African Multidisciplinary Scholarship Journal (AMSJ)

Volume 1, Issue 1

journal homepage https://ijcsacademia.com/index.php/amsj

Artificial Intelligence Techniques and Cryptocurrency Fraud Detection in Kenya: A Systematic Literature Review Using the PRISMA Framework

Charles Guandaru Kamau[1]*

[1]Department of Accounting and Finance, School of Business, Technical University of Mombasa

*Corresponding author

Key Words
Artificial Intelligence, Cryptocurrency Fraud Detection, Machine Learning, Blockchain Analytics, Kenya

DOI:
10.59413/amsj/v1.i1.6

Published on:
1st August 2026

Abstract

The increasing adoption of cryptocurrencies has created new opportunities for digital financial innovation while simultaneously exposing individuals and institutions to sophisticated forms of financial fraud. Conventional rule-based fraud detection systems have become inadequate in addressing the dynamic and complex nature of blockchain-enabled financial crimes, leading to growing interest in the application of artificial intelligence (AI). This study systematically reviews the literature on artificial intelligence techniques for cryptocurrency fraud detection, with particular emphasis on their relevance to the Kenyan digital financial ecosystem. The review was conducted using the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) 2020 framework. Peer-reviewed studies published between 2020 and 2026 were identified from Scopus, Web of Science, IEEE Xplore, ScienceDirect, SpringerLink, and Google Scholar. Following the screening and eligibility assessment, 19 studies were included in the final qualitative synthesis. The findings reveal that machine learning, deep learning, hybrid AI models, and blockchain analytics significantly enhance cryptocurrency fraud detection by improving anomaly detection, transaction monitoring, predictive accuracy, and anti-money laundering compliance. Compared with traditional rule-based approaches, AI techniques provide faster, more adaptive, and scalable solutions capable of detecting evolving fraud patterns in decentralized financial systems. However, the review also identifies challenges relating to limited high-quality datasets, algorithmic bias, lack of explainability, cybersecurity risks, privacy concerns, and inadequate regulatory frameworks, particularly within developing economies. Furthermore, the review highlights a scarcity of empirical research focusing on cryptocurrency fraud detection in Kenya and identifies opportunities for developing localized datasets, explainable AI models, and context-specific regulatory frameworks. The study concludes that artificial intelligence has considerable potential to strengthen cryptocurrency fraud detection and financial security in Kenya, provided that technological, ethical, and regulatory challenges are adequately addressed. The findings provide valuable insights for researchers, financial institutions, technology developers, and policymakers seeking to enhance AI-driven fraud prevention within the country's evolving digital financial ecosystem.

1. INTRODUCTION

The rapid advancement of digital technologies has transformed the global financial landscape, with cryptocurrencies emerging as a significant innovation in digital finance. Unlike conventional financial systems that rely on central authorities such as banks and governments, cryptocurrencies operate on blockchain technology, a decentralized digital ledger that records transactions securely and transparently. Since the introduction of Bitcoin in 2009, cryptocurrencies such as Ethereum, Binance Coin, and Solana have gained widespread acceptance for investment, cross-border payments, and decentralized financial services.

However, the decentralized, borderless, and pseudonymous nature of cryptocurrencies has also created opportunities for cybercriminals to engage in fraudulent activities, including phishing attacks, Ponzi schemes, fake investment platforms, money laundering, ransomware payments, wallet theft, and market manipulation. These emerging threats have increased the need for more intelligent and adaptive fraud detection mechanisms capable of identifying increasingly sophisticated financial crimes (Sabry et al., 2020; Hussaini et al., 2022).

Conventional fraud detection approaches largely depend on predefined rules, manual monitoring, and threshold-based systems to identify suspicious transactions. Although these methods remain useful for detecting known fraud patterns, they often fail to recognize complex or previously unseen fraudulent activities occurring within dynamic blockchain networks. Cryptocurrency transactions generate massive volumes of data at high speed, making manual investigation and traditional statistical methods inadequate for effective fraud prevention. Consequently, artificial intelligence (AI) has become an important technological solution because it can process large datasets, identify hidden behavioural patterns, detect anomalies in real time, and continuously improve its predictive performance through machine learning. The transition from rule-based systems to AI-driven analytics has significantly improved the ability of financial institutions and cryptocurrency exchanges to detect and prevent fraudulent transactions before substantial financial losses occur (Kumar, 2022; Agberxonu et al., 2023).

The application of artificial intelligence in financial services has expanded considerably over the past decade. AI techniques, particularly machine learning and deep learning, are increasingly used to strengthen digital payment systems, automate risk assessment, improve customer verification, and enhance fraud detection. Agberxonu et al. (2023) argue that AI has become a major driver of innovation in financial technology by improving fraud detection accuracy while supporting financial inclusion. Similarly, Ali et al. (2026) observe that integrating artificial intelligence with blockchain technology creates intelligent financial ecosystems capable of continuously monitoring transactions, improving cybersecurity, and strengthening financial transparency. This convergence of AI and blockchain technologies has therefore become an important strategy for securing decentralized financial systems against emerging cyber threats.

Machine learning has become one of the most widely adopted artificial intelligence techniques for cryptocurrency fraud detection because of its ability to learn from historical transaction data and identify suspicious behavioural patterns. Supervised learning algorithms, including Random Forest, Support Vector Machines, Decision Trees, Logistic Regression, and Extreme Gradient Boosting (XGBoost), have demonstrated high levels of accuracy in classifying legitimate and fraudulent cryptocurrency transactions. In addition, unsupervised learning methods such as clustering and anomaly detection algorithms enable the identification of unusual transaction patterns where labelled datasets are unavailable (Kumar, 2022). These capabilities allow AI systems to detect emerging fraud schemes that conventional monitoring systems may overlook.

Recent studies further demonstrate the growing effectiveness of deep learning techniques in cryptocurrency fraud detection. Kamisetty et al. (2021) found that deep neural networks outperform several traditional machine learning algorithms in detecting fraudulent Bitcoin transactions because they automatically learn complex transaction characteristics without requiring extensive manual feature engineering. Likewise, Dutta et al. (2023) developed the ChaosNet model for Ethereum fraud prediction and reported improved fraud detection accuracy with lower false positive rates. These findings suggest that deep learning models are particularly suitable for analysing the complex transaction networks associated with blockchain-based financial systems.

Beyond predictive modelling, researchers have increasingly explored the integration of artificial intelligence with blockchain analytics to strengthen cryptocurrency security. Balusamy and Rengasamy (2025) argue that AI-powered blockchain technology enables continuous monitoring of cryptocurrency transactions, automated verification of smart contracts, and rapid identification of suspicious financial activities. Similarly, Ali et al. (2026) emphasize that intelligent blockchain systems improve financial security by combining the transparency of blockchain with the adaptive learning capabilities of artificial intelligence. Together, these technologies provide stronger protection against increasingly sophisticated cryptocurrency fraud schemes.

Several recent review studies have synthesized evidence regarding the application of artificial intelligence in cryptocurrency fraud detection and financial compliance. Rodríguez Valencia et al. (2025) found that AI significantly enhances compliance monitoring, anti-money laundering initiatives, and fraud detection through advanced anomaly detection and predictive analytics. However, the authors also highlight important challenges relating to algorithm transparency, explainability, and regulatory compliance. Likewise, Yahia et al. (2026), in a systematic review and bibliometric analysis, report a substantial increase in research examining artificial intelligence, blockchain technology, and cryptocurrency security. Their findings identify machine learning, cybersecurity, blockchain analytics, and explainable AI as emerging research priorities that are likely to shape future developments in cryptocurrency fraud prevention.

The increasing adoption of artificial intelligence in fraud detection has also been demonstrated across broader financial systems. Ampumuza et al. (2026), in their systematic review of AI-driven fraud detection in Savings and Credit Cooperative Organizations (SACCOs), conclude that machine learning techniques substantially improve the detection of suspicious financial transactions compared to conventional auditing approaches. Similarly, Osei-Dwomoh and Forkuo (2026) observe that artificial intelligence is transforming African economies by enhancing financial innovation and organizational performance. Nevertheless, they caution that AI implementation introduces ethical concerns relating to data privacy, algorithmic bias, explainability, accountability, and cybersecurity, all of which require appropriate governance frameworks to ensure responsible adoption.

Within Kenya, research on artificial intelligence has primarily focused on broader financial crimes rather than cryptocurrency fraud. Kamau and Kinyua (2025) established that AI significantly improves the detection of creative accounting tendencies among Kenyan corporations by enhancing predictive analytics and anomaly detection. Similarly, Ochieng et al. (2025) found that artificial intelligence strengthens anti-money laundering efforts in Kenyan commercial banks through improved identification of suspicious financial transactions and enhanced regulatory compliance. These studies demonstrate the growing application of AI within Kenya's financial sector and suggest that similar technologies could be extended to cryptocurrency fraud detection.

Kenya's rapid adoption of digital financial services, mobile money platforms, and fintech innovations has created favourable conditions for cryptocurrency adoption while simultaneously increasing exposure to cryptocurrency-related fraud. Despite this growing digital financial ecosystem, there is limited empirical evidence regarding the application of artificial intelligence to cryptocurrency fraud detection within the Kenyan context. Existing studies largely focus on algorithm development using datasets from developed economies, with comparatively little attention given to implementation challenges, regulatory readiness, ethical considerations, and the suitability of AI techniques for developing countries. Furthermore, no comprehensive systematic literature review has synthesized current evidence on artificial intelligence techniques for cryptocurrency fraud detection from a Kenyan perspective.

This study therefore seeks to address this knowledge gap by systematically reviewing recent literature on artificial intelligence techniques applied to cryptocurrency fraud detection using the PRISMA framework. By synthesizing evidence on machine learning, deep learning, blockchain analytics, implementation challenges, and future research directions, the review aims to provide insights that will inform researchers, financial institutions, regulators, and policymakers on the potential application of artificial intelligence in strengthening cryptocurrency fraud detection within Kenya's evolving digital financial ecosystem.

1.2 Problem Statement

The rapid growth of cryptocurrencies has transformed digital financial transactions by offering decentralized, secure, and efficient payment and investment platforms. However, this growth has been accompanied by an increase in cryptocurrency-related fraud, including phishing attacks, Ponzi schemes, fake investment platforms, wallet theft, ransomware payments, market manipulation, and money laundering. The decentralized and pseudonymous nature of blockchain transactions makes fraudulent activities difficult to detect using conventional rule-based fraud detection systems, thereby increasing financial losses and undermining trust in cryptocurrency markets (Hussaini et al., 2022; Sabry et al., 2020).

Artificial intelligence has emerged as a promising solution for addressing these challenges because of its ability to analyse large volumes of transaction data, identify hidden behavioural patterns, detect anomalies in real time, and continuously adapt to evolving fraud techniques. Existing studies demonstrate that machine learning, deep learning, and blockchain analytics significantly improve the accuracy and efficiency of cryptocurrency fraud detection compared to traditional approaches (Dutta et al., 2023; Kamisetty et al., 2021; Balusamy & Rengasamy, 2025). Recent systematic reviews further confirm the growing application of AI in cryptocurrency compliance and fraud prevention while highlighting emerging issues related to algorithm transparency, explainability, ethical governance, and regulatory compliance (Rodríguez Valencia et al., 2025; Yahia et al., 2026).

Despite these advancements, the existing body of knowledge exhibits several important gaps. First, most studies have been conducted in developed economies using data from international cryptocurrency exchanges, limiting the applicability of their findings to developing countries such as Kenya. Second, local studies on artificial intelligence have concentrated primarily on creative accounting and anti-money laundering within conventional financial institutions rather than cryptocurrency fraud (Kamau & Kinyua, 2025; Ochieng et al., 2025). Third, there is no comprehensive systematic literature review that synthesizes current evidence on artificial intelligence techniques for cryptocurrency fraud detection while examining their relevance to Kenya's digital financial environment. This knowledge gap limits the availability of consolidated evidence to guide researchers, financial institutions, regulators, and policymakers in selecting appropriate AI techniques for combating cryptocurrency fraud. Therefore, this study seeks to systematically review existing literature using the PRISMA framework to synthesize current evidence, identify research gaps, and provide recommendations for advancing artificial intelligence-driven cryptocurrency fraud detection in Kenya.

1.3 Research Objectives

General Objective

To systematically review the existing literature on artificial intelligence techniques for cryptocurrency fraud detection and evaluate their applicability to the Kenyan digital financial ecosystem using the PRISMA framework.

Specific Objectives

The study seeks to:

- To identify the artificial intelligence techniques applied in cryptocurrency fraud detection.
- To examine the effectiveness of artificial intelligence techniques in detecting cryptocurrency fraud.
- To identify the challenges associated with the implementation of artificial intelligence techniques for cryptocurrency fraud detection.
- To identify research gaps and propose future research directions for the application of artificial intelligence in cryptocurrency fraud detection within the Kenyan context.1.4:

2. REVIEW METHODOLOGY

This study adopted a systematic literature review methodology guided by the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) 2020 framework to ensure a transparent, rigorous, and reproducible review process. PRISMA was selected because it provides internationally accepted guidelines for identifying, screening, selecting, appraising, and synthesizing relevant studies while minimizing selection bias. A review protocol was developed to define the research objectives, search strategy, eligibility criteria, quality assessment procedures, data extraction, and synthesis methods before the review commenced. Literature was searched from Scopus, Web of Science, IEEE Xplore, ScienceDirect, SpringerLink, and Google Scholar using combinations of keywords and Boolean operators, including

Artificial Intelligence, Machine Learning, Deep Learning, Blockchain Analytics, Cryptocurrency, Bitcoin, Ethereum, Fraud Detection, Money Laundering, and Financial Crime. The search was limited to studies published between 2020 and 2026 in English. Eligible studies included peer-reviewed journal articles, conference proceedings, systematic reviews, and scholarly book chapters that examined the application of artificial intelligence to cryptocurrency fraud detection or related financial crime domains. Editorials, opinion papers, theses, non-English publications, duplicate records, and studies unrelated to artificial intelligence or cryptocurrency fraud detection were excluded. The quality of eligible studies was assessed based on the clarity of research objectives, methodological rigor, data sources, description of AI techniques, validity of findings, and relevance to the review objectives, with only high- and moderate-quality studies included in the final synthesis. A standardized data extraction form was used to collect information on the author(s), publication year, country, research design, AI techniques, fraud application, datasets, key findings, limitations, and recommendations. The extracted data were synthesized using thematic analysis, enabling the identification of recurring themes relating to artificial intelligence techniques, their effectiveness, implementation challenges, ethical and regulatory concerns, and research gaps relevant to cryptocurrency fraud detection in Kenya.

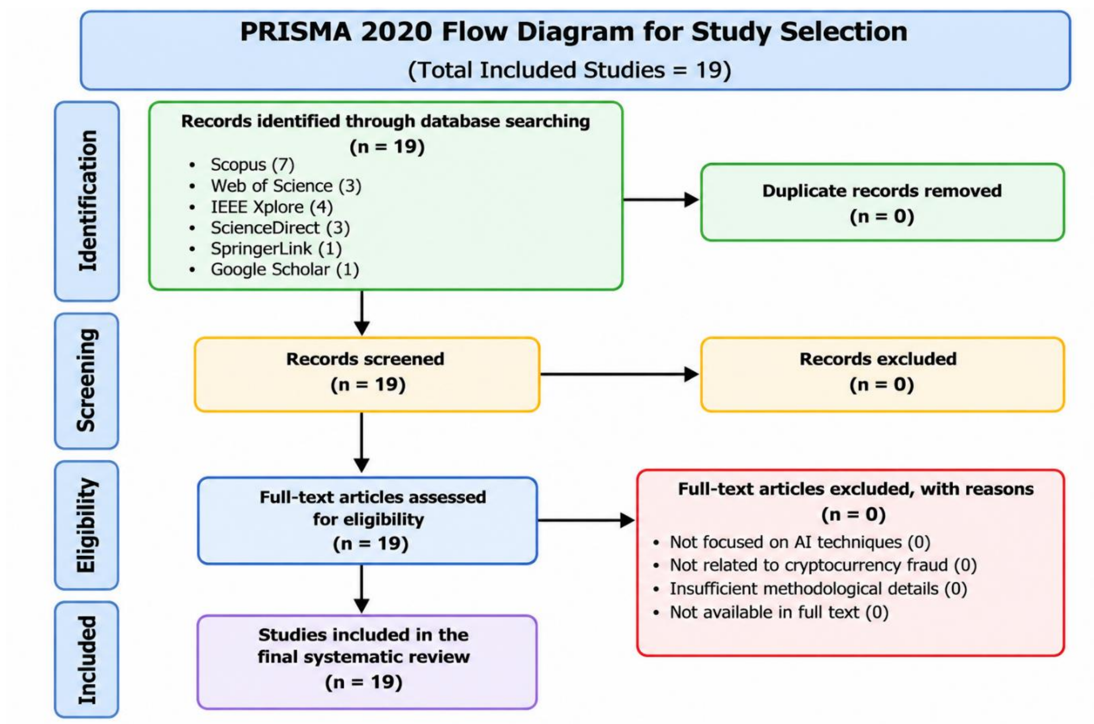

Figure 1: PRISMA 2020 flow diagram illustrating the study selection process

Figure 1 illustrates the study selection process followed in this systematic literature review using the PRISMA 2020 guidelines. It shows the sequential stages of identifying, screening, assessing eligibility, and including relevant studies. The process ensured that only studies meeting the predefined inclusion criteria were retained for the final review, resulting in 19 studies being included in the thematic synthesis. The PRISMA framework enhanced the transparency, rigor, and reproducibility of the review process by systematically documenting the reasons for study selection and exclusion.

3. RESULTS AND FINDINGS

This chapter presents the findings of the systematic literature review conducted using the PRISMA 2020 framework. The findings are synthesized from the nineteen studies that met the inclusion criteria and are organized into seven major themes aligned with the study objectives. Rather than discussing each study individually, the chapter integrates and compares evidence across the selected literature to identify common patterns, contrasting findings, emerging trends, and research gaps. The thematic synthesis focuses on the evolution of artificial intelligence (AI) in cryptocurrency fraud detection, machine learning techniques, deep learning and hybrid models, AI-enabled blockchain analytics and compliance, the effectiveness of AI techniques, implementation challenges and ethical issues, and future research directions relevant to Kenya.

3.1 Theme One: Evolution of Artificial Intelligence in Cryptocurrency Fraud Detection

The application of artificial intelligence (AI) in cryptocurrency fraud detection has evolved considerably over the past decade, driven by the rapid expansion of blockchain technologies, digital assets, and increasingly sophisticated financial crimes. Early cryptocurrency security mechanisms primarily relied on rule-based systems and manual transaction monitoring, which were effective only in identifying known fraud patterns. However, the rapid growth in cryptocurrency transactions, coupled with the emergence of decentralized finance (DeFi), anonymous wallets, and cross-border digital payments, exposed the limitations of traditional fraud detection approaches. These systems struggled to process the large volumes of blockchain transaction data and failed to detect complex or previously unseen fraudulent activities, thereby necessitating the adoption of intelligent and adaptive analytical techniques (Sabry et al., 2020; Hussaini et al., 2022).

The reviewed studies indicate that artificial intelligence has transformed cryptocurrency fraud detection from reactive investigation to proactive prediction. Sabry et al. (2020) argue that AI has become an essential component of blockchain security because it enables automated analysis of transaction networks, behavioural profiling, anomaly detection, and predictive risk assessment. Their review further highlights that the integration of AI with blockchain technology has created opportunities for developing intelligent financial systems capable of responding to emerging cyber threats in real time. Similarly, Kumar (2022) observes that advances in machine learning algorithms have significantly enhanced the ability of financial institutions and cryptocurrency exchanges to identify suspicious transactions, replacing static rule-based systems with models capable of learning continuously from historical transaction data.

The growing importance of AI is also reflected in recent systematic reviews examining cryptocurrency security and financial compliance. Rodríguez Valencia et al. (2025) report that AI applications have expanded beyond fraud detection to include regulatory compliance, anti-money laundering (AML), know-your-customer (KYC) verification, and financial risk management. Their review demonstrates that AI techniques are increasingly used to support cryptocurrency exchanges in monitoring large-scale transaction networks, identifying suspicious behavioural patterns, and improving compliance with evolving financial regulations. However, the authors also note that the increasing complexity of AI models has raised concerns regarding explainability, transparency, and accountability, emphasizing the need for responsible AI governance.

Similarly, Yahia et al. (2026), through a systematic review and bibliometric analysis, identify a significant increase in scholarly publications at the intersection of artificial intelligence, blockchain technology, and cryptocurrency security between 2020 and 2026. Their analysis reveals that machine learning, blockchain analytics, cybersecurity, fraud detection, and decentralized finance have become dominant research themes. The authors further observe that future research is shifting towards explainable AI, federated learning, privacy-preserving machine learning, and intelligent blockchain systems capable of adapting to continuously evolving fraud techniques. This trend suggests that AI is no longer viewed merely as a computational tool but as an integral component of modern financial governance.

Beyond cryptocurrency-specific research, several studies demonstrate that the evolution of AI in fraud detection has been influenced by broader developments within financial technology. Agberxonu et al. (2023) found that artificial intelligence has revolutionized digital financial services by improving fraud detection, customer authentication, credit risk analysis, and financial inclusion. Their findings suggest that AI's ability to analyse massive datasets and identify subtle behavioural anomalies has significantly improved financial security across multiple fintech applications. Likewise, Ali et al. (2026) argue that combining AI with blockchain technology enhances cybersecurity by enabling continuous transaction monitoring, intelligent smart contract verification, and automated identification of fraudulent activities. This convergence has strengthened the resilience of digital financial ecosystems while improving operational efficiency and transparency.

The reviewed literature further indicates that advances in AI have extended beyond traditional banking into decentralized financial systems. Ampumuza et al. (2026), although focusing on SACCO transactions rather than cryptocurrencies, demonstrate that machine learning models consistently outperform traditional auditing methods in identifying fraudulent financial behaviour. Their findings reinforce the growing consensus that AI provides adaptable fraud detection mechanisms capable of responding to increasingly dynamic financial environments. Similarly, Osei-Dwomoh and Forkuo (2026) observe that AI is transforming African financial systems by improving organizational performance and financial innovation, although they caution that issues relating to algorithmic bias, data privacy, cybersecurity, and ethical governance remain significant concerns that require effective regulatory oversight.

Within Kenya, the evolution of AI applications has primarily focused on conventional financial crimes. Kamau and Kinyua (2025) established that AI significantly improves the detection of creative accounting practices among Kenyan corporations through predictive analytics and anomaly detection techniques. Likewise, Ochieng et al. (2025) found that artificial intelligence strengthens anti-money laundering systems within Kenyan commercial banks by improving the identification of suspicious transactions and enhancing regulatory compliance. Although these studies do not specifically address cryptocurrency fraud, they demonstrate the increasing acceptance and application of AI within Kenya's financial sector and provide a strong foundation for extending intelligent fraud detection techniques to cryptocurrency markets.

Overall, the reviewed studies consistently demonstrate that the evolution of artificial intelligence has fundamentally transformed cryptocurrency fraud detection from traditional rule-based monitoring to intelligent predictive analytics. Advances in machine learning, deep learning, and blockchain analytics have substantially improved the speed, accuracy, and scalability of fraud detection systems while expanding their application to compliance monitoring, anti-money laundering, and cybersecurity. Nevertheless, the literature also indicates that future developments will depend not only on improving predictive performance but also on addressing issues of explainability, ethical governance, regulatory compliance, and contextual adaptation, particularly within emerging economies such as Kenya. These findings establish the foundation for examining the specific artificial intelligence techniques employed in cryptocurrency fraud detection, which is discussed in the next theme.

3.2 Theme Two: Machine Learning Techniques for Cryptocurrency Fraud Detection

Machine learning (ML) has emerged as the most widely applied artificial intelligence technique for cryptocurrency fraud detection because of its ability to analyse large volumes of blockchain transaction data, identify hidden behavioural patterns, and continuously improve prediction accuracy through experience. Unlike traditional rule-based fraud detection systems that rely on predefined conditions, machine learning algorithms automatically learn from historical data and adapt to evolving fraud strategies. The reviewed studies consistently identify machine learning as the foundation of modern cryptocurrency fraud detection systems due to its high predictive capability, scalability, and suitability for real-time transaction monitoring (Kumar, 2022; Agberxonu et al., 2023).

The literature indicates that supervised machine learning algorithms are the most frequently applied techniques for detecting fraudulent cryptocurrency transactions. These algorithms are trained using labelled datasets containing both legitimate and fraudulent transactions, enabling them to classify new transactions with considerable accuracy. Kumar (2022) reports that Decision Trees, Logistic Regression, Support Vector Machines (SVM), Random Forest, and Extreme Gradient Boosting (XGBoost) are among the most effective supervised learning algorithms used in blockchain fraud detection. These models successfully distinguish normal transaction behaviour from suspicious activities by analysing multiple transaction characteristics, including transaction frequency, wallet interactions, transaction value, and network connectivity. Their ability to identify complex nonlinear relationships has significantly improved fraud detection compared with conventional statistical methods.

Among the supervised learning models, ensemble learning techniques have received particular attention because they combine predictions from multiple algorithms to improve classification performance. Agberxonu et al. (2023) found that Random Forest and Gradient Boosting models consistently achieve high fraud detection accuracy while reducing false positive rates. Their review attributes this performance to the algorithms' ability to analyse numerous decision paths simultaneously and capture complex behavioural interactions within financial transaction data. Such capabilities are especially valuable in cryptocurrency markets, where fraudulent activities frequently mimic legitimate transaction patterns to evade detection.

In addition to supervised learning, unsupervised machine learning techniques have become increasingly important because labelled cryptocurrency fraud datasets are often limited or unavailable. Unlike supervised models, unsupervised algorithms identify unusual transaction behaviours without prior knowledge of fraud labels by detecting anomalies within blockchain transaction networks. Kumar (2022) highlights clustering techniques and anomaly detection algorithms such as Isolation Forest and K-Means clustering as effective tools for discovering suspicious wallet behaviour and previously unknown fraud schemes. These methods are particularly useful for identifying emerging fraud techniques that have not yet been incorporated into labelled training datasets, thereby enabling earlier detection of evolving cyber threats.

Several studies also demonstrate the application of specialized machine learning architectures designed specifically for blockchain transaction analysis. Dutta et al. (2023) proposed the ChaosNet model for detecting fraudulent Ethereum transactions and found that the model significantly improved prediction accuracy while reducing false positive classifications. Their findings suggest that customized machine learning architectures designed for blockchain environments outperform many conventional algorithms because they capture the unique transactional characteristics of decentralized financial networks. Similarly, Kumari (2025) reports that machine learning techniques have expanded beyond fraud detection to include cryptocurrency price prediction, scam identification, behavioural analysis, and investment risk assessment. This broader application illustrates the increasing versatility of machine learning within cryptocurrency ecosystems.

The reviewed literature further indicates that machine learning contributes significantly to regulatory compliance and anti-money laundering efforts. Rodríguez Valencia et al. (2025) observed that machine learning models are increasingly integrated into compliance systems to support Know Your Customer (KYC) verification, anti-money laundering (AML) monitoring, and suspicious transaction reporting. By continuously analysing transaction histories and identifying abnormal financial behaviour, these models enable cryptocurrency exchanges and regulatory agencies to strengthen compliance while reducing manual investigation efforts. Similarly, Ali et al. (2026) argue that integrating machine learning with blockchain technology improves financial security through automated transaction verification, intelligent monitoring, and enhanced cybersecurity, thereby reducing opportunities for financial crime within decentralized systems.

Although machine learning has demonstrated substantial success in cryptocurrency fraud detection, the reviewed studies also identify several limitations. Hussaini et al. (2022) note that the effectiveness of supervised learning algorithms depends heavily on the availability of high-quality labelled datasets, which remain scarce because many fraudulent cryptocurrency transactions are undiscovered or unreported. Consequently, models trained on incomplete datasets may fail to recognize newly emerging fraud patterns. Furthermore, Agberxonu et al. (2023) caution that machine learning models may produce biased predictions if training data are unrepresentative, while Osei-Dwomoh and Forkuo (2026) emphasize concerns regarding algorithmic transparency, fairness, and explainability, particularly where AI-generated decisions influence financial investigations and regulatory enforcement.

The Kenyan studies included in this review provide indirect evidence supporting the applicability of machine learning within cryptocurrency fraud detection. Kamau and Kinyua (2025) found that machine learning techniques significantly improve the detection of creative accounting practices through anomaly detection and predictive analytics. Likewise, Ochieng et al. (2025) established that AI-based transaction monitoring enhances anti-money laundering efforts within Kenyan commercial banks by improving the identification of suspicious financial activities. Although neither study focuses specifically on cryptocurrencies, their findings suggest that machine learning techniques have already demonstrated effectiveness within Kenya's financial sector and could be adapted to monitor cryptocurrency transactions as digital asset adoption continues to expand.

Overall, the reviewed literature demonstrates that machine learning has become the cornerstone of cryptocurrency fraud detection because of its ability to classify transactions accurately, identify anomalies, adapt to evolving fraud techniques, and support regulatory compliance. Supervised algorithms such as Random Forest, Support Vector Machines, Logistic Regression, and XGBoost remain the most widely applied approaches, while unsupervised learning methods complement them by detecting previously unknown fraud patterns. Nevertheless, challenges relating to data quality, explainability, algorithmic bias, and limited localized datasets continue to constrain the effective implementation of machine learning, particularly in emerging economies such as Kenya. These limitations have encouraged researchers to explore more sophisticated approaches, particularly deep learning and hybrid artificial intelligence models, which are discussed in the next theme.

3.3 Theme Three: Deep Learning and Hybrid Artificial Intelligence Models

Deep learning represents an advanced branch of artificial intelligence that has gained increasing attention in cryptocurrency fraud detection because of its ability to automatically learn complex features from large volumes of blockchain transaction data. Unlike conventional machine learning algorithms that often require manual feature engineering, deep learning models employ multiple hidden neural network layers to extract hierarchical patterns from highly complex datasets. The reviewed studies indicate that deep learning techniques have become particularly valuable in cryptocurrency environments, where fraud schemes continuously evolve and transaction networks exhibit intricate relationships that are difficult to capture using traditional analytical approaches (Kamisetty et al., 2021; Dutta et al., 2023).

One of the major advantages of deep learning is its ability to model nonlinear relationships among blockchain transactions. Cryptocurrency fraud frequently involves interconnected wallets, multiple transaction pathways, and sophisticated laundering techniques that cannot easily be detected through simple statistical methods. Kamisetty et al. (2021) demonstrated that deep neural networks significantly outperform several conventional machine learning algorithms in detecting fraudulent Bitcoin transactions because they automatically learn hidden behavioural characteristics from transaction histories. Their study showed that deep learning models improve fraud classification accuracy while minimizing manual intervention during feature extraction, making them particularly suitable for large-scale blockchain environments.

Similarly, Dutta et al. (2023) introduced the ChaosNet model for Ethereum fraud detection and reported superior predictive performance compared to conventional classification algorithms. The model effectively identified fraudulent transaction patterns while maintaining lower false-positive rates, an important consideration in cryptocurrency fraud detection where legitimate transactions may exhibit characteristics similar to fraudulent ones. The findings suggest that deep learning architectures designed specifically for blockchain transaction analysis are capable of capturing subtle behavioural anomalies that may remain undetected by traditional machine learning approaches.

Beyond standalone deep learning models, recent studies emphasize the emergence of hybrid artificial intelligence models that integrate multiple computational techniques to improve fraud detection performance. Rather than relying on a single algorithm, hybrid systems combine machine learning, deep learning, blockchain analytics, and other intelligent technologies to leverage the strengths of each approach. Ali et al. (2026) argue that integrating artificial intelligence with blockchain technology creates intelligent financial ecosystems capable of continuous transaction monitoring, automated smart contract verification, and enhanced cybersecurity. Such hybrid systems improve fraud detection by combining predictive analytics with blockchain's transparency and immutability, thereby increasing both detection accuracy and system resilience.

Balusamy and Rengasamy (2025) similarly demonstrate that AI-powered blockchain technology strengthens the protection of cryptocurrency networks through intelligent monitoring and automated fraud prevention mechanisms. Their study highlights the importance of combining blockchain infrastructure with advanced AI models to identify suspicious transactions in real time while reducing operational costs associated with manual fraud investigations. The authors further note that hybrid AI models provide enhanced scalability, enabling financial institutions and cryptocurrency exchanges to manage increasing transaction volumes without compromising detection performance.

The reviewed literature also indicates that hybrid AI models contribute significantly to regulatory compliance and financial governance. Rodríguez Valencia et al. (2025) found that integrating machine learning, deep learning, and blockchain analytics enhances anti-money laundering (AML) compliance, Know Your Customer (KYC) verification, and risk management by enabling continuous monitoring of cryptocurrency transactions. Likewise, Yahia et al. (2026) observed that current research increasingly focuses on combining explainable AI, blockchain analytics, federated learning, and privacy-preserving techniques to develop more transparent and accountable fraud detection systems. These developments reflect a shift from maximizing predictive accuracy alone toward building intelligent systems that are also interpretable, secure, and compliant with evolving regulatory requirements.

Despite their superior predictive capabilities, deep learning and hybrid AI models face several implementation challenges. Deep learning algorithms require substantial computational resources, extensive labelled datasets, and specialized technical expertise, making them costly to deploy and maintain. Hussaini et al. (2022) note that limited availability of high-quality cryptocurrency fraud datasets constrains model training and may reduce predictive performance. Furthermore, Osei-Dwomoh and Forkuo (2026) caution that highly complex neural networks often function as "black-box" models, making it difficult for financial institutions and regulators to understand how fraud detection decisions are reached. This lack of explainability raises concerns regarding transparency, accountability, and trust, particularly in highly regulated financial environments.

Within the Kenyan context, evidence on the application of deep learning and hybrid AI models to cryptocurrency fraud detection remains scarce. Existing studies by Kamau and Kinyua (2025) and Ochieng et al. (2025) demonstrate the successful application of AI in detecting creative accounting and money laundering within conventional financial institutions but do not examine advanced deep learning architectures or hybrid blockchain-based fraud detection systems. This suggests that while Kenya has begun adopting AI for financial crime detection, considerable opportunities remain for research into deep learning and hybrid AI models tailored to the country's rapidly growing cryptocurrency ecosystem. Overall, the reviewed literature indicates that deep learning and hybrid AI approaches represent the next generation of cryptocurrency fraud detection technologies by offering greater predictive accuracy, adaptability, and scalability. However, their successful implementation will require improved computational infrastructure, high-quality localized datasets, explainable AI frameworks, and supportive regulatory policies, particularly within emerging economies such as Kenya.

3.4 Theme Four: AI-Enabled Blockchain Analytics and Compliance

The integration of artificial intelligence with blockchain analytics has emerged as a significant advancement in cryptocurrency fraud detection by enabling continuous monitoring, intelligent transaction analysis, and regulatory compliance. While blockchain technology provides a decentralized and immutable ledger that records every transaction, it does not inherently detect fraudulent activities. Artificial intelligence complements blockchain by analysing large volumes of transactional data, identifying suspicious behavioural patterns, and generating predictive insights that support fraud prevention. The reviewed studies consistently demonstrate that combining AI with blockchain analytics enhances the capability of financial institutions, cryptocurrency exchanges, and regulatory agencies to detect, investigate, and prevent financial crimes in decentralized digital environments (Ali et al., 2026; Balusamy & Rengasamy, 2025).

One of the principal advantages of AI-enabled blockchain analytics is its ability to monitor blockchain transactions in real time. Unlike traditional financial systems, blockchain transactions are irreversible and occur continuously across distributed networks, making timely fraud detection essential. Ali et al. (2026) argue that integrating AI with blockchain technology enables automated transaction verification, behavioural profiling, and intelligent monitoring of cryptocurrency ecosystems. Their study further demonstrates that AI algorithms can identify suspicious wallet interactions, unusual transaction frequencies, and abnormal fund movements, allowing investigators to detect fraudulent activities before they escalate into significant financial losses. These capabilities significantly strengthen cybersecurity within decentralized financial systems.

The reviewed literature also indicates that blockchain analytics plays a critical role in regulatory compliance. Rodríguez Valencia et al. (2025) found that AI-driven compliance systems are increasingly employed to strengthen Anti-Money Laundering (AML) and Know Your Customer (KYC) processes within cryptocurrency exchanges. By continuously analysing blockchain transactions and customer behaviour, AI systems can identify suspicious activities that require further investigation while reducing reliance on manual compliance procedures. The authors emphasize that AI-powered compliance tools improve operational efficiency by enabling real-time risk assessment, automated transaction monitoring, and early identification of financial crimes. Consequently, AI has evolved beyond fraud detection to become an essential component of regulatory technology (RegTech) within cryptocurrency markets.

Similarly, Yahia et al. (2026) report that research at the intersection of artificial intelligence and blockchain has increasingly focused on developing intelligent compliance systems capable of supporting financial governance. Their bibliometric analysis shows growing interest in explainable AI, blockchain forensics, privacy-preserving analytics, and decentralized artificial intelligence as emerging research areas. These technologies are intended to improve the transparency and accountability of fraud detection systems while ensuring compliance with evolving financial regulations. The findings suggest that future cryptocurrency security solutions will increasingly combine predictive analytics with governance frameworks that promote responsible AI deployment.

Blockchain analytics has also enhanced the investigation of complex financial crimes by enabling the tracing of cryptocurrency transactions across multiple digital wallets and exchanges. Kumar (2022) observes that AI-powered blockchain analytics can reconstruct transaction networks, identify hidden relationships among wallet addresses, and detect sophisticated money laundering schemes that would be difficult to uncover using conventional investigative methods. Likewise, Hussaini et al. (2022) note that blockchain analytics enables investigators to monitor transaction flows across decentralized networks, thereby improving the identification of illicit financial activities such as ransomware payments, darknet transactions, and cryptocurrency-based money laundering. These capabilities demonstrate the increasing importance of blockchain analytics in supporting financial crime investigations.

The reviewed studies further reveal that integrating blockchain analytics with machine learning and deep learning enhances fraud detection performance. Balusamy and Rengasamy (2025) found that AI-powered blockchain systems improve the security of cryptocurrency networks by combining predictive analytics with the transparency and immutability of blockchain technology. Their findings indicate that hybrid AI-blockchain systems provide more accurate fraud detection while reducing operational costs associated with manual monitoring and investigation. Similarly, Dutta et al. (2023) and Kamisetty et al. (2021) demonstrate that AI models achieve higher predictive accuracy when trained using blockchain transaction data because blockchain provides comprehensive, tamper-resistant datasets that improve algorithm performance.

Despite these advantages, several implementation challenges remain. Osei-Dwomoh and Forkuo (2026) argue that AI-enabled blockchain analytics raises concerns regarding data privacy, algorithmic accountability, cybersecurity risks, and ethical governance. Although blockchain records are transparent, linking wallet addresses to individual users often presents legal and privacy challenges. Furthermore, Rodríguez Valencia et al. (2025) caution that highly complex AI models may reduce transparency if their decision-making processes cannot be adequately explained to regulators or law enforcement agencies. These concerns highlight the need for explainable AI frameworks and appropriate regulatory standards to support trustworthy implementation.

Within Kenya, the application of AI-enabled blockchain analytics remains relatively underdeveloped despite increasing adoption of digital financial services. Existing studies by Kamau and Kinyua (2025) and Ochieng et al. (2025) demonstrate the successful use of AI in detecting creative accounting and money laundering within conventional financial institutions but provide limited evidence regarding blockchain-based cryptocurrency investigations. Consequently, there remains considerable scope for developing AI-powered blockchain analytics systems tailored to Kenya's emerging cryptocurrency market. Overall, the reviewed literature indicates that integrating artificial intelligence with blockchain analytics significantly enhances cryptocurrency fraud detection, financial compliance, and cybersecurity. However, maximizing these benefits will require stronger regulatory frameworks, improved technical infrastructure, and greater emphasis on explainable and ethical AI to support secure and accountable cryptocurrency governance in Kenya.

3.5 Theme Five: Effectiveness of Artificial Intelligence Techniques in Detecting Cryptocurrency Fraud

The reviewed literature consistently demonstrates that artificial intelligence (AI) techniques are more effective than conventional rule-based systems in detecting cryptocurrency fraud because of their ability to process large volumes of transaction data, identify complex behavioural patterns, and adapt to emerging fraud strategies. Unlike traditional fraud detection methods, which depend on predefined rules and manual monitoring, AI models continuously learn from historical and real-time transaction data, enabling them to detect both known and previously unseen fraudulent activities. This adaptability has significantly improved fraud detection accuracy, reduced false positives, and enhanced the speed of identifying suspicious cryptocurrency transactions (Kumar, 2022; Agberxonu et al., 2023).

One of the key indicators of AI effectiveness is its high predictive accuracy. Several empirical studies reviewed reported that machine learning and deep learning algorithms consistently outperform traditional statistical methods in classifying legitimate and fraudulent cryptocurrency transactions. Kamisetty et al. (2021) found that deep neural networks achieved superior classification performance in detecting fraudulent Bitcoin transactions because of their ability to automatically extract complex features from blockchain transaction data. Similarly, Dutta et al. (2023) demonstrated that the ChaosNet model improved the prediction of fraudulent Ethereum transactions while significantly reducing false-positive classifications. These findings indicate that AI techniques provide more reliable fraud detection by capturing subtle behavioural patterns that conventional methods often fail to recognize.

The effectiveness of AI also stems from its capability to detect anomalies in real time. Cryptocurrency transactions occur continuously across decentralized blockchain networks, making timely fraud detection essential to minimize financial losses. Kumar (2022) observes that machine learning algorithms can analyse transaction characteristics such as transaction frequency, wallet interactions, transaction values, and network behaviour almost instantaneously, allowing suspicious activities to be identified before fraudulent transactions are completed. Likewise, Ali et al. (2026) argue that integrating AI with blockchain technology enables continuous monitoring of cryptocurrency ecosystems, thereby improving the speed and responsiveness of fraud detection systems. This real-time analytical capability represents a significant improvement over manual auditing processes, which are often reactive and time-consuming.

The reviewed studies further reveal that AI techniques improve the detection of a wide range of cryptocurrency-related financial crimes. Rodríguez Valencia et al. (2025) found that AI models effectively support fraud detection, anti-money laundering (AML), compliance monitoring, and Know Your Customer (KYC) verification by continuously analysing customer behaviour and transaction histories. Similarly, Balusamy and Rengasamy (2025) demonstrated that AI-powered blockchain systems strengthen the protection of cryptocurrency networks by detecting suspicious transaction patterns, preventing unauthorized activities, and enhancing financial security. These findings suggest that AI is increasingly becoming a comprehensive financial risk management tool rather than merely a fraud detection mechanism.

The effectiveness of AI extends beyond cryptocurrency markets into broader financial systems, providing additional evidence of its reliability. Ampumuza et al. (2026), in their review of AI-driven fraud detection within SACCOs, concluded that machine learning algorithms significantly improve the identification of fraudulent financial behaviour compared to traditional auditing methods. Likewise, Agberxonu et al. (2023) reported that AI enhances fraud detection across digital payment platforms by identifying complex transaction anomalies that conventional systems cannot easily detect. Although these studies were conducted outside cryptocurrency environments, they reinforce the broader effectiveness of AI in combating financial fraud.

Within the Kenyan context, available evidence also supports the effectiveness of AI in financial crime detection. Kamau and Kinyua (2025) found that AI techniques significantly improve the identification of creative accounting tendencies through predictive analytics and anomaly detection, while Ochieng et al. (2025) established that AI enhances anti-money laundering efforts in Kenyan commercial banks by strengthening the detection of suspicious financial transactions. Although neither study specifically addresses cryptocurrency fraud, their findings demonstrate that AI technologies are already producing positive outcomes within Kenya's financial sector and possess considerable potential for application in cryptocurrency fraud detection.

Despite the overall effectiveness of AI techniques, the reviewed studies identify several factors that influence their performance. Hussaini et al. (2022) note that the predictive accuracy of AI models depends heavily on the quality, completeness, and representativeness of training datasets. Incomplete or biased datasets may reduce model performance and increase false-positive or false-negative classifications. Similarly, Osei-Dwomoh and Forkuo (2026) argue that algorithmic bias, limited explainability, and ethical concerns may undermine user confidence and regulatory acceptance of AI-based fraud detection systems. Rodríguez Valencia et al. (2025) further emphasize that achieving high predictive accuracy alone is insufficient; AI systems must also be transparent, accountable, and compliant with financial regulations to support sustainable implementation.

Overall, the reviewed literature provides strong evidence that artificial intelligence techniques significantly improve the detection of cryptocurrency fraud by increasing prediction accuracy, enabling real-time monitoring, identifying complex transaction patterns, and strengthening regulatory compliance. Machine learning, deep learning, and hybrid AI models consistently outperform conventional fraud detection approaches across a variety of financial applications. Nevertheless, their effectiveness is influenced by data quality, computational resources, explainability, and regulatory readiness. These findings suggest that while AI has become an indispensable tool for cryptocurrency fraud detection, successful implementation requires not only technological advancement but also robust governance frameworks, high-quality datasets, and institutional capacity, particularly within emerging economies such as Kenya.

3.6 Theme Six: Challenges, Ethical Issues, and Regulatory Considerations in AI-Based Cryptocurrency Fraud Detection

Although artificial intelligence has demonstrated significant potential in improving cryptocurrency fraud detection, the reviewed literature identifies several technical, ethical, and regulatory challenges that continue to hinder its widespread adoption. These challenges include limited availability of high-quality datasets, algorithmic bias, lack of explainability, cybersecurity threats, privacy concerns, computational complexity, and inadequate regulatory frameworks. Collectively, these issues influence the reliability, transparency, and acceptance of AI-based fraud detection systems, particularly within developing economies where digital financial regulations and technological infrastructure are still evolving (Rodríguez Valencia et al., 2025; Osei-Dwomoh & Forkuo, 2026).

A major challenge highlighted across the reviewed studies is the availability and quality of training data. Artificial intelligence models rely heavily on large, representative, and accurately labelled datasets to achieve high predictive performance. However, Hussaini et al. (2022) observe that many cryptocurrency fraud datasets are incomplete because fraudulent transactions are often undiscovered, underreported, or intentionally concealed by cybercriminals. Similarly, Dutta et al. (2023) note that the dynamic nature of blockchain transactions requires continuous updating of datasets to ensure that AI models remain effective against emerging fraud patterns. Consequently, models trained on outdated or biased data may experience reduced predictive accuracy and generate higher rates of false-positive or false-negative classifications.

Another significant challenge concerns the explainability and transparency of AI models. While advanced machine learning and deep learning algorithms achieve high detection accuracy, many function as "black-box" systems whose internal decision-making processes are difficult for investigators and regulators to interpret. Rodríguez Valencia et al. (2025) argue that limited explainability reduces trust in AI-generated decisions, particularly in highly regulated financial environments where institutions must justify why a transaction has been classified as fraudulent. Yahia et al. (2026)

similarly identify explainable artificial intelligence (XAI) as one of the fastest-growing research areas because financial institutions increasingly require AI systems that provide both accurate predictions and understandable explanations to support regulatory compliance and operational accountability.

Ethical concerns also feature prominently in the reviewed literature. Osei-Dwomoh and Forkuo (2026) caution that artificial intelligence may inadvertently reinforce algorithmic bias if training datasets are unbalanced or unrepresentative of diverse transaction behaviours. Biased algorithms may incorrectly classify legitimate transactions as fraudulent or disproportionately target certain users or transaction patterns, leading to unfair outcomes and potential discrimination. Furthermore, AI systems frequently process sensitive financial and personal data, raising concerns regarding data privacy, informed consent, and compliance with data protection regulations. These ethical considerations underscore the need for responsible AI governance frameworks that balance fraud prevention with individual rights and privacy protection.

Cybersecurity and adversarial threats present another important challenge. As AI-based fraud detection systems become more sophisticated, cybercriminals are also developing advanced techniques to evade detection. Ali et al. (2026) observe that attackers increasingly exploit weaknesses in machine learning models through adversarial attacks designed to manipulate AI predictions or disguise fraudulent transactions as legitimate activities. Likewise, Balusamy and Rengasamy (2025) argue that although integrating AI with blockchain technology strengthens cybersecurity, continuous system updates and proactive threat monitoring remain essential because fraud techniques evolve rapidly. These findings suggest that AI systems must continuously learn and adapt to maintain their effectiveness against increasingly sophisticated cyber threats.

The reviewed studies also identify regulatory uncertainty as a significant barrier to AI implementation in cryptocurrency markets. Rodríguez Valencia et al. (2025) emphasize that cryptocurrency regulations differ substantially across jurisdictions, creating uncertainty regarding compliance requirements, cross-border investigations, and legal accountability. Similarly, Yahia et al. (2026) argue that many countries lack comprehensive governance frameworks addressing the ethical use of artificial intelligence in decentralized financial systems. Without clear regulatory guidelines, financial institutions may hesitate to invest in AI technologies despite their demonstrated effectiveness. This challenge is particularly relevant in emerging economies where cryptocurrency regulation remains relatively underdeveloped.

Within Kenya, these challenges are even more pronounced due to the country's evolving digital financial ecosystem. While Kamau and Kinyua (2025) and Ochieng et al. (2025) demonstrate the successful application of AI in detecting creative accounting and money laundering within conventional financial institutions, neither study addresses regulatory or ethical issues relating specifically to cryptocurrency fraud detection. Furthermore, Kenya continues to face limitations in AI expertise, computational infrastructure, locally generated blockchain datasets, and comprehensive cryptocurrency regulations. These constraints may impede the effective deployment of AI-based fraud detection systems despite increasing cryptocurrency adoption.

Overall, the reviewed literature indicates that the successful implementation of AI for cryptocurrency fraud detection depends not only on technological advancement but also on addressing challenges related to data quality, explainability, ethics, cybersecurity, and regulation. Strengthening governance frameworks, promoting responsible AI practices, improving access to high-quality datasets, and developing clear regulatory policies will be essential for ensuring trustworthy and sustainable AI adoption. Addressing these challenges is particularly important for Kenya, where the growing cryptocurrency market presents both opportunities for financial innovation and risks associated with emerging digital financial crimes. These findings provide the basis for identifying existing knowledge gaps and future research priorities, which are discussed in the final theme.

3.7 Theme Seven: Research Gaps and Future Research Directions for Kenya

The systematic review reveals that although considerable progress has been made in applying artificial intelligence (AI) to cryptocurrency fraud detection, important knowledge gaps remain, particularly regarding the application of these technologies in developing economies such as Kenya. Most existing studies focus on developing and evaluating machine learning and deep learning algorithms using datasets from developed countries, while comparatively little attention has been given to contextual factors influencing AI implementation in African financial systems. Consequently, there is limited evidence to guide researchers, financial institutions, and policymakers on the most appropriate AI techniques for addressing cryptocurrency fraud within Kenya's rapidly evolving digital financial environment (Rodríguez Valencia et al., 2025; Yahia et al., 2026).

One of the most significant research gaps identified is the geographical concentration of existing studies. The majority of empirical investigations reviewed were conducted in North America, Europe, and Asia, where blockchain infrastructure, cryptocurrency markets, and regulatory frameworks are relatively mature (Kamisetty et al., 2021; Dutta et al., 2023; Balusamy & Rengasamy, 2025). While these studies provide valuable insights into AI model development, their findings may not be directly transferable to Kenya because of differences in financial systems, technological infrastructure, digital literacy, and regulatory environments. The limited number of African studies suggests that locally generated evidence remains insufficient to support context-specific AI adoption strategies.

The review further indicates that existing Kenyan studies have concentrated primarily on conventional financial crimes rather than cryptocurrency fraud. For example, Kamau and Kinyua (2025) examined the application of AI in detecting creative accounting tendencies among Kenyan corporations, while Ochieng et al. (2025) investigated AI-based detection of money laundering in commercial banks. Both studies demonstrate the effectiveness of AI in strengthening financial crime detection within traditional financial institutions. However, neither examines blockchain transaction analysis, cryptocurrency exchanges, decentralized finance (DeFi), or AI-driven cryptocurrency fraud detection. This highlights a clear empirical gap that warrants further investigation as cryptocurrency adoption continues to expand in Kenya.

Another important gap relates to the availability of localized datasets. Many AI models reported in the reviewed studies were trained and validated using publicly available datasets obtained from international cryptocurrency exchanges and blockchain repositories (Kumar, 2022; Hussaini et al., 2022). While these datasets facilitate algorithm development, they may not adequately capture transaction behaviours, fraud patterns, or user characteristics unique to the Kenyan context. The absence of locally generated cryptocurrency transaction datasets limits the development of AI models capable of accurately identifying fraud within Kenya's digital financial ecosystem. Future research should therefore prioritize the creation of secure, anonymized, and representative local datasets through collaboration between financial institutions, regulators, and academic researchers.

The review also identifies a methodological gap within the current literature. Most empirical studies emphasize improving predictive accuracy by comparing machine learning and deep learning algorithms, while relatively few investigate the practical implementation of these technologies within organizational settings. Rodríguez Valencia et al. (2025) and Osei-Dwomoh and Forkuo (2026) argue that issues such as organizational readiness, user acceptance, governance structures, ethical considerations, and regulatory compliance remain underexplored despite their importance for successful AI adoption. Consequently, future studies should move beyond algorithm development to examine institutional, managerial, and policy factors influencing the deployment of AI-enabled fraud detection systems.

Ethical and explainability issues also represent important areas requiring further research. Although advanced deep learning models generally achieve higher predictive accuracy, their decision-making processes often lack transparency. Yahia et al. (2026) identify explainable artificial intelligence (XAI) as one of the fastest-growing research areas because financial institutions increasingly require AI systems whose decisions can be understood, justified, and audited. Similarly, Osei-Dwomoh and Forkuo (2026) emphasize the need to investigate algorithmic fairness, privacy protection, accountability, and responsible AI governance, particularly within emerging economies where regulatory frameworks are still developing. Future Kenyan studies should therefore examine how explainable AI can enhance public trust and regulatory acceptance while maintaining high fraud detection performance.

The reviewed studies further suggest opportunities for investigating hybrid AI models that integrate machine learning, deep learning, blockchain analytics, and cybersecurity technologies. Ali et al. (2026) and Balusamy and Rengasamy

(2025) demonstrate that combining AI with blockchain infrastructure enhances fraud detection accuracy and system resilience. However, limited research has examined the applicability of these hybrid approaches within African financial environments. Future studies could evaluate the effectiveness of integrated AI-blockchain frameworks for detecting cryptocurrency fraud in Kenya while considering local infrastructure, regulatory requirements, and resource constraints.

Overall, the review demonstrates that artificial intelligence has considerable potential to strengthen cryptocurrency fraud detection; however, significant research gaps remain regarding contextual adaptation, localized datasets, institutional implementation, ethical governance, explainable AI, and hybrid intelligent systems. Addressing these gaps will contribute to both academic knowledge and practical policy development by supporting the design of AI-based fraud detection systems that are technically robust, ethically responsible, and appropriate for Kenya's emerging cryptocurrency ecosystem. Future research should therefore adopt multidisciplinary approaches that integrate computer science, finance, cybersecurity, and public policy to develop sustainable AI solutions capable of enhancing financial security while promoting innovation in Kenya's digital economy.

3.8 Summary

This chapter synthesized findings from the nineteen studies included in the systematic literature review and organized them into seven themes. The review established that artificial intelligence has significantly enhanced cryptocurrency fraud detection through machine learning, deep learning, hybrid AI models, and blockchain analytics, offering greater accuracy, speed, and adaptability than traditional rule-based systems. The findings also showed that AI supports regulatory compliance through anti-money laundering (AML), Know Your Customer (KYC), and real-time transaction monitoring.

Despite these benefits, several challenges remain, including limited datasets, algorithmic bias, lack of explainability, privacy concerns, cybersecurity threats, and inadequate regulatory frameworks. The review further identified significant research gaps, particularly the limited evidence from developing countries such as Kenya, highlighting the need for localized datasets, explainable AI, hybrid models, and stronger governance frameworks. Overall, the findings demonstrate that AI has considerable potential to strengthen cryptocurrency fraud detection in Kenya, provided that technological, ethical, and regulatory challenges are adequately addressed.

4. DISCUSSION

The findings of this systematic literature review demonstrate that artificial intelligence (AI) has emerged as a transformative technology for cryptocurrency fraud detection by providing more accurate, adaptive, and efficient fraud detection capabilities than conventional rule-based systems. Across the reviewed studies, machine learning, deep learning, and hybrid AI models consistently outperformed traditional approaches because of their ability to analyse large volumes of blockchain transaction data, identify hidden behavioural patterns, and adapt to emerging fraud techniques. These findings support the growing consensus that AI has become an essential component of financial crime prevention within decentralized digital financial systems (Kumar, 2022; Agberxonu et al., 2023; Dutta et al., 2023).

The review indicates that supervised machine learning algorithms, including Random Forest, Support Vector Machines, Logistic Regression, and Extreme Gradient Boosting (XGBoost), remain the most widely adopted techniques for cryptocurrency fraud detection due to their high predictive accuracy and ability to classify legitimate and fraudulent transactions effectively. Deep learning models further improve fraud detection by automatically learning complex transaction characteristics from blockchain data without extensive manual feature engineering (Kamisetty et al., 2021; Dutta et al., 2023). Moreover, integrating AI with blockchain analytics enhances real-time transaction monitoring, anti-money laundering (AML), Know Your Customer (KYC) compliance, and financial risk management, thereby improving both operational efficiency and regulatory compliance (Rodríguez Valencia et al., 2025; Ali et al., 2026).

Despite these benefits, the review identified several challenges that may hinder the effective implementation of AI-based cryptocurrency fraud detection, particularly in developing countries such as Kenya. One major challenge is the limited availability of high-quality, labelled cryptocurrency transaction datasets. Most AI models have been developed using data from developed countries, which may not accurately represent transaction behaviours, fraud typologies, or user characteristics within Kenya's digital financial ecosystem (Hussaini et al., 2022). Consequently, AI models trained using foreign datasets may produce biased predictions or reduced detection accuracy when applied in local contexts.

The review also highlights important ethical and governance concerns associated with AI deployment. Highly sophisticated machine learning and deep learning models often function as "black-box" systems, making it difficult for regulators and financial institutions to explain or justify fraud detection decisions. This lack of transparency may reduce stakeholder confidence and complicate regulatory oversight (Rodríguez Valencia et al., 2025). Furthermore, issues relating to algorithmic bias, privacy protection, cybersecurity, and responsible AI governance remain significant barriers to widespread adoption (Osei-Dwomoh & Forkuo, 2026). Addressing these concerns will require the development of explainable AI models, robust data governance policies, and regulatory frameworks that promote fairness, accountability, and transparency.

From a Kenyan perspective, the findings reveal a significant research and implementation gap. Although studies by Kamau and Kinyua (2025) and Ochieng et al. (2025) demonstrate the successful application of AI in detecting creative accounting and money laundering, there is limited research focusing specifically on cryptocurrency fraud detection. This suggests that Kenya has begun adopting AI for financial crime detection but has yet to fully exploit its potential within cryptocurrency markets. As cryptocurrency adoption continues to grow, there is an urgent need to develop localized AI models, establish secure blockchain datasets, and strengthen institutional capacity to support AI-driven fraud detection.

Based on the synthesized findings, a conceptual framework is proposed to explain the relationships among the key constructs influencing AI-based cryptocurrency fraud detection in Kenya. The framework identifies Artificial Intelligence Techniques as the independent variable, comprising machine learning, deep learning, hybrid AI models, and blockchain analytics. These techniques influence the dependent variable, Cryptocurrency Fraud Detection, measured through fraud detection accuracy, anomaly detection capability, real-time transaction monitoring, reduced false positives, and improved regulatory compliance. The relationship is moderated by Regulatory Framework, Data Availability and Quality, ICT Infrastructure, Cybersecurity Capacity, and Human Expertise, which influence the effectiveness of AI implementation. Ultimately, effective application of AI techniques is expected to strengthen financial security, improve public trust, reduce cryptocurrency-related fraud, and support the sustainable growth of Kenya's digital financial ecosystem.

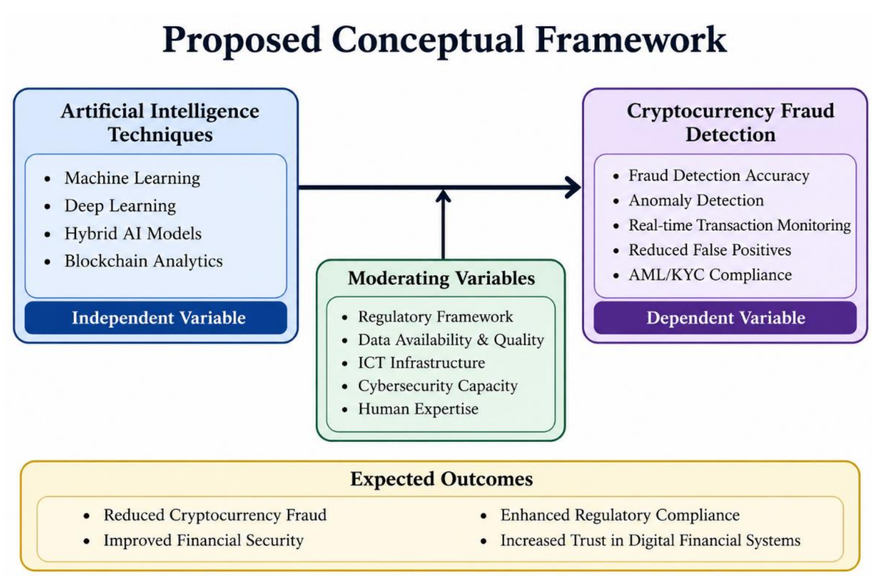

Figure 2: Proposed Conceptual Framework

The conceptual framework illustrates the relationship between artificial intelligence techniques and cryptocurrency fraud detection. It proposes that machine learning, deep learning, hybrid AI models, and blockchain analytics enhance fraud detection by improving detection accuracy, anomaly detection, real-time transaction monitoring, and regulatory compliance. The effectiveness of this relationship is moderated by factors such as the regulatory framework, data availability and quality, ICT infrastructure, cybersecurity capacity, and human expertise, ultimately contributing to reduced cryptocurrency fraud and improved financial security.

5. CONCLUSIONS AND RECOMMENDATIONS

This chapter presents the conclusions drawn from the systematic literature review on artificial intelligence techniques for cryptocurrency fraud detection in Kenya. The conclusions are based on the synthesis of evidence from the nineteen studies reviewed using the PRISMA 2020 framework. The chapter also outlines recommendations for researchers, financial institutions, regulators, and policymakers, and proposes areas for future research.

5.1 Conclusions

The review established that artificial intelligence has become an indispensable technology in cryptocurrency fraud detection because of its ability to analyse large volumes of blockchain transaction data, detect anomalous behaviour, and adapt to evolving fraud patterns. Machine learning techniques, particularly Random Forest, Support Vector Machines, Logistic Regression, and XGBoost, emerged as the most widely applied approaches due to their high predictive accuracy and ability to classify fraudulent transactions effectively. In addition, deep learning and hybrid AI models demonstrated superior performance in analysing complex blockchain transaction networks and identifying sophisticated fraud schemes.

The findings further revealed that integrating artificial intelligence with blockchain analytics enhances transaction monitoring, anti-money laundering (AML), Know Your Customer (KYC) compliance, and financial risk management. Compared with conventional rule-based systems, AI-driven approaches provide faster, more accurate, and scalable fraud detection capabilities, making them suitable for the dynamic nature of cryptocurrency ecosystems.

Despite these advancements, the review identified several challenges that hinder the effective implementation of AI-based cryptocurrency fraud detection. These include limited access to quality datasets, algorithmic bias, lack of model explainability, cybersecurity threats, privacy concerns, high computational requirements, and inadequate regulatory frameworks. The review also found that research on AI-driven cryptocurrency fraud detection is concentrated mainly in developed countries, with limited empirical evidence from Kenya and other African economies.

Overall, the study concludes that artificial intelligence has significant potential to strengthen cryptocurrency fraud detection in Kenya. However, realizing this potential requires context-specific research, improved regulatory frameworks, localized datasets, responsible AI governance, and collaboration among researchers, financial institutions, technology providers, and government agencies.

5.2 Recommendations

Based on the findings of the review, the following recommendations are proposed:

Recommendations for Financial Institutions and Cryptocurrency Service Providers

Financial institutions, cryptocurrency exchanges, and fintech firms should invest in AI-powered fraud detection systems capable of analysing blockchain transactions in real time. They should also integrate machine learning and blockchain analytics into their anti-money laundering and transaction monitoring systems to improve fraud detection accuracy and operational efficiency.

Recommendations for Policymakers and Regulators

Government agencies and financial regulators should develop comprehensive regulatory frameworks governing the application of artificial intelligence in cryptocurrency markets. Policies should promote responsible AI use, strengthen cybersecurity standards, encourage information sharing, and establish guidelines for explainable and ethical AI in financial crime detection.

Recommendations for Researchers

Future studies should focus on developing localized AI models using Kenyan cryptocurrency transaction data. Researchers should also investigate explainable artificial intelligence, hybrid AI models, blockchain forensics, and the organizational factors influencing AI adoption within cryptocurrency ecosystems.

Recommendations for Capacity Building

Universities, research institutions, and industry stakeholders should strengthen capacity building in artificial intelligence, blockchain technology, and cybersecurity through training, collaborative research, and knowledge-sharing initiatives. Building local expertise will support the sustainable implementation of AI-based fraud detection systems in Kenya.

5.3 Suggestions for Future Research

Future studies should address the following areas:

- Development of Kenyan cryptocurrency fraud datasets for AI model training and validation.
- Comparative evaluation of machine learning, deep learning, and hybrid AI models using local data.
- Application of explainable artificial intelligence (XAI) in cryptocurrency fraud detection.
- Integration of blockchain analytics with AI for enhanced financial crime investigation.
- Organizational readiness and factors influencing AI adoption within cryptocurrency exchanges and financial institutions in Kenya.
- Ethical, legal, and regulatory implications of AI-driven cryptocurrency fraud detection in emerging economies.

REFERENCES

Agberxonu, E., Disu, A., Dike, C., Mustapha, T., & Abakah, L. (2023). Machine Learning and Artificial Intelligence in FinTech: Driving Innovation in Digital Payments, Fraud Detection, and Financial Inclusion. Communication In Physical Sciences, 9(4), 1037-1057.

Ali, Guma, Otim Emmanuel, Maad M. Mijwil, Bosco Apparatus Buruga, Aida Vafae Eslahi, and Ioannis Adamopoulos. "A survey on securing smart finance using artificial intelligence and blockchain." SHIFRA 2026 (2026): 1-61. https://doi.org/10.70470/SHIFRA/2026/001

Ampumuza, D., Katushabe, C., & Tamale, M. (2026). A systematic review and future directions for AI-driven detection of fraud patterns in SACCO transactions. Frontiers in Artificial Intelligence, 8, 1690482. https://doi.org/10.3389/frai.2025.1690482

Balusamy, S., & Rengasamy, R. (2025, May). Protecting Financial Transactions and Cryptocurrency Networks from Fraud Using AI-Powered Blockchain Technology. In 2025 Global Conference in Emerging Technology (GINOTECH) (pp. 1-6). IEEE. https://doi.org/10.1109/GINOTECH63460.2025.11076940

Chithanuru, V., & Ramaiah, M. (2023). An anomaly detection on blockchain infrastructure using artificial intelligence techniques: Challenges and future directions-A review. Concurrency and Computation: Practice and Experience, 35(22), e7724. https://doi.org/10.1002/cpe.7724

Dutta, A., Voumik, L. C., Ramamoorthy, A., Ray, S., & Raihan, A. (2023). Predicting cryptocurrency fraud using ChaosNet: The Ethereum manifestation. Journal of Risk and Financial Management, 16(4), 216. https://doi.org/10.3390/jrfm16040216

Hussaini, Y., Waziri, V. O., Isah, A. O., & Ojeniyi, J. A. (2022). Cryptocurrency Fraud Detection: A systematic Literature review. 4th International Engineering Conference (IEC 2022).

Kamau, C. G., & Kinyua, N. N. (2025). Application of Artificial Intelligence in Detecting Creative Accounting Tendencies Among Corporations in Kenya. African Journal of Commercial Studies, 6(6), 103-112. https://doi.org/10.59413/ajocs/v6.i6.9

Kamau, C. G., & Yavuzaslan, A. (2023). CryptoAudit: Nature, requirements and challenges of Blockchain transactions audit. African Journal of Commercial Studies, 3(2), 101-107. https://doi.org/10.59413/ajocs/v3.i2.3

Kamisetty, A., Onteddu, A. R., Kundavaram, R. R., Gummadi, J. C. S., Kothapalli, S., & Nizamuddin, M. (2021). Deep learning for fraud detection in bitcoin transactions: An artificial intelligence-based strategy. NEXG AI Review of America, 2(1), 32-46.

Kumar, Y. (2022). AI techniques in blockchain technology for fraud detection and prevention. In Security engineering for embedded and cyber-physical systems (pp. 207-224). CRC Press. https://doi.org/10.1201/9781003278207-14

Kumari, S. (2025). Machine Learning Applications in Cryptocurrency: Detection, Prediction, and Behavioral Analysis of Bitcoin Market and Scam Activities in the USA. International Journal of Sustainable Science and Technology, 3(1). https://doi.org/10.22399/ijsusat.8

Lin, C. Y., Liao, H. K., & Tsai, F. C. (2022). A systematic review of detecting illicit bitcoin transactions. Procedia Computer Science, 207, 3217-3225. https://doi.org/10.1016/j.procs.2022.09.379

Ochieng, D. O., Olala, S., & Asembo, K. O. (2025). The Application of Artificial Intelligence in Detecting Money Laundering in Kenyan Commercial Banks. The Eastern Africa Journal of Policy and Strategy, 118-139.

Osei-Dwomoh, E., & Forkuo, G. O. (2026). Artificial intelligence in African economics: a systematic review of performance and ethical risks. Future Business Journal, 12(1), 84. https://doi.org/10.1186/s43093-026-00776-y

Rodríguez Valencia, L., Ochoa Arellano, M. J., Gutiérrez Figueroa, S. A., Mur Nuño, C., Monsalve Piqueras, B., Corrales Paredes, A. D. V., ... & Levi Alfaroviz, A. (2025). A systematic review of artificial intelligence applied to compliance: Fraud detection in cryptocurrency transactions. Journal of Risk and Financial Management, 18(11), 612. https://doi.org/10.3390/jrfm18110612

Rodríguez Valencia, L., Ochoa Arellano, M. J., Gutiérrez Figueroa, S. A., Mur Nuño, C., Monsalve Piqueras, B., Corrales Paredes, A. D. V., ... & Levi Alfaroviz, A. (2025). A systematic review of artificial intelligence applied to compliance: Fraud detection in cryptocurrency transactions. Journal of Risk and Financial Management, 18(11), 612. https://doi.org/10.3390/jrfm18110612

Sabry, F., Labda, W., Erbad, A., & Malluhi, Q. (2020). Cryptocurrencies and artificial intelligence: Challenges and opportunities. IEEe Access, 8, 175840-175858. https://doi.org/10.1109/ACCESS.2020.3025211

Yahia, A., Mouhssine, Y., Alaoui, A. E., & Alaoui, S. O. E. (2026). Exploring the role of Artificial Intelligence in Cryptocurrency Evolution: A Systematic Review and Bibliometric Analysis at the Intersection. Journal of the Knowledge Economy, 17(2), 5600-5647. https://doi.org/10.1007/s13132-025-02857-9