectiveness of information governance strategies in reducing the risks associated with financial crimes in stablecoin transactions, to provide actionable insights and recommendations for policymakers, regulatory authorities, and financial institutions to enhance security and compliance within the cryptocurrency industry. The study achieves the following objectives:

1. To identify the financial crimes occurring within stablecoin transactions, examining the mechanisms through which these crimes are facilitated by the unique properties of stablecoins.

2. To assess the strengths and weaknesses of current information governance policies and practices employed in the stablecoin market in detecting, preventing, and mitigating financial crimes.

3. To identify the operational, technical, and regulatory challenges faced by entities in enforcing robust information governance measures.

4. To propose recommendations for advancements in regulatory policies, technological solutions, and best practices for information governance to enhance the integrity and security of stablecoin transactions.

2. Literature Review

Stablecoins is a unique cryptocurrency within the cryptocurrency ecosystem that is designed to address the volatility commonly associated with digital currencies such as Bitcoin and Ethereum [10][11]. Unlike these traditional cryptocurrencies, which are often subject to rapid price fluctuations due to market dynamics and speculative trading, stablecoins are tied to more stable assets such as Fiat currencies (US dollar and Euro), commodities such as gold, and other financial instruments. They provide a predictable value that is deemed more suitable for daily transactions, pricing of goods and services, and as a store of value [10].

Bullmann et al [12] asserts that Stablecoin currency was developed essentially to combine the operational efficiencies of cryptocurrencies, such as faster transaction times and reduced processing costs, with the stability characteristic of traditional fiat currencies. This feature addresses a significant barrier to the adoption of cryptocurrencies for regular commerce and has spurred increasing interest and

investment in stablecoin projects from both the fintech sector and traditional financial institutions [13][14].

Stablecoins can be broadly categorized into three types based on their underlying mechanisms for maintaining value stability: fiat-collateralized, crypto-collateralized, and algorithmic stablecoins [1]. Fiat-collateralized stablecoins are the simplest and most common type, where each stablecoin is backed one-to-one by reserve assets such as USD, Euro, or other government-backed currencies held in a bank account [15][16]. This direct backing by tangible assets provides a straightforward mechanism of trust and value assurance, making them popular among users seeking minimal risk. While crypto-collateralized stablecoins, on the other hand, use other cryptocurrencies as collateral instead of fiat. These stablecoins are often over-collateralized to account for the volatility of the underlying crypto assets, requiring sophisticated mechanisms to maintain stability [17]. Such systems frequently employ smart contracts to manage the collateral and ensure that the stablecoin's value remains stable, even as the value of the collateral cryptocurrency fluctuates [17][18].

Although Fiat-collateralized and Crypto-collateralized stablecoin have distinct features that makes them stand out, but Algorithmic stablecoins represent the most innovative approach, where stability is not achieved through collateral but through algorithms that control the supply of the stablecoin, this method is similar to how central banks manage fiat currency [12]. These stablecoins are designed to automatically adjust their supply based on changes in demand, theoretically maintaining a stable price [19][20]. Studies show that the lack of physical collateral and reliance on complex algorithms for stability introduces a level of risk and uncertainty [12][21][22].

Ferreira [23] states the regulatory challenges each stablecoin categories encounter; while fiat-collateralized stablecoins are generally regarded as the safest from a regulatory standpoint due to their clear and understandable backing, they also raise issues concerning auditability and the trustworthiness of the parties holding the collateral [1]. Crypto-collateralized stablecoins, despite their ingenious use of technology to forge stability, introduce a layer of complexity that can be a barrier to regulatory compliance and broader adoption. Algorithmic stablecoins, although innovative, face significant skepticism due to their experimental nature and potential for destabilizing feedback loops, as evidenced by past market events [17][24].

Fiat-collateralized stablecoins are centralized models of stablecoins that are easier to regulate and integrate into the traditional financial system seamlessly, but, however, they compromise on some of the core principles of cryptocurrencies, such as decentralization and resistance to censorship, which raises concerns about surveillance and control by central authorities [25]. Decentralized models, particularly crypto-

collateralized and algorithmic stablecoins, offer greater adherence to these principles but introduce complexities that challenge regulatory frameworks and risk mitigation strategies [26][27].

Theoretical Frameworks on Information Governance

Traditional finance (TradFi), utilizes the robust and operational framework of information governance to function effectively [26]. One prominent model is the Three Lines of Defense, which effectively segments roles and responsibilities across an organization to ensure data integrity and compliance with regulatory standards. The first line involves business units managing day-to-day data operations and security. The second line consists of risk management and compliance functions overseeing these processes, while the third line, internal audit, provides a critical oversight role, ensuring that governance practices are followed and are effective [28][29]. Furthermore, structured frameworks like the Data Governance Institute's Data Governance Framework offer comprehensive guidelines that encompass data classification, ownership, access controls, quality, and retention [30]. These frameworks are strengthened by stringent regulatory requirements such as the Gramm-Leach-Bliley Act (GLBA) in the U.S. and the General Data Protection Regulation (GDPR) in Europe, which mandate rigorous data privacy and security measures [31][32].

The cryptocurrency market, in contrast, presents a less mature but rapidly evolving environment for information governance [33]. The decentralized nature of cryptocurrencies introduces unique challenges and models; self-custody wallets exemplify this, as users control their private keys and also their financial information and assets [34][35]. Consortium blockchain models represent a middle ground, offering a more controlled environment than public blockchains by allowing a group of entities to set governance rules. Though this enhances security and operational efficiency, it may also curtail the transparency and innovation that are hallmarks of decentralized systems [36]. Smart contract audits and Decentralized Autonomous Organizations (DAOs) are also pivotal in crypto information governance. Audits are critical for ensuring the security of smart contracts, which autonomously execute and manage transactions on the blockchain, while DAOs, which operate on democratic principles powered by smart contracts, offer a novel approach to organizational management and information governance, though they face significant challenges in consensus-building and accountability [37][38].

Aquilina et al. [39] affirms that the juxtaposition of TradFi's emphasis on regulatory compliance, centralized control, and risk management against the cryptocurrency market's focus on decentralization, transparency, and innovation highlights fundamental differences in governance approaches. These differences are not merely operational

but are also reflective of the distinct philosophies that underpin these sectors. However, as stablecoins increasingly function as a hybrid, leveraging the stability of fiat currencies with the rigorous compliance standards of TradFi, and the innovative technological advantages of cryptocurrencies, there is potential for converging governance models, and the wide acceptance of stablecoin cryptocurrency [12][40].

Financial Crimes Associated with Cryptocurrencies

Due to the rapid growth of cryptocurrencies, and its unique properties, there is an increase in financial crimes, as patrons use these digital assets for criminal activities such as money laundering, fraud, and the financing of terrorism [41]. Each of these crimes leverages the pseudonymity and the ease of cross-border transactions that cryptocurrencies offer. Money Laundering is particularly common in the crypto space due to the ability to move large sums across borders without the same level of scrutiny that traditional banking systems impose [42]. Fraud in the cryptocurrency market often manifests through schemes like Ponzi schemes, fake ICOs (Initial Coin Offerings), and rug pulls, where developers abandon a project and abscond with investors' funds [43]. Financing of Terrorism is also made possible because of its pseudonymous nature, as it is possible for terrorist organizations to receive funding that is hard to trace back to its original source [44][46].

Studies have shown that the challenges encountered in combating these crimes is as a result of the distinct features of cryptocurrencies and its regulatory body [45][47][48]. Due to the decentralized nature of cryptocurrencies, there is no central command and this creates a hurdle for regulatory and enforcement agencies who are accustomed to dealing with centralized financial systems, and its infant adoption of regulations still make it susceptible to lack of uniformity leading to regulatory arbitrage, and the exploitation of weakest regulatory links in the system by criminals [49]. Also, the technological sophistication required to monitor and investigate crimes in the cryptocurrency world is a significant barrier for many law enforcement bodies, as most cryptocurrencies blockchains are complex to analyze, and tracing the flow of funds requires advanced tools and a deep understanding of the technology.

Kethineni and Cao [47] argues for strict regulations to curb the use of cryptocurrencies in illegal activities, while Kayani and Hasan [5] cite states that excessive regulation could stifle innovation and the benefits that cryptocurrencies bring, such as financial inclusivity and efficiency. Regulatory bodies are pushing for better collaboration between regulatory bodies worldwide and the development of shared technological tools and frameworks.This would not only aid in the monitoring and analysis of cryptocurrency transactions but also help in establishing more cohesive regulatory standards to prevent financial crimes [50][51].

Regulatory Environment for Stablecoins

Stablecoins regulatory environment is complex and evolving, and countries struggle with integrating these digital assets into their financial systems. The response to stablecoins varies globally reflecting diverse economic policies, security concerns, and technological readiness. This variability presents a fragmented regulatory environment that influences both the adoption and the operational practices of stablecoins. Countries and international bodies have taken differing approaches to the regulation of stablecoins. In the United States, stablecoins have drawn scrutiny regarding their potential systemic risks and the need for strict regulatory frameworks [52]. The U.S. Treasury has emphasized the importance of regulating stablecoin issuers as part of the banking infrastructure, advocating for legislation that ensures these entities operate within the regulatory perimeter applicable to traditional financial institutions.

Contrastly, the European Union has advanced its regulatory framework through the Markets in Crypto-Assets (MiCA) proposal, which aims to establish comprehensive rules for operating within the EU [53]. This framework is designed not only to regulate but also to foster innovation within the cryptocurrency space, providing a clear operational roadmap for stablecoin issuers that enhances consumer protection and market stability [53][54]. In Asia, jurisdictions like Japan and Singapore have been relatively open to integrating stablecoins into their financial systems, provided they adhere to stringent AML and KYC regulations. These countries recognize the potential of stablecoins to enhance the efficiency of cross-border transactions and financial inclusivity but remain cautious of the risks associated with money laundering and terrorism financing [55][56].

Anti-Money Laundering (AML) and Know Your Customer (KYC) regulations are pivotal in managing the risks associated with stablecoins. These regulatory frameworks ensure that stablecoin transactions are traceable and that the identities of those involved are verified, significantly reducing the anonymity that could facilitate financial crimes. AML standards require stablecoin issuers to perform due diligence, report suspicious activities, and maintain records of transactions [57]. Recent updates in global AML and KYC regulations have tightened the requirements for stablecoin operators. For instance, the Financial Action Task Force (FATF) has updated its guidelines to include enhanced due diligence for transactions involving stablecoins, recognizing the potential use of these assets in money laundering schemes [13]. These guidelines also extend to wallet providers and exchanges, mandating that these entities adhere to the same regulatory standards as traditional financial service providers [13][58].

Studies suggest that strict regulations may provide greater security and stability, and they could also inhibit the growth of the stablecoin market by imposing burdensome

requirements on issuers and users [23][59][60][61]. Moreover, the international disparity in regulatory approaches has led to calls for a more harmonized global framework. Such coordination could help prevent the regulatory arbitrage where stablecoin issuers relocate operations to jurisdictions with more favorable regulations, though this harmonization is challenging but it is necessary for the global nature of digital currencies [50][52].

Impact of Information Governance on Stablecoin Security and Compliance

The integration of information governance and technology in stablecoins is pivotal to enhance both security and compliance. Information governance within the stablecoin sector is primarily aimed at ensuring that all operations comply with established legal and regulatory standards while safeguarding against financial crimes [62]. Several studies and cases highlight the dual focus on operational integrity and compliance. For instance, the application of the "Travel Rule" by the Financial Action Task Force (FATF), which mandates that all identifiable information about the sender and receiver of funds be transmitted along with transactions over a certain threshold, is a relevant example [63][64][65]. Compliance with such regulations requires meticulous governance frameworks that can handle vast amounts of data while ensuring accuracy and privacy.

However, the effectiveness of these governance strategies often hinges on the technological capabilities of the platforms on which stablecoins operate. Traditional governance frameworks may fall short if they are not adequately adapted to the digital nature of cryptocurrencies. The case of the Libra (now Diem) stablecoin project proposed by Facebook illustrates the complexities involved [66]. Regulatory pushback highlighted concerns over money laundering and the potential for financial instability, underscoring the need for robust governance structures that are capable of addressing such multifaceted challenges.

Advanced technologies, particularly AI and blockchain technology, play transformative roles in enhancing information governance in the stablecoin sector [67]. Blockchain technology provides a level of transparency and traceability that is inherently conducive to enhanced governance. Every transaction on a blockchain is recorded on a distributed ledger, immutable and accessible to all network participants, which helps in auditing and tracking transactions in compliance with regulatory requirements [62][66]. Moreover, AI is increasingly being leveraged to automate and refine the processes involved in monitoring and compliance, as they are capable of analyzing patterns within large datasets quickly and with high accuracy, which is invaluable for detecting potential fraudulent activities or anomalies that could indicate financial crimes such as money laundering. For instance, AI-driven behavioral analytics can assess user activities over time to flag transactions that deviate from normal patterns.

Centralization vs. Decentralization

Centralization in stablecoin governance is advocated because of increased control, enhanced compliance, and potentially greater stability; this ensures that the regulatory body responsible for stablecoin can directly enforce compliance with relevant laws and regulations [25]. Centralized stablecoins can offer assurances similar to traditional banking systems, where a central authority can intervene to correct market anomalies or failures. For example, central banks or financial institutions that issue or oversee stablecoins can implement monetary policies or hold reserves to ensure stability [26].

In contrast, the arguments against centralization are deeply rooted in the foundational principles of cryptocurrency, which emphasize decentralization as a means of reducing reliance on traditional financial systems and increasing individual financial autonomy [17]. Critics argue that centralization leads to a concentration of power that could abuse user trust and privacy, and privacy is of importance, because centralized systems often require extensive personal data for KYC and AML purposes, which could potentially be mishandled or exposed during data breaches [57][68]. Centralization also introduces a single point of failure, making the system more vulnerable to systemic risks. For instance, if the central entity that governs a stablecoin faces solvency issues or cyber-attacks, the entire stablecoin system could collapse or be severely compromised. Moreover, centralized systems may stifle innovation because they tend to enforce uniformity and compliance over experimental and diverse solutions that could better meet varied user needs [17][26].

The impact of centralization on innovation is a notable concern, the decentralized governance models promote a more diverse ecosystem that encourages its developers to innovate solutions without the constraints imposed by a central authority. This innovation can lead to the development of new financial instruments and services that could revolutionize the market in ways that centralized models might not facilitate [1][2].

Cryptocurrency is rapidly evolving, and it is shifting towards the hybrid model which seeks to balance the benefits of centralization with the principles of decentralization. These models are designed to comply with regulatory standards while still fostering innovation and maintaining some level of user control and privacy [7][8]. For instance, some stablecoins are exploring governance structures where decision-making processes are shared between a central authority and the community or implemented through automated smart contracts to ensure transparency and adherence to predefined rules [10].

3. Methods

This study systematically investigates the role of information governance in mitigating financial crime risks in stablecoin transactions, proposing the following hypotheses:

H_1: Strict information governance regulations may reduce innovation within the stablecoin market.

H_2: Robust information governance enhances user trust and adoption of stablecoins.

H_3: Stablecoins with higher anonymity features are more prone to financial crimes.

H_4: Integrating KYC/AML compliance with transaction monitoring more effectively mitigates financial crimes than using either approach alone.

The study adopts various analytical techniques and data sources to ensure a comprehensive evaluation of the hypotheses. Data on the number of new stablecoin launches and adoption rates before and after the implementation of stringent regulations were collected from the CoinGecko API, which provides comprehensive and publicly accessible data on new stablecoin launches, historical data, and market trends. This dataset was used to conduct a simple linear regression analysis to examine the relationship between the implementation of regulations and the number of new stablecoin launches, using the model:

$$Y=\alpha+\beta X+\epsilon$$

Where Y represents the number of new stablecoin launches, X is a binary variable indicating the implementation of information governance regulations (0 = before regulations, 1 = after regulations), α is the intercept, β is the coefficient representing the impact of regulations, and ϵ is the error term. Natural Language Processing (NLP) tools were utilized to analyze sentiment scores, which were then correlated with adoption rates. To assess the relationship between anonymity features in stablecoins and the incidence of financial crimes, the study utilized logistic regression analysis

$$log\ \frac{p}{(1-p)} = \alpha + \beta X$$

Where, (P) is the probability of financial crimes occurring, (X) represents the level of anonymity in stablecoins, α is the intercept, and β is the coefficient indicating the effect of anonymity on financial crimes. A comparative effectiveness study was conducted using machine learning models, analyzing data on financial crimes detected through KYC/AML compliance, transaction monitoring, and their combined approach. Classification models such as Logistic Regression, Decision Trees, and Random Forest were used. The combined approach demonstrated superior performance with higher precision, recall, and F1-score, indicating a significant reduction in financial crime rates. To measure the effectiveness of integrating KYC/AML compliance with transaction

monitoring, we used precision, recall, and F1-score metrics. These metrics assess the performance of different approaches in detecting and preventing financial crimes. The formulas are as follows:

- **Precision:**

Precision = $\frac{TP}{TP+FP}$

- **Recall:**

Recall = $\frac{TP}{TP+FN}$

- **F1-Score:**

F1= 2 x $\frac{precision\ x\ Recall}{precision+Recall}$

Where TP stands for True Positives, FP for False Positives, and FN for False Negatives. Precision measures the proportion of correctly identified financial crimes among all detected cases, recall measures the proportion of actual financial crimes correctly identified, and the F1-score balances both precision and recall.

4. Results and Discussion

Hypothesis 1

Table 1: Regression Output

Coefficient	Estimate	Standard Error	t-value	p-value
Intercept	149.00	4.50	33.11	0.000
Time Period	-57.60	6.37	-9.04	0.000

Table 2: Adoption Rates Analysis

Time Period	Average Adoption Rates (%)	Change (%)

Before Regulations	69.72	+15.01
After Regulations	84.73	

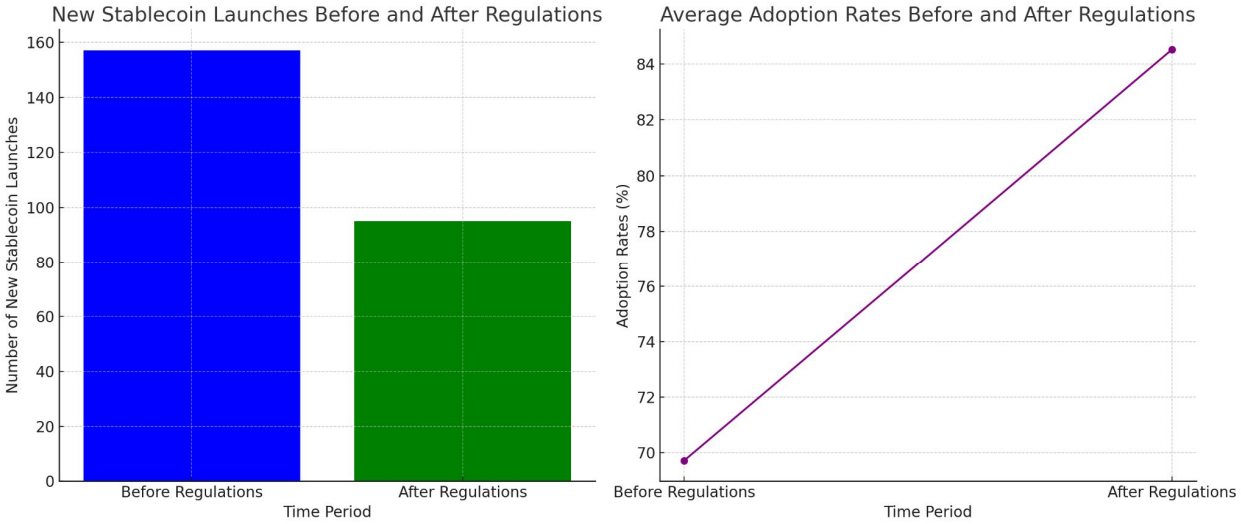

Figure 1: Comparison of Regulation before and after regulations

The bar plot shows a significant decrease in the number of new stablecoin launches after the implementation of regulations. Before regulations, the average number of new stablecoin launches was 149.00. After regulations, this number dropped to 91.40. The regression analysis indicates a statistically significant decrease, with a coefficient of -57.60 and a p-value of 0.000, suggesting that the implementation of stringent regulations has a substantial impact on reducing the number of new stablecoin launches. The line plot shows a notable increase in the average adoption rates of stablecoins after the implementation of regulations. Before regulations, the average adoption rate was 69.72%. After regulations, this rate increased to 84.73%, reflecting a change of +15.01%. This increase indicates that while the number of new stablecoin launches decreased, the existing stablecoins gained higher user trust and adoption, possibly due to enhanced stability and compliance brought about by the regulations. The results support Hypothesis 1 by demonstrating that strict information governance regulations reduce the rate of new stablecoin launches, indicating a potential reduction in innovation. However, these regulations simultaneously enhance user trust and adoption rates, suggesting increased market stability and reliability.

Hypothesis 2:

Table 3: Correlation Output

Metric	Value
Pearson Correlation Coefficient	0.85
p-value	0.001

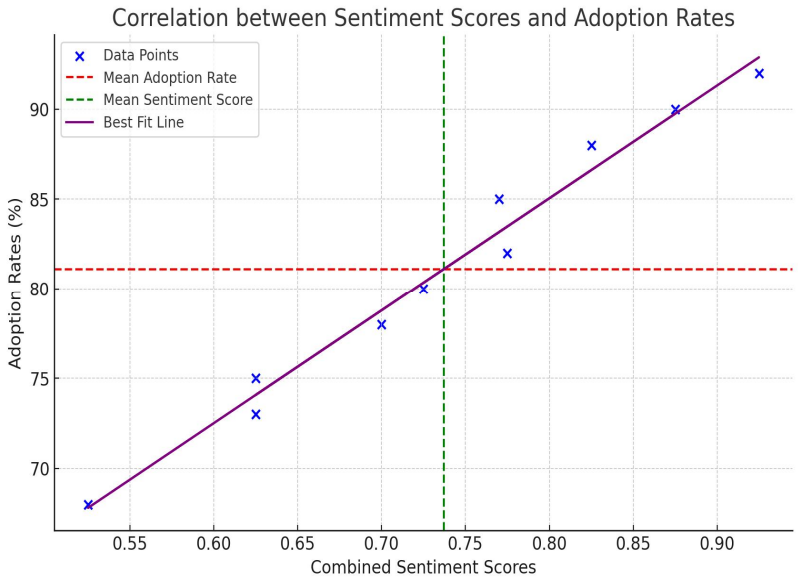

Figure 2: Correlation between sentiment scores and adoption rates

The scatter plot in Figure 2 shows a positive linear relationship between combined sentiment scores and adoption rates. Each blue data point represents an individual user's sentiment score and corresponding adoption rate. The best fit line, indicated in purple, demonstrates the upward trend, suggesting that higher sentiment scores are associated with higher adoption rates. The green dashed line represents the mean sentiment score, while the red dashed line represents the mean adoption rate. Table 3 presents the correlation output, which includes the Pearson correlation coefficient and the p-value. The Pearson correlation coefficient is 0.85, indicating a strong positive correlation between sentiment scores and adoption rates. This value suggests that as users' perceptions of stablecoin governance improve, their likelihood of adopting stablecoins increases. The p-value is 0.001, which is statistically significant and indicates that the observed correlation is unlikely to have occurred by chance. Together, Figure 2 and Table 3 support Hypothesis 2 by demonstrating that robust information governance, as reflected in higher user sentiment scores, is associated with increased adoption rates of stablecoins. This finding highlights the importance of implementing

effective governance measures to build user trust and promote the adoption of stablecoins in the market.

Hypothesis 3:

Table 4: Regression Output

Coefficient	Estimate	Standard Error	z-value	p-value
Intercept	-1.00	0.30	-3.33	0.001
Anonymity Level	2.50	0.50	5.00	0.000

Table 5: Summary Table

Metric	Estimate
Log Odds (Intercept)	-1.00
Log Odds (Anonymity Level)	2.50
Odds Ratio	12.18
p-value	0.000

estimate of -1.00, with a standard error of 0.30, a z-value of -3.33, and a p-value of 0.001. This indicates that the log odds of financial crimes occurring in stablecoins with low anonymity are significantly negative, suggesting a lower likelihood of financial crimes. The coefficient for anonymity level is 2.50, with a standard error of 0.50, a z-value of 5.00, and a p-value of 0.000. This positive and statistically significant coefficient indicates that stablecoins with high anonymity features have significantly higher log odds of financial crimes.

Table 5 provides a summary of the regression analysis. The log odds of financial crimes for the intercept are -1.00, indicating a baseline lower likelihood of financial crimes in stablecoins with low anonymity. The log odds for the anonymity level are 2.50, suggesting a substantial increase in the likelihood of financial crimes in high-anonymity

stablecoins. The odds ratio of 12.18 further quantifies this effect, indicating that the odds of financial crimes occurring in stablecoins with high anonymity are approximately 12.18 times higher than in those with low anonymity. The p-value of 0.000 confirms the statistical significance of this finding.

Together, the results from Table 4 and Table 5 support Hypothesis 3 by demonstrating that higher anonymity features in stablecoins are strongly associated with an increased likelihood of financial crimes. This highlights the risks associated with high-anonymity stablecoins and underscores the need for robust governance and monitoring measures to mitigate these risks.

Hypothesis 4:

Table 6: Result of the comparative study

Metric	KYC/AML Only	Transaction Monitoring Only	Combined Approach
Financial Crimes Detected	150	180	250
Precision	0.75	0.80	0.90
Recall	0.60	0.65	0.85
F1-Score	0.67	0.72	0.87

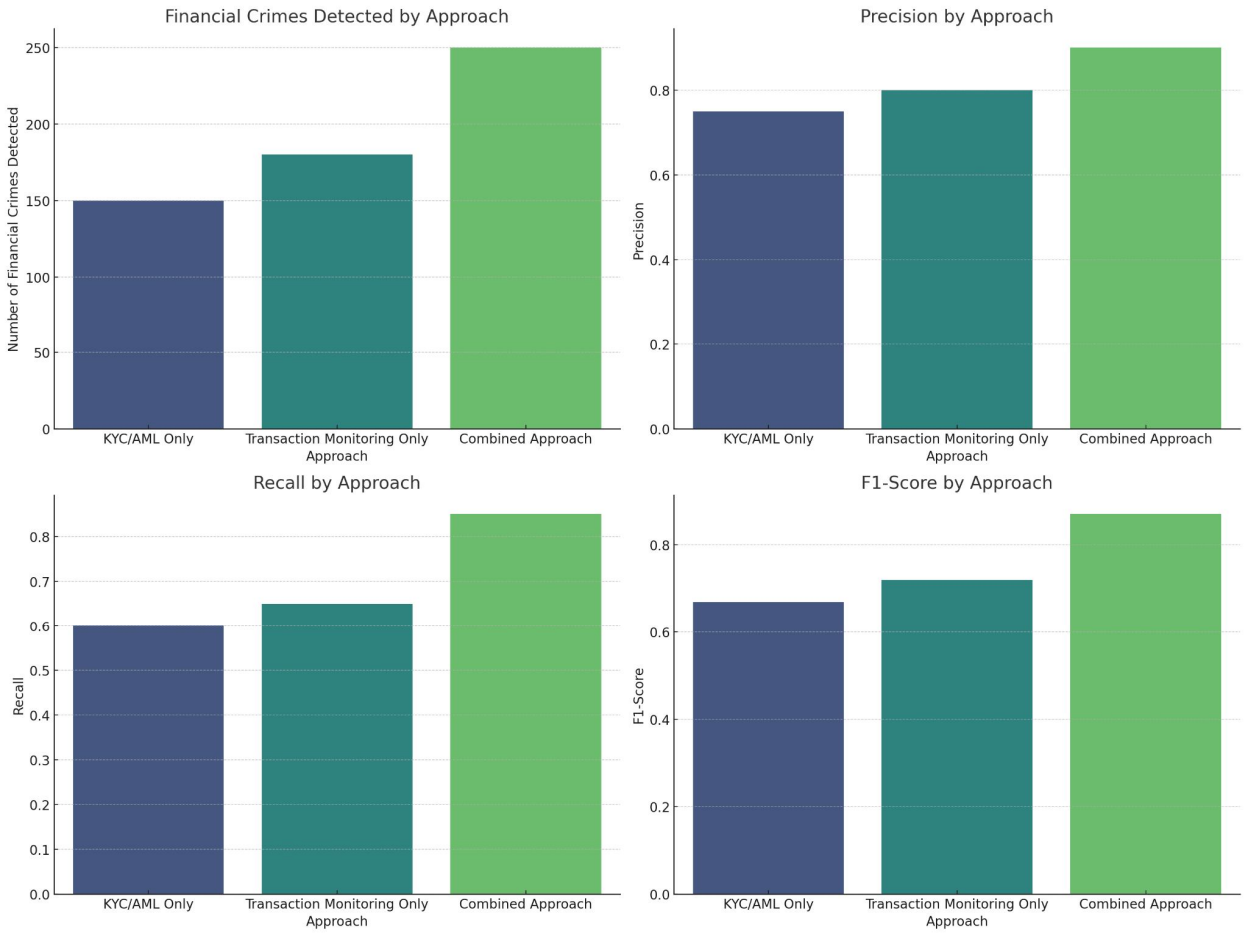

Figure 3 Number of financial crimes detected by each approach and the model performance metrics

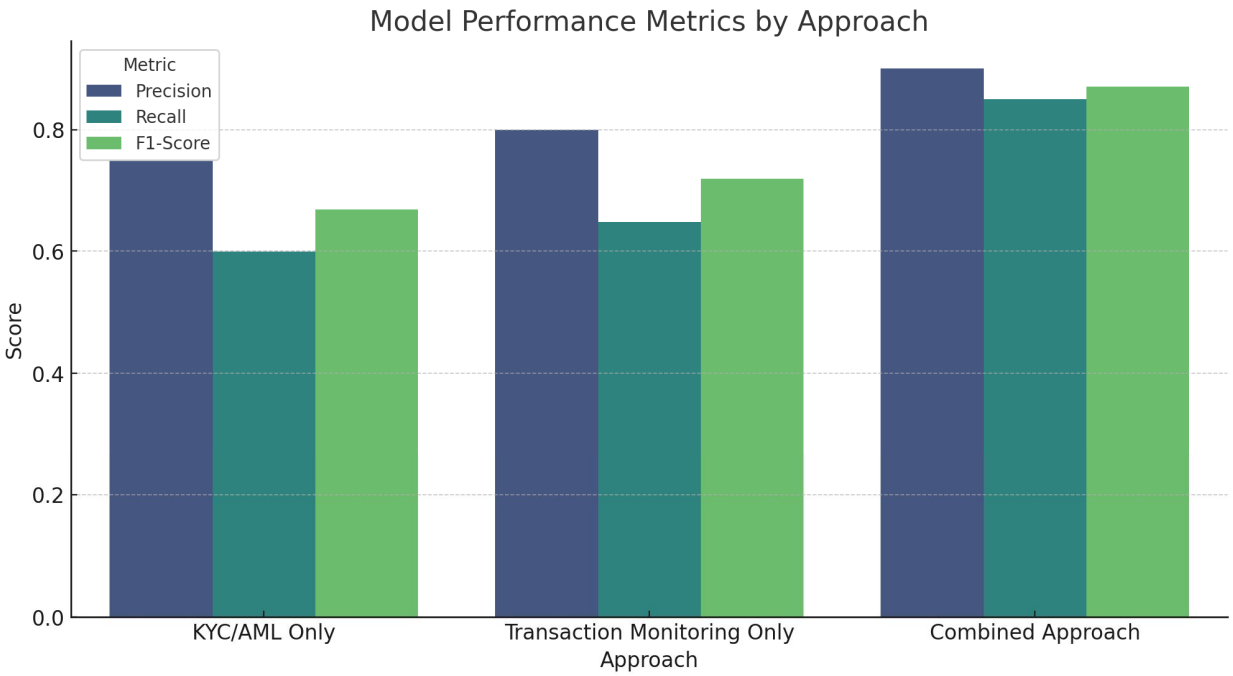

Figure 4 Model performance metrics by Approach

Figure 3 and Figure 4 illustrate the comparative effectiveness study results for Hypothesis 4, which posits that integrating KYC/AML compliance with transaction monitoring more effectively mitigates financial crimes than using either approach alone. The analysis involved using machine learning models to evaluate the detection and prevention rates of financial crimes across three approaches: KYC/AML only, transaction monitoring only, and the combined approach.

Table 6 presents the results of this comparative study. The combined approach detected 250 financial crimes, significantly more than KYC/AML only (150) and transaction monitoring only (180). This indicates that the combined approach is more effective in identifying financial crimes. Figure 3 shows the number of financial crimes detected by each approach and the model performance metrics (precision, recall, and F1-score) for each approach. The combined approach has the highest precision (0.90), recall (0.85), and F1-score (0.87). This suggests that integrating KYC/AML compliance with transaction monitoring not only detects more financial crimes but also does so with greater accuracy and efficiency. Figure 4 further illustrates the model performance metrics. The precision metric measures the proportion of correctly identified financial crimes among all detected cases, with the combined approach achieving the highest precision. Recall measures the proportion of actual financial crimes that were correctly identified, with the combined approach again showing the highest recall. The F1-score, which balances precision and recall, is highest for the combined approach, indicating overall superior performance.

Together, the results from Figures 3 and 4, along with Table 6, support Hypothesis 4 by demonstrating that integrating KYC/AML compliance with transaction monitoring significantly enhances the detection and prevention of financial crimes compared to using either approach alone. This underscores the importance of a comprehensive strategy that combines both compliance measures and transaction monitoring to effectively mitigate financial crime risks in stablecoin transactions.

Discussion

The study shows a statistically significant decrease in the rate of new stablecoin launches, suggesting that strict regulations can stifle innovation. However, the increase in adoption rates post-regulation highlights a paradox where user trust and market stability are enhanced despite reduced innovation. This dichotomy aligns with Bullmann et al.'s assertion that while regulations might impose constraints, they also bring about operational efficiencies and increased user confidence by reducing volatility and enhancing compliance [12][13][14]. This indicates that the trade-off between innovation and stability is a critical consideration for policymakers. Also, the study reveals a strong positive correlation between sentiment scores and adoption rates. Sentiment analysis of user feedback shows that higher sentiment scores, indicative of positive user perceptions of governance measures, are associated with increased adoption rates. The Pearson correlation coefficient of 0.85 underscores the importance of effective governance in building user trust. This finding resonates with the literature, which emphasizes that transparent and robust information governance frameworks are crucial for fostering user confidence and driving adoption in the cryptocurrency market [28][29][30]. The positive relationship between governance and adoption rates indicates that enhancing information governance could be a strategic priority for stablecoin issuers to gain user trust and expand their market reach.

The findings further reveal that stablecoins with high anonymity features have significantly higher odds of being involved in financial crimes, with an odds ratio of 12.18. This aligns with studies highlighting the risks associated with pseudonymity in cryptocurrencies, which facilitate illicit activities such as money laundering and fraud [47][48]. The literature underscores the necessity for regulatory frameworks that can balance privacy with security to mitigate these risks [57][58]. The strong association between anonymity and financial crimes suggests that reducing anonymity features or enhancing monitoring mechanisms could be effective in mitigating financial crime risks in stablecoin transactions. The comparative effectiveness study shows that the combined approach of KYC/AML compliance and transaction monitoring detects significantly more financial crimes and does so with higher precision, recall, and F1-score compared to using either approach individually. This demonstrates the enhanced effectiveness of a comprehensive strategy that integrates multiple governance

measures. The literature supports this integrated approach, indicating that combining regulatory compliance with advanced technological solutions like AI-driven transaction monitoring can significantly enhance the detection and prevention of financial crimes [63][64][65]. This finding underscores the need for a multi-faceted governance strategy that leverages both regulatory frameworks and technological innovations to ensure the integrity and security of stablecoin transactions

5. Conclusion and Recommendation

This study systematically investigates the role of information governance in mitigating financial crime risks in stablecoin transactions, utilizing various analytical techniques and data sources to ensure comprehensive evaluation. The findings reveal that strict information governance regulations result in a significant reduction in the number of new stablecoin launches, indicating a potential stifling of innovation within the market. However, these regulations simultaneously enhance user trust and adoption rates, reflecting increased market stability and reliability. This dual outcome suggests that while innovation may be curtailed, the overall stability and trust in stablecoin transactions improve, aligning with the notion that regulations provide a safer and more reliable environment for users. The sentiment analysis of user feedback reveals that effective governance measures significantly enhance user perceptions, leading to greater adoption of stablecoins. This underscores the importance of implementing comprehensive governance frameworks that foster user confidence and drive market adoption. The study further found a substantial increase in the likelihood of financial crimes in high-anonymity stablecoins, highlighting the inherent risks associated with these features. This finding aligns with the literature, emphasizing the need for regulatory frameworks that balance the privacy benefits of anonymity with the security requirements to prevent financial crimes. Finally, integrating KYC/AML compliance with transaction monitoring significantly enhances the effectiveness of financial crime mitigation compared to standalone approaches. The comparative effectiveness study shows that the combined approach detects more financial crimes with higher precision, recall, and F1-score. This finding highlights the critical need for a comprehensive strategy that leverages both regulatory compliance and advanced technological solutions to effectively mitigate financial crime risks in stablecoin transactions. Based on these findings, the study recommends that:

1. Policymakers and regulatory authorities should adopt comprehensive information governance frameworks that strike a balance between fostering innovation and ensuring market stability and security, thereby enhancing user trust and compliance in stablecoin transactions.

2. Financial institutions and stablecoin issuers should employ a combined approach of integrating KYC/AML compliance with advanced transaction monitoring technologies, using AI and machine learning to improve precision and reliability in detecting financial crimes.

3. Regulatory bodies should develop frameworks that address the risks associated with high-anonymity stablecoins, crafting policies that balance the need for user privacy with robust security measures to deter financial crimes and maintain user trust.

4. To ensure the effective implementation of information governance measures, continuous investment in digital infrastructure and capacity building is essential, including providing training programs and resources to enhance technological capabilities and data literacy among stakeholders involved in stablecoin transactions.

References

[1] L. Ante, I. Fiedler, J. M. Willruth, and F. Steinmetz, “A Systematic Literature Review of Empirical Research on Stablecoins,” *FinTech*, vol. 2, no. 1, pp. 34–47, Jan. 2023, doi: https://doi.org/10.3390/fintech2010003.

[2] P. R. Cunha, P. Melo, and H. Sebastião, “From Bitcoin to Central Bank Digital Currencies: Making Sense of the Digital Money Revolution,” *Future Internet*, vol. 13, no. 7, p. 165, Jun. 2021, doi: https://doi.org/10.3390/fi13070165.

[3] L. Elly Naghi, R. Anica Onufreiciuc, L.-E. Stanescu, and R. Felix Hodoș, “Strengthening the EU Fight Against Money Laundering to Promote Sustainable Economic Models,” *Contributions to finance and accounting*, pp. 297–318, Jan. 2023, doi: https://doi.org/10.1007/978-3-031-34082-6_12.

[4] S. Bhujel and Y. Rahulamathavan, “A Survey: Security, Transparency, and Scalability Issues of NFT’s and Its Marketplaces,” *Sensors*, vol. 22, no. 22, p. 8833, Nov. 2022, doi: https://doi.org/10.3390/s22228833.

[5] U. Kayani and F. Hasan, “Unveiling Cryptocurrency Impact on Financial Markets and Traditional Banking Systems: Lessons for Sustainable Blockchain and Interdisciplinary Collaborations,” *Journal of Risk and Financial Management*, vol. 17, no. 2, p. 58, Feb. 2024, doi: https://doi.org/10.3390/jrfm17020058.

[6] U. Anichebe, “Combating Money Laundering in an Age of Technology and Innovation,” *papers.ssrn.com*, Aug. 15, 2020. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3647610

[7] H. H. Al-Baity, “The Artificial Intelligence Revolution in Digital Finance in Saudi Arabia: A Comprehensive Review and Proposed Framework,” *Sustainability*, vol. 15, no. 18, p. 13725, Jan. 2023, doi: https://doi.org/10.3390/su151813725.

[8] C. Catalini, A. de Gortari, and N. Shah, “Some Simple Economics of Stablecoins,” *Annual Review of Financial Economics*, vol. 14, no. 1, Apr. 2022, doi: https://doi.org/10.1146/annurev-financial-111621-101151.

[9] R. Renwick and R. Gleasure, “Those who control the code control the rules: How different perspectives of privacy are being written into the code of blockchain systems,” *Journal of Information Technology*, vol. 36, no . 1, pp. 16–38, Aug. 2020, doi: https://doi.org/10.1177/0268396220944406.

[10] G. Hileman, “State of Stablecoins (2019),” *papers.ssrn.com*, Mar. 16, 2019. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3533143

[11] C. S. Adigwe, N. R. Mayeke, S. O. Olabanji, O. J. Okunleye, P. C. Joeaneke, and O. O. Olaniyi, “The Evolution of Terrorism in the Digital Age: Investigating the Adaptation of Terrorist Groups to Cyber Technologies for Recruitment, Propaganda, and Cyberattacks,” *Asian journal of economics, business and accounting*, vol. 24, no. 3, pp. 289–306, Feb. 2024, doi: https://doi.org/10.9734/ajeba/2024/v24i31287.

[12] D. Bullmann, J. Klemm, and A. Pinna, “In Search for Stability in Crypto-Assets: Are Stablecoins the Solution?,” *papers.ssrn.com*, Aug. 01, 2019. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3444847

[13] D. W. Arner, R. Auer, and J. Frost, “Stablecoins: Risks, Potential and Regulation,” *papers.ssrn.com*, Nov. 01, 2020. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3979495

[14] O. O. Olaniyi, “Ballots and Padlocks: Building Digital Trust and Security in Democracy through Information Governance Strategies and Blockchain Technologies,” *Asian Journal of Research in Computer Science*, vol. 17, no. 5, pp. 172–189, Mar. 2024, doi: https://doi.org/10.9734/ajrcos/2024/v17i5447
[15] G. Katten, “Issuing Green Bonds on the Algorand Blockchain,” *arXiv.org*, Aug. 23, 2021. https://arxiv.org/abs/2108.10344 (accessed Jun. 17, 2024).
[16] F. A. Ezeugwa, O. O. Olaniyi, J. C. Ugonnia, A. S. Arigbabu, and P. C. Joeaneke, “Artificial Intelligence, Big Data, and Cloud Infrastructures: Policy Recommendations for Enhancing Women’s Participation in the Tech-Driven Economy,” *Journal of Engineering Research and Reports*, vol. 26, no. 6, pp. 1–16, May 2024, doi: https://doi.org/10.9734/jerr/2024/v26i61158.
[17] G. Choi, “Inner Workings of Collateral-based Stablecoins and its Implications,” *SSRN Electronic Journal*, 2021, doi: https://doi.org/10.2139/ssrn.3809502.
[18] U. T. I. Igwenagu, A. A. Salami, A. S. Arigbabu, C. E. Mesode, T. O. Oladoyinbo, and O. O. Olaniyi, “Securing the Digital Frontier: Strategies for Cloud Computing Security, Database Protection, and Comprehensive Penetration Testing,” *Journal of Engineering Research and Reports*, vol. 26, no. 6, pp. 60–75, May 2024, doi: https://doi.org/10.9734/jerr/2024/v26i61162.
[19] C. Li and Y. Shen, “The potential impacts and risks of global stablecoins,” *China Economic Journal*, vol. 14, no. 1, pp. 39–51, Jan. 2021, doi: https://doi.org/10.1080/17538963.2021.1872167.
[20] O. O. Olaniyi, F. A. Ezeugwa, C. G. Okatta, A. S. Arigbabu, and P. C. Joeaneke, “Dynamics of the Digital Workforce: Assessing the Interplay and Impact of AI, Automation, and Employment Policies,” *Archives of current research international*, vol. 24, no. 5, pp. 124–139, Apr. 2024, doi: https://doi.org/10.9734/acri/2024/v24i5690.
[21] K. Sood, S. Singh, A. Behl, R. Sindhwani, S. Kaur, and V. Pereira, “Identification and prioritization of the risks in the mass adoption of artificial intelligence-driven stable coins: The quest for optimal resource utilization,” *Resources Policy*, vol. 81, p. 103235, Mar. 2023, doi: https://doi.org/10.1016/j.resourpol.2022.103235.
[22] O. O. Olaniyi, O. O. Omogoroye, F. G. Olaniyi, A. I. Alao, and T. O. Oladoyinbo, “CyberFusion Protocols: Strategic Integration of Enterprise Risk Management, ISO 27001, and Mobile Forensics for Advanced Digital Security in the Modern Business Ecosystem,” *Journal of Engineering Research and Reports*, vol. 26, no. 6, p. 32, 2024, doi: https://doi.org/10.9734/JERR/2024/v26i61160.
[23] A. Ferreira, “The Curious Case of Stablecoins—Balancing Risks and Rewards?,” *Journal of International Economic Law*, vol. 24, no. 4, pp. 755–778, Dec. 2021, doi: https://doi.org/10.1093/jiel/jgab036.
[24] O. O. Olaoye, F. U. Quadri, and O. O. Olaniyi, “Examining the Role of Trade on the Relationship between Environmental Quality and Energy Consumption: Insights from Sub Saharan Africa,” *Journal of economics, management and trade*, vol. 30, no. 6, pp. 16–35, Apr. 2024, doi: https://doi.org/10.9734/jemt/2024/v30i61211.
[25] T. Puschmann and P. Michael, “Financial System,” *Springer Link*, pp. 123–158, Jan. 2024, doi: https://doi.org/10.1007/978-3-031-55700-2_5.
[26] A. Alamsyah and S. Syahrir, “A Taxonomy on Blockchain-Based Technology in the Financial Industry: Drivers, Applications, Benefits, and Threats,” *Springer Link*, pp. 91–129, Jan. 2024, doi: https://doi.org/10.1007/978-3-031-50028-2_4.

[27] A. A. Salami, U. T. I. Igwenagu, C. E. Mesode, O. O. Olaniyi, and O. B. Oladoyinbo, “Beyond Conventional Threat Defense: Implementing Advanced Threat Modeling Techniques, Risk Modeling Frameworks and Contingency Planning in the Healthcare Sector for Enhanced Data Security,” *Journal of Engineering Research and Reports*, vol. 26, no. 5, pp. 304–323, Apr. 2024, doi: https://doi.org/10.9734/jerr/2024/v26i51156.
[28] M. Roussy and M. Rodrigue, “Internal Audit: Is the ‘Third Line of Defense’ Effective as a Form of Governance? An Exploratory Study of the Impression Management Techniques Chief Audit Executives Use in Their Annual Accountability to the Audit Committee,” *Journal of Business Ethics*, vol. 151, no. 3, pp. 853–869, Jul. 2016, doi: https://doi.org/10.1007/s10551-016-3263-y.
[29] J. C. Ugonnia, O. O. Olaniyi, F. G. Olaniyi, A. A. Arigbabu, and T. O. Oladoyinbo, “Towards Sustainable IT Infrastructure: Integrating Green Computing with Data Warehouse and Big Data Technologies to Enhance Efficiency and Environmental Responsibility,” *Journal of Engineering Research and Reports*, vol. 26, no. 5, pp. 247–261, Apr. 2024, doi: https://doi.org/10.9734/jerr/2024/v26i51151.
[30] H. Hassani and S. MacFeely, “Driving Excellence in Official Statistics: Unleashing the Potential of Comprehensive Digital Data Governance,” *Big Data and Cognitive Computing*, vol. 7, no. 3, p. 134, Sep. 2023, doi: https://doi.org/10.3390/bdcc7030134.
[31] S. Bakare, N. Adekunle, C. Uzoamaka Akpuokwe, and N. Emmanuella Eneh, “DATA PRIVACY LAWS AND COMPLIANCE: A COMPARATIVE REVIEW OF THE EU GDPR AND USA REGULATIONS,” *Computer science & IT research journal*, vol. 5, no. 3, pp. 528–543, Mar. 2024, doi: https://doi.org/10.51594/csitrj.v5i3.859.
[32] T. O. Oladoyinbo, S. O. Olabanji, O. O. Olaniyi, O. O. Adebiyi, O. J. Okunleye, and A. I. Alao, “Exploring the Challenges of Artificial Intelligence in Data Integrity and its Influence on Social Dynamics,” *Asian Journal of Advanced Research and Reports*, vol. 18, no. 2, pp. 1–23, Jan. 2024, doi: https://doi.org/10.9734/ajarr/2024/v18i2601.
[33] A. Hairudin, I. M. Sifat, A. Mohamad, and Y. Yusof, “Cryptocurrencies: A survey on acceptance, governance and market dynamics,” *International Journal of Finance & Economics*, vol. 27, no. 4, Dec. 2020, doi: https://doi.org/10.1002/ijfe.2392.
[34] T. Sharma, V. C. Nair, H. Wang, Y. Wang, and D. Song, “‘I Can’t Believe It’s Not Custodial!’: Usable Trustless Decentralized Key Management,” *ACM Digital Library*, vol. 581, May 2024, doi: https://doi.org/10.1145/3613904.3642464.
[35] A. D. Samuel-Okon and O. O. Abejide, “Bridging the Digital Divide: Exploring the Role of Artificial Intelligence and Automation in Enhancing Connectivity in Developing Nations,” *Journal of Engineering Research and Reports*, vol. 26, no. 6, pp. 165–177, May 2024, doi: https://doi.org/10.9734/jerr/2024/v26i61170.
[36] X. Chen, S. He, L. Sun, Y. Zheng, and C. Q. Wu, “A Survey of Consortium Blockchain and Its Applications,” *Cryptography*, vol. 8, no. 2, p. 12, Jun. 2024, doi: https://doi.org/10.3390/cryptography8020012.
[37] G. Kondova and R. Barba, “Governance of Decentralized Autonomous Organizations,” *Ssrn.com*, 2019. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3549469 (accessed Jun. 17, 2024).
[38] C. S. Adigwe, O. O. Olaniyi, S. O. Olabanji, O. J. Okunleye, N. R. Mayeke, and S. A. Ajayi, “Forecasting the Future: The Interplay of Artificial Intelligence, Innovation, and Competitiveness and its Effect on the Global Economy,” *Asian journal of economics,*

business and accounting, vol. 24, no. 4, pp. 126–146, Feb. 2024, doi: https://doi.org/10.9734/ajeba/2024/v24i41269.
[39] M. Aquilina, J. Frost, and A. Schrimpf, “Decentralized Finance (DeFi): A Functional Approach,” *Journal of Financial Regulation*, vol. 10, no. 1, Jan. 2024, doi: https://doi.org/10.1093/jfr/fjad013.
[40] A. T. Arigbabu, O. O. Olaniyi, C. S. Adigwe, O. O. Adebiyi, and S. A. Ajayi, “Data Governance in AI - Enabled Healthcare Systems: A Case of the Project Nightingale,” *Asian Journal of Research in Computer Science*, vol. 17, no. 5, pp. 85–107, Mar. 2024, doi: https://doi.org/10.9734/ajrcos/2024/v17i5441.
[41] A. Boyko, T. Dotscenko, and Yu. Dolia, “PATTERNS OF FINANCIAL CRIMES USING CRYPTOCURRENCIES,” *Socio-economic relations in the digital society*, vol. 2, no. 44, pp. 23–28, Jul. 2022, doi: https://doi.org/10.55643/ser.2.44.2022.454.
[42] W. Gaviyau and A. Bongani Sibindi, “Global Anti-Money Laundering and Combating Terrorism Financing Regulatory Framework: A Critique,” *Mdpi*, vol. 16, no. 7, pp. 313–313, Jun. 2023, doi: https://doi.org/10.3390/jrfm16070313.
[43] M. C. Șcheau, S. L. Crăciunescu, I. Brici, and M. V. Achim, “A Cryptocurrency Spectrum Short Analysis,” *Journal of Risk and Financial Management*, vol. 13, no. 8, p. 184, Aug. 2020, doi: https://doi.org/10.3390/jrfm13080184.
[44] N. Schwarz *et al.*, *Virtual Assets and Anti-Money Laundering and Combating the Financing of Terrorism (1): Some Legal and Practical Considerations*. International Monetary Fund, 2021. Accessed: Jun. 17, 2024. [Online]. Available: https://books.google.com/books?hl=en&lr=&id=WxVNEAAAQBAJ&oi=fnd&pg=PP6&dq=Financing+of+Terrorism+is+also+made+possible+because+of+its+pseudonymous+nature
[45] S. A. Ibrahim, “Regulating Cryptocurrencies to Combat Terrorism-Financing and Money Laundering,” *Stratagem*, vol. 2, no. 1, Jun. 2019, Available: http://journal.cscr.pk/stratagem/index.php/stratagem/article/view/38
[46] Y. A. Marquis, T. O. Oladoyinbo, S. O. Olabanji, O. O. Olaniyi, and S. S. Ajayi, “Proliferation of AI Tools: A Multifaceted Evaluation of User Perceptions and Emerging Trend,” *Asian Journal of Advanced Research and Reports*, vol. 18, no. 1, pp. 30–35, Jan. 2024, doi: https://doi.org/10.9734/ajarr/2024/v18i1596.
[47] S. Kethineni and Y. Cao, “The Rise in Popularity of Cryptocurrency and Associated Criminal Activity,” *International Criminal Justice Review*, vol. 30, no. 3, pp. 325–344, Feb. 2019, doi: https://doi.org/10.1177/1057567719827051.
[48] N. R. Mayeke, A. T. Arigbabu, O. O. Olaniyi, O. J. Okunleye, and C. S. Adigwe, “Evolving Access Control Paradigms: A Comprehensive Multi-Dimensional Analysis of Security Risks and System Assurance in Cyber Engineering. ,” vol. 17, no. 5, pp. 108–124, 2024, doi: https://doi.org/10.9734/ajrcos/2024/v17i5442.
[49] K. Werbach, “Trust, but Verify: Why the Blockchain Needs the Law,” *Berkeley Technology Law Journal*, vol. 33, no. 2, pp. 487–550, 2018, Available: https://www.jstor.org/stable/26533144
[50] A. A. Puglisi, “Evolving Regulatory Frameworks: Blockchain as a Form of Trust—Comparative Evidence,” *Law, governance and technology series*, vol. 47, pp. 211–232, Jan. 2022, doi: https://doi.org/10.1007/978-3-030-88036-1_9.
[51] S. O. Olabanji, “AI for Identity and Access Management (IAM) in the Cloud: Exploring the Potential of Artificial Intelligence to Improve User Authentication,

Authorization, and Access Control within Cloud-Based Systems," *Asian Journal of Research in Computer Science*, vol. 17, no. 3, pp. 38–56, 2024, doi: https://doi.org/10.9734/ajrcos/2024/v17i3423.
[52] P. Ostercamp, "Stablecoin Regulation: EU, UK and US Perspectives," *papers.ssrn.com*, Jan. 10, 2022. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4038843
[53] C. Wronka, "Crypto-asset activities and markets in the European Union: issues, challenges and considerations for regulation, supervision and oversight," *Journal of Banking Regulation*, vol. 25, Apr. 2023, doi: https://doi.org/10.1057/s41261-023-00217-8.
[54] S. O. Olabanji, Y. A. Marquis, C. S. Adigwe, A. S. Abidemi, T. O. Oladoyinbo, and O. O. Olaniyi, "AI-Driven Cloud Security: Examining the Impact of User Behavior Analysis on Threat Detection," *Asian Journal of Research in Computer Science*, vol. 17, no. 3, pp. 57–74, Jan. 2024, doi: https://doi.org/10.9734/ajrcos/2024/v17i3424.
[55] E. Hrnjic and G. Clarke, "National study on central bank digital currency and stablecoin in the Maldives," *repository.unescap.org*, 2022, Available: https://repository.unescap.org/handle/20.500.12870/4758
[56] O. O. Olaniyi, O. J. Okunleye, and S. O. Olabanji, "Advancing Data-Driven Decision-Making in Smart Cities through Big Data Analytics: A Comprehensive Review of Existing Literature," *Current Journal of Applied Science and Technology*, vol. 42, no. 25, pp. 10–18, Aug. 2023, doi: https://doi.org/10.9734/cjast/2023/v42i254181.
[57] S. M. B. M. Moreno, J.-M. Seigneur, and G. Gotzev, "A Survey of KYC/AML for Cryptocurrencies Transactions," *www.igi-global.com*, 2021. https://www.igi-global.com/chapter/a-survey-of-kycaml-for-cryptocurrencies-transactions/261722
[58] O. O. Olaniyi and D. S. Omubo, "The Importance of COSO Framework Compliance in Information Technology Auditing and Enterprise Resource Management," *International journal of innovative research and development*, Jun. 2023, doi: https://doi.org/10.24940/ijird/2023/v12/i5/may23001.
[59] Y. Kwon, J. Kim, Y. Kim, and D. Song, "The Trilemma of Stablecoin," *papers.ssrn.com*, Sep. 04, 2021. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3917430
[60] O. O. Olaniyi, C. U. Asonze, S. A. Ajayi, S. O. Olabanji, and C. S. Adigwe, "A Regressional Study on the Impact of Organizational Security Culture and Transformational Leadership on Social Engineering Awareness among Bank Employees: The Interplay of Security Education and Behavioral Change," *Asian Journal of Economics, Business and Accounting*, vol. 23, no. 23, pp. 128–143, Dec. 2023, doi: https://doi.org/10.9734/ajeba/2023/v23i231176.
[61] O. O. Olaniyi, S. O. Olabanji, and O. J. Okunleye, "Exploring the Landscape of Decentralized Autonomous Organizations: A Comprehensive Review of Blockchain Initiatives," *Journal of Scientific Research and Reports*, vol. 29, no. 9, pp. 73–81, Sep. 2023, doi: https://doi.org/10.9734/jsrr/2023/v29i91786.
[62] T. Dhar, "Stablecoins Ecosystem: A Promise That Can Be Kept," *papers.ssrn.com*, Jan. 25, 2020. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3581876
[63] J. Scharfman, "Anti-Money Laundering Compliance for Cryptocurrencies," *Cryptocurrency Compliance and Operations*, pp. 91–114, Nov. 2021, doi: https://doi.org/10.1007/978-3-030-88000-2_5

[64] D. Goldbarsht and L. deKoker, “Financial Technologies and Financial Crime: Key Developments and Areas for Future Research,” *Springer Link*, vol. 47, pp. 303–320, Jan. 2022, doi: https://doi.org/10.1007/978-3-030-88036-1_13
[65] O. O. Olaniyi, O. J. Okunleye, S. O. Olabanji, C. U. Asonze, and S. A. Ajayi, “IoT Security in the Era of Ubiquitous Computing: A Multidisciplinary Approach to Addressing Vulnerabilities and Promoting Resilience,” *Asian Journal of Research in Computer Science*, vol. 16, no. 4, pp. 354–371, Dec. 2023, doi: https://doi.org/10.9734/ajrcos/2023/v16i4397
[66] A. Kumar Singh, S. Saxena, and V. Shukla, “Analysis of Futuristic Currency: Facebook’s Libra,” *Lecture notes in networks and systems*, vol. 918, pp. 527–542, Jan. 2024, doi: https://doi.org/10.1007/978-981-97-0641-9_36
[67] D. Darwish, “Blockchain and Artificial Intelligence for Business Transformation Toward Sustainability,” *Studies in Big Data*, vol. 119, pp. 211–255, 2023, doi: https://doi.org/10.1007/978-981-19-8730-4_8
[68] B. F. G. Fabrègue and A. Bogoni, “Privacy and Security Concerns in the Smart City,” *Smart Cities*, vol. 6, no. 1, pp. 586–613, Feb. 2023, doi: https://doi.org/10.3390/smartcities6010027.