BUILDING A BLOCKCHAIN BASED ARTIFICIAL INTELLIGENCE (AI) CLASSIFICATION MODEL TO DETECT FRAUDS IN A LIVE TRANSACTIONAL FINANCIAL SYSTEM

by

K SRINIVAS, M.Phil, M.Sc, MHRM, B.Sc

DISSERTATION

Presented to the Swiss School of Business and Management Geneva

In Partial Fulfillment

Of the Requirements

For the Degree

DOCTOR OF BUSINESS ADMINISTRATION

SWISS SCHOOL OF BUSINESS AND MANAGEMENT GENEVA

MARCH, 2024

BUILDING A BLOCKCHAIN BASED ARTIFICIAL INTELLIGENCE (AI) CLASSIFICATION MODEL TO DETECT FRAUDS IN A LIVE TRANSACTIONAL FINANCIAL SYSTEM

by

K SRINIVAS

Supervised by

Dr. Anna Provodnikova

APPROVED BY

____

Dissertation chair

RECEIVED/APPROVED BY:

____

Admissions Director

Dedication

I hereby dedicate that the thesis entitled "Building A Blockchain Based Artificial Intelligence (AI) Classification Model to Detect Frauds In A Live Transactional Financial System" submitted to SSBM, Geneva for the award of degree of Doctor of Business Administration, is my original research work. This thesis or any part thereof has not been submitted partially or fully for the fulfillment of any degree of discipline in any other University/Institution.

(Srinivas Ketha)

ACKNOWLEDGEMENT

I would like to acknowledge and give my warmest thanks to my Supervisor Dr. Anna L Provodnikova, PhD (Professor) for her continuous guidance, advice and support during the period to accomplish my research work. Her timely help with observations has greatly helped my research to attain its present form.

I would like to thank research committee members and faculty members of the SSBM, Geneva. Their support and encouragement for research was worth for me.

Last but not least, I would like to remember my late father Shri Ketha Adinarayana Rao and my beloved mother Ketha Leelavathi for all their blessings, empowering and instilling in me the importance of life-long education. I would also like to give special thanks to my wife Dearest Ketha Vivandana and the fortune of my life my children Abhay & Simran, who have given great support and cheered me up while proceeding towards my research work.

Finally, I would like to thank Almighty, for letting me through all the difficulties. I have experienced your guidance day by day. I will keep on trusting you for my future.

(K Srinivas)

ABSTRACT

BUILDING A BLOCKCHAIN BASED ARTIFICIAL INTELLIGENCE (AI) CLASSIFICATION MODEL TO DETECT FRAUDS IN A LIVE TRANSACTIONAL FINANCIAL SYSTEM

K Srinivas

2024

Dissertation Chair: <Chair’s Name>

Co-Chair: <If applicable. Co-Chair’s Name>

This research is being conducted to understand and explore on how to integrate two most trending, disruptive and innovative technologies of the current era that is Blockchain and Artificial Intelligence to find a solution to the business problem of detecting frauds in a live transactional financial system. The goal is to propose a conceptual framework encompassing Blockchain and Artificial Intelligence to detect and

prevent frauds in a live transactional financial system for future research in the same domain to increase the chances of their success.

The ongoing research aims to forge a deeper comprehension and exploration into the seamless integration of two cutting-edge and revolutionary technologies prevalent in today's landscape: Blockchain and Artificial Intelligence (AI). This integration seeks to tackle the pressing business challenge of detecting fraudulent activities within a dynamic, live transactional financial system. The primary objective revolves around devising a conceptual framework that harmonizes Blockchain and AI, ultimately aiming to proactively identify and mitigate fraud instances within such financial ecosystems.

At its core, this research endeavors to leverage the inherent strengths of both Blockchain and AI. Blockchain technology, renowned for its decentralized and immutable nature, forms a robust foundation that ensures the integrity and transparency of transactions within a financial system. Simultaneously, AI with its prowess in pattern recognitionand data analysis, holds the potential to significantly enhance fraud detection capabilities by swiftly identifying anomalous patterns or irregularities amidst a myriad of transactions.

The overarching ambition is to propose a comprehensive conceptual blueprint that encapsulates the synergy between Blockchain and AI. This blueprint serves as a foundational framework for future research endeavors within the same domain, fostering an environment conducive to heightened probabilities of success in addressing fraud detection and prevention. By intricately merging Blockchain's secure, transparent ledger with AI's analytical capabilities, the proposed framework aspires to fortify the existing defenses against fraudulent activities within live transactional systems. Through this amalgamation, the research aims to establish an innovative approach that not only detects ongoing fraud instances in real time but also proactively prevents potentially fraudulent activities, thereby fostering a more resilient and secure financial environment.

TABLE OF CONTENTS

LISTOF TABLES

LIST OF FIGURES

CHAPTER I:

INTRODUCTION

In this particular section will specify a high level outline of the subject under study within the current knowledge set. A background of the subject along with key points will be provided, and the importance of the research will be underscored. Furthermore, the motivation and expected outcomes of the research will be outlined in this section, along with the justification of why the research is important, and why it must be performed. Next, the problem statement will be presented, and later used to propose research questions. Finally, this section will address the gap this research will fill in existing literature.

1.1 Research Background and Scope

The intricate phenomenon of financial transactions in today's interconnected world is an orchestra of real-time exchanges and digital marvels. Yet, within this dynamic symphony lies a persistent threat: the specter of fraud. Frauds in live transactional financial systems have emerged as a formidable challenge, eroding trust, and imperiling the integrity of global commerce. The significance of understanding these fraudulent activities transcends mere monetary loss; it strikes at the core of economic stability, consumer confidence, and the very foundation of a secure financial ecosystem.

In recent years, the rise in financial fraud within live transactional systems has been nothing short of alarming. The convergence of rapid technological advancements, the proliferation of digital platforms, and the ever-evolving sophistication of tactics used by fraudsters have created a fertile ground for fraudulent activities. The statistics tell a shocking tale: a relentless surge in financial fraud cases reported across various sectors and regions.

The advent of real-time transactional systems, while a boon for seamless commerce, has inadvertently provided an avenue for fraudsters to exploit vulnerabilities. The speed and complexity of these systems, coupled with the interconnectivity of global financial networks, have amplified the challenges in detecting and preventing fraudulent activities.

Cyber fraud, a potent and pervasive form of financial malfeasance, has witnessed an exponential rise. The labyrinthine networks of online platforms, digital payment gateways, and interconnected databases have become prime targets for cybercriminals. Phishing, identity theft, ransomware attacks, and data breaches have become distressingly common, causing substantial financial losses and compromising sensitive personal and corporate information (Sarkarand Shukla, 2023, p.32).

The shifting landscape of financial transactions has also witnessed a metamorphosis in the modus operandi of fraudsters. From sophisticated social engineering tactics to exploiting loopholes in regulatory frameworks, these individuals or organized groups constantly adapt and evolve, staying several steps ahead of traditional security measures.

Furthermore, the global nature of financial systems has led to an intricate web of regulatory frameworks and compliance standards. While these measures aim to fortify the defenses against fraud, the ever-evolving nature of financial technology often outpaces regulatory adaptations. The resulting gaps in oversight create opportunities for exploitation, adding another layer of complexity to the fight against fraud.

The consequences of financial fraud reverberate far beyond monetary losses. They corrode trust and confidence in financial institutions, denting the credibility of entire systems. Consumer trust, a cornerstone of thriving economies, faces erosion when individuals fear that their hard-earned assets are vulnerable to fraudulent activities. Businesses, too, bear the brunt, grappling with financial losses, reputational damage, and the arduous task of rebuilding trust among their clientele.

The societal impact of financial fraud extends to broader ramifications, affecting not only individuals and businesses, but also governments and economies at large. As fraud undermines the stability of financial systems, it poses systemic risks that can ripple through economies, leading to reduced investments, increased borrowing costs, and a general slowdown in economic growth.

In this intricate dance between technological innovation and the malevolent ingenuity of fraudsters, the need for a multifaceted approach to combat financial fraud becomes imperative. It necessitates a synergy between cutting-edge technology, robust cyber security measures, stringent regulatory frameworks, and a vigilant, proactive approach from financial institutions, businesses, regulatory bodies, and consumers alike.

To address the burgeoning threat of fraud in live transactional financial systems, a holistic strategy encompassing prevention, detection, and response is indispensable. Proactive measures such as advanced authentication protocols, real-time monitoring systems, artificial intelligence-driven anomaly detection, and encryption technologies are pivotal in fortifying the defenses against fraudulent activities (Meduri, 2024, p. 915).

Moreover, fostering a culture of awareness and education is paramount. Equipping individuals and businesses with the knowledge to identify potential threats, adhere to best practices, and promptly report suspicious activities can serve as a bulwark against fraud. Collaboration and information sharing among stakeholders across industries and borders are equally critical. A unified front in sharing insights, intelligence, and best practices can fortify defenses and preempt potential vulnerabilities in live transactional systems.

In conclusion, the escalating prevalence of fraud in live transactional financial systems poses a pressing challenge that demands a concerted and holistic response. Understanding the significance of these fraudulent activities, acknowledging their impact, and collectively endeavoring to fortify the defenses against them is indispensable in safeguarding the integrity, stability, and trustworthiness of global financial systems.

Frauds in a live transactional financial system are akin to stealthy adversaries lurking within the intricate web of commerce. In the realm of dynamic and real-time monetary exchanges, the menace of fraudulent activities casts a shadow over the reliability and integrity of the system. These fraudulent practices, whether through deceitful manipulations, sophisticated cyber breaches, or cunning schemes, undermine the trust and security upon which financial transactions rely. Exploring the nuances of these fraudulent endeavors within the pulsating heart of live transactional systems unveils the complexities and challenges in safeguarding against these threats (Nordstrom and Carlson, 2014).

1.2 Online Fraud Statistics

As the world glances to move on from COVID-19, do customers now feel more liable than ever to the danger of fraud?

In partnership with Propeller Insights, Marqeta (2021) investigated 2,000 customers in the UK and US to apprehend how our digital lives post-pandemic have affected our perspectives toward payment fraud. The survey indicates the scope to which customers have been influenced by the events of the past year, both in expected and unexpected ways:

- One out of every four consumers who have experienced fraudulent activity stated that they were impacted within the previous year.
- Customers' worry over fraud has increased by 65% since the beginning of COVID-19.
- Since the onset of COVID-19, 56% of customers have observed an increase in phishing attempts aimed at obtaining payment details.

The impact of fraud during COVID-19 has been felt most by younger consumers. A survey revealed that consumers aged 18-34 were 40% more likely to encounter fraud for the first time in the past year. Despite concerns, most consumers have not actively adopted better habits to protect themselves from fraud in the last year (Marqueta, 2021).

How will apprehension about fraud influence consumers' willingness to embrace new payment technologies? With the world increasingly transitioning to digital platforms during the pandemic, fraudsters are finding more opportunities to exploit vulnerabilities. The survey highlights consumer sentiments towards the rise of digital payment technologies and suggests measures that financial institutions can take to enhance consumer trust.

The figures mentioned in the Juniper Research report (2023) about online payment fraud in November 2022 demonstrate the magnitude of online payment fraud and emphasize the importance of businesses taking proactive measures to safeguard themselves. Here are several vital statistics from that report Juniper Research report.

The anticipated global expenditure on online payment fraud is set to hit $206 billion by 2025, a significant increase from the $130 billion recorded in 2020. The transition to e-commerce and mobile commerce has opened up fresh avenues for malicious individuals to engage in deceptive practices. As online shopping and digital payment methods become more popular, fraudsters have more potential targets and a comprehensive array of methods to access confidential data (Cara, 2023).

The rapid spread of COVID-19 contributed to the expansion of online shopping and digital transactions, as more individuals opted for virtual purchases to minimize face-to-face interactions. This has created fresh opportunities for deceptive individuals to exploit the surge in online shopping to execute more sophisticated fraudulent activities and schemes. The COVID-19 pandemic has expedited the transition to online commerce, resulting in a 20% uptick in the value of digital transactions. As a result of the 2020 lockdowns and social distancing measures, a substantial number of traditional retail stores were compelled to cease operations (Goel et al., 2022, p.100). The pandemic caused a significant rise in online shopping as people sought a safer and more convenient option. Consequently, there was a substantial increase in e-commerce activity, with online transaction values seeing a 20% boost. While e-commerce has been a crucial support for some businesses that may have otherwise shut down, it has also brought about new challenges and risks, particularly in dealing with the growing threat of online payment fraud and other security issues. Synthetic identity fraud is on the rise and is projected to result in losses reaching $14 billion by 2025 (Shaw et al., 2022, p.103). In the case of synthetic identity fraud, a deceptive individual fabricates a false identity by blending authentic and invented details. This could be your identity. For instance, they might utilize a genuine Social Security number along with a fabricated name and address. Using this identity, they might seek credit cards, establish bank accounts, or conduct transactions, all without being noticed by credit bureaus and other official bodies(Julia, 2021). The rise in synthetic identity theft is due to two main factors. First, the easy access to personal information online, coupled with technological advancements, has made it simpler for criminals to produce authentic-looking fake identities. Second, consumers' dependence on digital platforms for financial transactions and other activities has opened up new opportunities for fraudulent individuals to exploit weaknesses in the system. The adoption of biometric authentication methods is projected to increase by 47% in the next five years, offering a more secure means of confirming identities online. Biometric authentication methods are gaining popularity to verify identities online, especially with mobile devices and mobile payments. Biometric authentication entails using distinct biological traits such as fingerprints, facial recognition, or iris scans to authenticate a user's identity and allow access to a device or online account (Jo Ann Barefoot, 2020).

The ubiquity of mobile devices and mobile payments has provided the adoption of authentication using biometric, since these devices often contain inbuilt biometric sensors for authentication. Many consider biometric authentication to be a more secure alternative to traditional password-oriented authentication, which can easily be compromised by fraudulent actors and hackers. While biometric authentication has been implemented and embraced widely by businesses and consumers because of its perceived high level of security, some fraudulent actors have found ways to work around it.

The regions with the highest impact from online payment fraud are North America and Europe, with anticipated losses of $50 billion and $35 billion by 2025, respectively. Online payment fraud has a significant impact on these regions, partly because of the widespread usage of digital payment methods, the advanced technology infrastructure, and high online connectivity levels (Yamaguti, 2024).

In the North American region, various elements have contributed to the increase in online payment fraud, such as the widespread utilization of credit and debit cards and the growing acceptance of mobile payments and online shopping. North America hosts numerous major financial institutions and technology firms, making them appealing targets for cybercriminals (Yamaguti, 2024).

In Europe, online payment fraud has been impacted by many of the same elements, as well as high levels of consumer spending and the presence of large ecommerce platforms and marketplaces.

The largest market for online payment fraud is in the Asia-Pacific region, and losses are projected to amount to $54 billion by 2025. This region's susceptibility to online payment fraud can be attributed to the rapid growth in the adoption of digital payment methods and the increasing internet connectivity of its large and diverse population (Everett, 2016,p.8).

Higher incomes, excellent internet and smartphone access, and the growth of the middle class have fueled e-commerce and mobile payment expansion in numerous Asia-Pacific nations. This has created fresh opportunities for fraudulent individuals, especially in countries with less rigorous regulations and security standards than more advanced markets (Everett, 2016, p.8).

It is important to remember that it faces significant repercussions from online payment fraud, which can result in substantial financial losses for businesses and consumers. Furthermore, it can harm companies' reputations and trust. The companies' reputations and trust fraud can erode confidence in digital payment methods and impede the advancement of e-commerce and mobile commerce, which are considered vital drivers of economic development in the region.

There's hope in the fight against online fraud. Machine learning and artificial intelligence are increasingly being used to counter this threat, and it's projected that by 2025, the investment in these technologies will reach a substantial $11.3 billion (Shete et al., 2024, p.18).

Machine learning and artificial intelligence (AI) play a crucial role in fighting online fraud by leveraging their capacity to analyze vast volumes of data and spot patterns and irregularities that conventional fraud detection techniques could overlook. Machine learning and AI can pinpoint questionable transactions, identify unusual user behavior, and scrutinize data from various origins to uncover fraudulent actions immediately (Apoorva, 2024).

The increasing prevalence of online fraud and the demand for more sophisticated fraud detection techniques have led to adopting machine learning and AI in fraud prevention. Technological progress has made it more accessible and cost-effective for even smaller businesses to incorporate machine learning and AI systems. Machine learning and AI offer a more efficient way to identify and stop fraudulent activities, lowering the risk of financial losses for businesses and their clientele. Additionally, they can decrease the instances of both false positives and false negatives. A false positive occurs when a genuine transaction is mistakenly identified as fraudulent, often due to a pattern or behavior that appears suspicious but is legitimate. Conversely, a false negative happens when a fraudulent transaction goes undetected by the fraud prevention system and is allowed to proceed. Limiting the occurrence of false positives and negatives can help mitigate the overall impact of fraud. The digital goods and money transfer sectors are anticipated to be most susceptible to online fraud, and combined losses are projected to reach $60 billion by 2025 (Gupta, 2023, p.47).

Businesses that sell digital products or engage in financial transactions are particularly susceptible to online fraud due to the nature of intangible goods and services, which can be challenging to authenticate. Moreover, these sectors often rely on digital payment methods and online platforms, making them more vulnerable to fraudulent activities compared to traditional payment methods.

Individuals conducting fraudulent activities for digital goods may utilize stolen credit card details to acquire software licenses, music, and e-books. Subsequently, they may unlawfully resell these products or utilize them for personal use. In the case of money transfers, fraudulent actors may employ various methods to deceive users into transferring funds to fictitious accounts or disclosing personal information that can be exploited for further fraudulent activities (Sadiq et al., 2019, p.241).

Key points for online retail businesses: It's crucial for businesses to remain vigilant about the increased risk of online and e-commerce fraud, which is anticipated to rise significantly in the future. In addition to potentially undermining customer trust and brand loyalty, security breaches and fraud can place a heavy burden on a company's internal resources. The objective should be to establish comprehensive protection across all channels that support various payment methods, and to utilize systems and tools that are not just implemented, maintained, and operated, but are also cutting-edge and efficient, to stay ahead of the evolving threat landscape(Edwards, 2023).

To combat fraud in online and e-commerce transactions, companies must implement a comprehensive security approach integrating advanced authentication technologies, fraud detection and prevention solutions such as Stripe Radar, and industry-best data security and privacy practices. This might entail integrating two-factor authentication, utilizing machine learning and AI for fraud identification, and ensuring that all customer data is securely encrypted and stored. Importantly, Stripe's payment solutions come with all these protective measures built-in.

In addition to these measures, businesses must collaborate with financial institutions and other partners to exchange information about emerging threats and work together on strategies to address fraud. Businesses should also educate their employees and customers about the perils of online fraud and provide training on identifying and preventing fraudulent activities. By taking these steps, companies can help safeguard themselves and their customers from the ever-growing risk of online and e-commerce fraud.

Transactional Systems dealing in financial transactions in millions are prone to financial frauds both due to internal as well as external factors. Due to the high volume of transactions and the challenges of anytime anywhere settlements including auto settlements, it is always hard to detect financial frauds by manual processes. Also, the fraud transactions could very well be disguised as genuine transactions making manual detection almost next to impossible (Tiwari et al, 2022, p.37).

1.3 Research Problem

Can blockchain and AI combined to detect Fraud in a live transactional financial system, and if you how exactly to go about it.

Any financial transaction depends on two distinct parts for the transaction to be validated and completed which are the Non-financial Part: like Name, DOB, Aadhaar, Gender, Bank Account No., IFSC Code, PAN etc and the Financial Part: comprises the actual amounts like Opening Balance, current transactions, Changes in Opening Balances, Transfer-ins and Transfer-outs and any other amounts which have the potential to change the final transacted amount.

Financial frauds can be triggered by manipulating either or both of the non-financial part and the financial part, i.e., the financial fraud could possibly be of three types viz., Manipulating only the non-financial information of the account holder for example changing the Bank Account Number, Manipulating only the financial information of the account holder for e.g., Balances or by Manipulating both the non-financial and financial information of the account holder for example, changing Bank Account Number and Balance simultaneously.

1.4 Theory of Reasoned Action

Hypothesis of the research: By leveraging combined features of Blockchain and AI technologies together, organizations will be better poised to tackle the mentioned business problem.

The work involves coming up with a practical model of combining the two technologies in a practical way to solve the business use-case. The central question is to explore building a blockchain based Artificial intelligence (AI) classification model to detect frauds in a live transactional financial system. The goal is to present a practical approach encompassing Blockchain and Artificial Intelligence to detect and prevent frauds in a live transactional financial system for future research in the same space to increase the chances of their success.

The hypothesis posits that a cohesive integration of blockchain technology and artificial intelligence (AI) into a singular classification model for detecting financial fraud in live transactional systems outperforms the effectiveness of disjoint systems, where blockchain and AI operate independently. The combined model synergizes the strengths of technologies, leveraging block chain's immutability, decentralization, and secure data handling alongside AI's sophisticated analytical capabilities. By unifying these technologies, the integrated model presents a holistic approach, providing a more comprehensive and robust framework for fraud detection. Unlike separate systems that may face challenges in synchronizing data or lack seamless interoperability, the combined model ensures a streamlined and cohesive environment. It harnesses the power of block chain's immutable ledger to securely store transactional data while employing AI algorithms to continuously analyze patterns, detect anomalies, and swiftly identify fraudulent activities. This cohesive integration, therefore, is theorized to offer a more effective, efficient, and proactive solution in combating financial fraud in live transactional financial systems (Odeyemi et al., 2024, p.271).

The result of this study that is to combine Blockchain and AI technologies to solve the business problem of detecting frauds in a live transactional financial system could be valuable to the organizations small as well as medium and big dealing in online live financial transactions.

1.5 Significance of the Study

Blockchain and artificial intelligence (AI) are seen as the most revolutionary technologies expected to impact all sectors of business and industries. Blockchain technologies enable the automation of cryptocurrency payments and provide decentralized, secure, and trustworthy access to a shared ledger of data, transactions, and logs. Through smart contracts, blockchain can govern interactions among participants without the need for intermediaries or trusted third parties. On the other hand, artificial intelligence (AI) provides machines with decision-making capabilities similar to those of humans.

Blockchain based AI systems can help combat and defeat application fraud by detecting illicit activity in the process. Financial Organizations are now deploying machine learning models that can detect suspicious transactions in almost real time, including stopping the transaction altogether or raising an alert and escalating the transaction for manual intervention before being ousted from the system.

Blockchain based AI systems could start with Machine Learning (ML) algorithms and then move on to Deep Learning (DL) models in due course based on experience and expertise gained in use and deployment of such systems.

1.6 Research Purpose and Questions

The Research purpose is to amalgamate Blockchain and AI technologies in general and use their combined strength to detect frauds in live transactional financial systems in particular.

The purpose of this study is to understand the integration of blockchain and AI to detect frauds in live transactional financial systems. The participants chosen for this study are those working on fraud detection using technology interventions.

This research goal is to resolve the following question and sub-questions

Central Question: How to model a combined blockchain and AI based solution?

Question 1: What is a primary advantage of using a blockchain-based AI model for fraud detection?

Question 2: Which technology ensures the immutability of transactional records in a blockchain?

Question 3: How does AI contribute to fraud detection in a live financial system?

Question 4: What is the significance of real-time monitoring in detecting financial frauds?

Question 5: What role does a smart contract play in a blockchain-based fraud detection system?

1.7 Structure of the Thesis

This thesis is breaked into five (6) major chapters

Chapter one involves introduction to the research, which delves into the research background and scope, giving online fraud Statistics. This chapter further defines the research problem, purpose of research, theory of reasoned action, Significance of the research, research purpose and lastly the structure the thesis follows in brief.

Chapter Two is a summary of the review of literature that the researcher studied as part of the research process. This section identifies major works that are relevant, highlights significant research and most importantly identifies the gap in existing literature. This research will try to present the gap.

Chapter Three deals with the approach taken for this research. It will cover the various data gathering used in this research and arriving at logic to move forward. The section will also provide insights into how the interview questions were formed along with the nature of these questions.

ChapterFourexamines the results with analysis of the questionnaire and also the analysis of the responses going on to summarize the findings. Various AI classification models are also discussed with their pros and cons as the relevant ones are used in coding the solution.

Chapter Five provides the discussion on this research. It contains the proposed steps to integrate the Artificial Intelligence and Blockchain into the final proposed model to achieve the primary and secondary objectives, along with deploying the blockchain based AI implemented system.

Chapter Six delves on the summary, Implications and recommendation of the amalgamated model highlighting the key takeaways of the research.

CHAPTER II:

REVIEW OF LITERATURE

2.1 Introduction

To acquaint oneself with what research already has been performed, and what the perspectives of other studies are, the researcher spent time in gathering, reading and summarizing existing publications, articles, papers and blogs.

The literature review conducted for this research lays out the current knowledge set available for the topic under scrutiny. By defining the boundaries of what is known, the identification of gaps in existing knowledge becomes possible. The literature review will also be used to identify existing material that supports the research topic in question. This chapter also looks to highlight important research that has been performed, and point out links between existing theories and practices.

Research papers exploring the application of Artificial Intelligence (AI) in detecting frauds within live transactional financial systems highlight the pivotal role of advanced technologies in fortifying security measures. These studies delve into the multifaceted applications of AI, machine learning, and data analytics to preempt, identify, and mitigate fraudulent activities in real-time transactions (Snyder, 2019, p. 333).

The research underscores the significance of AI-enabled solutions in combating the escalating sophistication of financial fraud. They explore how AI algorithms can analyze vast volumes of transactional data, identifying anomalous patterns or deviations from normal behavior. These anomalies serve as red flags for potentially fraudulent activities, enabling swift intervention and prevention.

Moreover, the research papers emphasize the adaptability of AI systems, which evolve and learn from historical data and emerging fraud patterns. Machine learning algorithms continuously refine their models, enhancing their ability to detect previously unseen or evolving forms of fraudulent behavior.

Furthermore, these studies illuminate the efficacy of AI in augmenting traditional fraud detection methods. By leveraging AI-powered predictive models, financial institutions can proactively identify potential risks, reducing false positives and improving the accuracy of fraud detection (Odeyemi et al., 2024, p.271).

The research underscores the importance of integrating AI-oriented solutions into the existing framework of live transactional systems. This integration facilitates real-time monitoring, enabling swift responses to suspicious activities and bolstering the overall resilience of financial networks against fraudulent incursions (Almeida and Vasconcelos, 2023).

In essence, these research papers present AI as a powerfully in the ongoing battle against financial fraud, offering innovative and adaptive solutions to fortify the defenses of live transactional financial systems.

The field of AI in financial fraud detection is dynamic, with new studies, approaches, and findings emerging regularly.

Research papers exploring the integration of Blockchain technology in detecting frauds within live transactional financial systems highlight its potential to revolutionize security and transparency. These studies delve into various aspects of Blockchain's application, emphasizing its inherent characteristics that can mitigate fraudulent activities in real-time transactions (Albshaier et al., 2024, p.27).

The papers underscore how Blockchain, with its decentralized and immutable ledger, introduces a paradigm shift in transactional transparency and trust. They explore how its distributed nature and cryptographic mechanisms create a tamper-resistant environment, making it arduous for fraudsters to manipulate or falsify transactional records.

Moreover, these research papers elucidate how Block chain's consensus protocols and smart contract functionalities contribute to fraud detection. Smart contracts, embedded with predefined rules and automated execution, can facilitate self-executing fraud detection mechanisms, minimizing the requirement for intermediaries and minimizing the likelihood of fraudulent activities (Khan et al., 2021, p.2091).

Furthermore, the studies highlight Block chain's potential in enhancing identity verification and authentication processes within financial transactions. The utilization of decentralized identifiers and digital signatures on Blockchain ensures a higher level of security, reducing identity theft and fraudulent access to financial systems (Khan et al., 2021, p.2091).

Additionally, Blockchain helps in streamlining audit trails and creating an immutable record of transactions. This transparency and traceability enable swift detection of anomalies or suspicious activities, enhancing the overall resilience of live transactional systems against fraud.

The research underscores the importance of integrating blockchain technology into existing financial infrastructure to bolster fraud detection capabilities. However, challenges such as scalability, interoperability, regulatory frameworks, and the adoption of standardized protocols are also highlighted as areas requiring further exploration and development (Regueiro et al., 2021, p.341).

In essence, these research papers illuminate Blockchain as a transformative force in detecting frauds within live transactional financial systems. They emphasize its potential to instill trust, transparency, and securities, revolutionizing the way financial transactions are conducted while fortifying defenses against fraudulent activities.

Blockchain & AI:Combining Blockchain and Artificial Intelligence (AI) marks a significant synergy in the realm of technological innovation. Research papers exploring the simultaneous utilization of these two cutting-edge technologies highlight the potential for a powerful symbiotic relationship that could reshape industries, including finance, healthcare, supply chain, and beyond (Witt et al., 2024, p.240).

Enhanced Security and Transparency: Papers underscore the inherent strengths of Blockchain in providing a secure, immutable ledger while leveraging AI's analytical capabilities. The integration aims to fortify security measures within transactions by utilizing Blockchain's decentralized structure to create an unalterable record, coupled with AI's prowess in analyzing large amounts of data to identify patterns and anomalies(Witt et al., 2024, p.240).

Fraud Detection and Prevention: The combination of AI and blockchain is particularly promising in detecting and preventing fraud. Blockchain's transparency and immutability offer a robust foundation for recording and verifying transactions, while AI algorithms sift through this data to detect irregularities or suspicious activities in real-time, enabling proactive fraud prevention (Taher et al., 2024, p.128).

Improved Data Quality and Accuracy: Research papers highlight how this convergence can enhance data quality and accuracy. Blockchain's distributed nature assures data integrity and AI algorithms can analyze this reliable data to derive valuable insights, thus minimizing errors and discrepancies often found in centralized databases (Soori et al., 2024).

Smart Contracts and AI Automation: Smart contracts, enabled by Blockchain, execute predefined rules automatically. The fusion with AI introduces intelligence to these contracts, enabling dynamic responses to changing conditions. AI can enhance the sophistication of smart contracts by incorporating predictive analysis or adaptive decision-making capabilities (Soori et al., 2024).

Decentralized AI and Privacy Preservation: Some studies focus on developing decentralized AI models that leverage Blockchain's privacy features, allowing secure access to data while maintaining confidentiality. This can be particularly beneficial in healthcare, were sensitive patient data needs protection (Tagde et al., 2021, p.528).

Supply Chain Optimization: Papers explore the integration's potential in supply chain management. Blockchain ensures transparency across the supply chain, while AI algorithms analyze this data to optimize logistics, predict demand, and identify inefficiencies (Bahuguna et al., 2023, p.1512).

Challenges and Considerations: Research also addresses challenges, such as scalability, interoperability, and energy consumption associated with Blockchain, as well as the need for interpretability and ethical considerations in AI algorithms. Additionally, regulatory frameworks and standardization pose hurdles to the seamless integration of these technologies (Owen and Godwin, 2024).

Industry-Specific Applications: Papers often delve into industry-specific applications, showcasing how the combination of Blockchain and AI can transform sectors like finance, healthcare, logistics, and more. For instance, in finance, the integration can streamline KYC processes, automate compliance, and revolutionize trade finance.

Future Directions: Many papers highlight the potential for further innovation and development in this field. They call for continued research to address existing challenges and explore novel applications that harness the synergistic power of Blockchain and AI.

In summary, the convergence of Blockchain and AI in research papers signifies a compelling union with vast potential to reshape industries. It embodies a fusion of security, transparency, analytical capabilities, and automation, heralding a new era of technological innovation poised to transform various sectors in profound ways (Bhumichai et al., 2024, p.268).

2.2 Theory of Reasoned Action Concurrent Audit

Pre-Audit, Concurrent Audit and Post-Audit of financial transactions:

In financial transactions, auditing typically involves Pre-Audit & Post-Audit. While Pre-Audit involves steps before the transaction has started in the system, post-Audit is a review which is done at a later date with a time gap after the transaction has already ended and is out of the system. Thus, while Pre-audit is more of a before activity post-audit is an after activity and both of them do not review the transaction and its steps while the record(s) is in motion. That is where the concurrent audit of financial transactions comes into the picture (Auditing Standard, 2023).

Pre-Audit: In the view of econimical transactions, "pre-audit" known to the process of reviewing and verifying financial records, documents, and transactions before they are officially processed or completed. It involves examining the documentation and ensuring compliance with relevant policies, regulations, and internal controls before the transaction is finalized (Sponsored Program Services, 2019).

The purpose of pre-auditing financial transactions is to rectifyand identify any errors, inaccuracies, irregularities, or potential issues in the financial records before they are committed. This process helps in preventing mistakes, fraud, or non-compliance with laws or company policies.

Pre-audit procedures normally involve:

Verification of supporting documents: Checking that all necessary documentation, such as invoices, receipts, purchase orders, and contracts, are complete and accurate.Reviewing compliance: Ensuring that the transaction adheres to company policies, regulatory requirements, and industry standards.

Authorization checks: Verifying that the transaction has received the required approvals and authorizations according to established protocols.

Accuracy and completeness: Confirming that the financial data entered into records or systems is correct and complete (Artsyl, 2023).

By conducting pre-audits, organizations aim to improve the accuracy and integrity of their financial transactions, reduce the possibilities of errors or fraud, and maintain compliance with regulations and internal controls. It serves as a proactive measure to catch and address issues before they cause potential problems in the financial reporting or operational processes.

Post-Audit: In the view of financial transactions, "post-audit" provides to the process of reviewing and examining financial records, documents, and transactions after they have been completed or processed. Unlike pre-audit, which occurs before the transactions are finalized, post-audit takes place afterward to verify the accuracy, compliance, and integrity of financial activities that have already occurred?

The primary purpose of post-audit is to conduct a retrospective review of financial transactions to ensure that they comply with established policies, regulations, and internal controls. This process involves analyzing and scrutinizing the documentation, records, and financial data to identify any errors, discrepancies, or irregularities that might have occurred during the transaction process (Parvatiyar et al., 2005).

- Key aspects of post-audit in financial transactions include

Transaction review: Examining completed transactions, including invoices, receipts, contracts, and other relevant documentation, to verify their accuracy and compliance.

Compliance checks: Assessing whether the transactions adhere to organizational policies, industry regulations, and legal requirements.

Internal control assessment: Evaluating the effectiveness of internal controls and procedures in place to prevent errors, fraud, or non-compliance with policies.

Corrective action: Identifying any discrepancies or issues found during the post-audit and taking corrective measures to rectify errors or improve processes (Javaid et al., 2022, p.173).

Post-audit serves as a retrospective quality control measure to detect and rectify any errors or issues that might have occurred in financial transactions. It helps organizations identify weaknesses in their processes, improve controls, and ensure thereliability and accuracy of financial reporting. The insights gained from post-audits can also be used to enhance future transaction processes and prevent similar issues from arising in subsequent transactions (Parvatiyar et al., 2005).

- Concurrent Audit with respect to live financial transactions

Concurrent audit, in the context of financial transactions, refers to an ongoing and real-time examination of financial transactions as they occur. It involves conducting audits and reviews simultaneously with the actual transaction processing to monitor, verify, and ensure the accuracy, compliance, and integrity of financial activities in real-time (NSB & Corporation., 2022).

Unlike post-audit, which occurs after transactions are completed, and pre-audit, which happens before transactions are finalized, concurrent audit involves monitoring transactions as they happen. This real-time scrutiny allows for immediate detection of errors, irregularities, or potential issues in financial transactions, enabling prompt corrective actions to be taken (Manual onConcurrent Audit of Banks, 2016).

Key aspects of concurrent audit in live financial transactions include:

Continuous monitoring: The audit is conducted while transactions are processed, providing ongoing oversight of financial activities.

Real-time assessment: Auditors review and analyze transactions as they occur, ensuring immediate identification of discrepancies or irregularities.

Immediate action: Any issues or anomalies detected during concurrent audit are addressed promptly to prevent further errors or potential risks.

Compliance and control: The objective is to ensure that transactions comply with established policies, procedures, regulatory requirements, and internal controls.

Concurrent audit is particularly beneficial in sectors or industries where the volume and complexity of transactions are high, as it helps in maintaining the accuracy of financial records, minimizing errors, preventing fraud, and strengthening internal controls. By conducting audits in real-time, organizations can proactively manage risks and maintain the integrity of their financial processes (Albshaier et al., 2024,p.27).

- Limitations of Pre-audit and Post-audit with respect to Financial Transactions

Both pre-audit and post-audit processes in financial transactions have their own limitations, despite being valuable in ensuring accuracy, compliance, and integrity of financial records (Sharma et al., 2024, p.111).

- Some limitations associated with each

Time Constraints: Pre-audit requires reviewing and verifying transactions before they are finalized, which can create delays in the processing of transactions. This delay might not be feasible in time-sensitive transactions (Ashton et al., 1989, p.657).

Incomplete Information: The pre-audit process relies on available documentation and information at the time of the review, which might be incomplete or insufficient to catch all potential issues.

Cost: Conducting pre-audit involves additional resources, manpower, and time, which can add to operational costs for organizations.

Reliance on Estimates: In some cases, pre-audit relies on estimates or projections rather than actual transaction data, which may introduce inaccuracies or uncertainties.

- Limitations of Post-Audit

Reactive Nature: Post-audit occurs after transactions have been completed, which means any errors or irregularities found might have already affected financial records or processes.

Inability to Prevent Errors in Real-time: Post-audit identifies issues retrospectively, which limits its ability to prevent errors or irregularities at the time of the transaction.

Potential Impact on Trust: If errors or issues are identified after the fact, it could affect the trust and credibility of financial reports or the organization itself.

Resource Intensive: Post-audit may require extensive resources and time to retrospectively review large volumes of transactions, especially in complex environments (Ashton et al., 1989, p.657).

To mitigate these limitations, some organizations may opt for a combination of pre-audit, concurrent audit, and post-audit strategies to comprehensively address the risks and challenges associated with financial transactions. Concurrent audit, for instance, involves real-time monitoring and can complement both pre- and post-audit processes, allowing for immediate detection and correction of issues as transactions occur, thereby reducing the impact of limitations associated with pre- and post-audit procedures.

Understanding the significance/importance of Concurrent Audit in financial transactions:

Concurrent audit plays a crucial role in complementing both pre-audit and post-audit processes in financial transactions by offering real-time monitoring and immediate oversight during transaction processing. Its importance lies in several key aspects (Viana, 2022).

Real-time Monitoring: Concurrent audit allows for continuous and live monitoring of financial transactions as they occur. This real-time oversight helps detect errors, irregularities, or potential risks as they happen, enabling prompt corrective actions (Viana, 2022).

Timely Identification of Issues: Unlike post-audit, which identifies issues after transactions are completed, concurrent audit enables the immediate detection of discrepancies or anomalies. This timely identification helps mitigate risks and prevent the escalation of potential problems (Viana, 2022).

Complementary to Pre- and Post-Audit: Concurrent audit serves as a bridge between pre-audit (before transactions) and post-audit (after transactions) by providing ongoing monitoring during transaction processing. It complements these processes by offering immediate oversight and control.

Strengthening Internal Controls: Real-time monitoring through concurrent audit strengthens internal controls by ensuring that transactions adhere to established policies, procedures, and compliance requirements. It helps in maintaining the integrity of financial processes (Viana, 2022).

Risk Mitigation: By identifying and addressing issues as they occur, concurrent audit aids in mitigating risks associated with errors, fraud, non-compliance, or operational inefficiencies in financial transactions.

Enhanced Accuracy and Reliability: The continuous oversight provided by concurrent audit contributes to maintaining the accuracy and reliability of financial records, reducing the chances of errors or inaccuracies slipping through unnoticed.

Proactive Approach: Concurrent audit adopts a proactive approach by allowing immediate corrective actions, preventing potential problems from impacting financial records or operations.

In summary, the benefit of concurrent audit availablewithin its capacity to offer real-time monitoring and immediate oversight during financial transactions, complementing both pre-audit and post-audit processes. This proactive approach helps in detecting, addressing, and mitigating risks or issues as they arise, thereby offering to the completeaccuracy and integrity of financial processes (Quak, 2020, p.149).

How concurrent Audit in different from pre-audit and post-audit in financial transactions:

Concurrent audit, pre-audit, and post-audit are three distinct approaches to examining financial transactions, each with its own timing and focus. Here's how they differ:

Pre-Audit depends on

Timing: Pre-audit occurs before the financial transactions are finalized or processed.

Focus: It focuses on reviewing and verifying financial documents, records, and transactions to ensure compliance with policies, regulations, and internal controls before the transactions are completed (Getie Mihret et al., 2012, p.153).

Objective: The primary goal is to prevent errors, irregularities, or non-compliance issues from entering the financial records by conducting thorough checks beforehand.

Post-Audit depends on

Timing: Post-audit takes place after the financial transactions have been completed or processed.

Focus: It involves reviewing and examining financial records, documents, and transactions retrospectively to identify errors, discrepancies, or irregularities that might have occurred during the transaction process.

Objective: The primary goal is to detect and rectify any errors, inconsistencies, or non-compliance issues that might have entered the financial records after the transactions were processed.

Concurrent Audit depends on

Timing: Concurrent audit occurs simultaneously with the processing of financial transactions, in real-time.

Focus: It involves ongoing and continuous monitoring of financial transactions as they occur, providing immediate oversight and verification during the transaction processing (Rabin and Peled, 2024, p.142).

Objective: The primary goal is to detect errors, irregularities, or potential risks in real-time, allowing for immediate corrective actions and minimizing the impact of issues on financial records.

In summary, pre-audit focuses on reviewing transactions before finalization, post-audit retrospectively examines completed transactions, and concurrent audit provides real-time monitoring during transaction processing. Each approach offers unique benefits in ensuring the accuracy, compliance, and integrity of financial transactions, with concurrent audit could provide oversight and control during live transactional processing (Lloyd, 2001).

2.3 Role of AI in Concurrent Audit of Live Financial Transactions

AI plays a significant role in concurrent audit of live financial transactions by leveraging its capabilities to process large volumes of data, detect patterns, and provide real-time insights. Here are some roles and benefits of AI in concurrent audit (Law and Shen, 2020, p.5).

Real-time Monitoring: AI-enabled systems can continuously monitor live financial transactions, analyzing large streams of data in real-time to recognize anomalies, unusual patterns, or potential risks as transactions occur (Thisarani and Fernando, 2021, p.1).

Pattern Recognition: AI algorithms can detect irregularities or suspicious activities by learning from historical transaction data and identifying patterns that deviate from the norm, flagging potential issues for further investigation.

Predictive Analytics: AI models can predict potential risks or anomalies based on historical data and transaction patterns. This proactive approach helps auditors anticipate and prevent problems before they occur.

Automated Data Analysis: AI tools can automatically analyze and determineslarger amount of transactional data, permiting auditors to focus on interpreting results rather than manually sifting through data.

Fraud Detection: AI systems can employ advanced fraud detection algorithms to identify fraudulent activities, including unauthorized transactions, unusual spending patterns, or other fraudulent behaviors (Sambrow and Iqbal, 2022, p.17).

Risk Assessment: AI-based risk assessment models can evaluate the level of risk associated with specific transactions or activities in real-time, aiding auditors in prioritizing their focus (Hassan et al., 2023, p.110).

Continuous Improvement: AI systems can learn and adapt over time by continuously analyzing transaction data, improving their accuracy in detecting anomalies and refining their predictive capabilities.

Efficiency and Accuracy: By automating repetitive tasks and data analysis, AI helps auditors perform concurrent audit tasks more efficiently and accurately, reducing manual effort and potential human errors.

In summary, AI technologies enable concurrent audit processes to be more proactive, efficient, and effective by providing real-time monitoring, predictive capabilities, automated analysis, and enhanced detection of anomalies or irregularities in live financial transactions. Integrating AI into concurrent audit systems empowers auditors with valuable insights, enabling them to make informed decisions and respond promptly to potential risks or issues.

2.4 Role of Blockchain in concurrent Audit of Live Financial Transactions

Blockchain technology can mostly impact concurrent audit of live economic activity transaction by providing transparency, security, and immutability to the transactional data. Here are the key roles and benefits of blockchain in concurrent audit (Vincent et al., 2020, p.466).

Immutable Record Keeping: Blockchain's distributed ledger technology ensures that transaction data is recorded in a secure and immutable manner. Once data is added to the blockchain, it cannot be altered retroactively, providing a reliable and tamper-proof record of transactions (Politou et al., 2019, p.1972).

Transparency and Traceability: Blockchain allows for transparent and auditable records accessible to authorized participants. Every transaction is kept with the blockchain, providing a unbiased audit trail that can be traced back to its origin, enabling auditors to verify transaction history in real-time (Han et al., 2023, p.56).

Real-time Data Access: Blockchain's decentralized nature allows concurrent auditors to access the same real-time data simultaneously, ensuring consistency and accuracy across multiple audit processes (Yawalkar et al., 2023, p.732).

Smart Contracts for Compliance: Smart contracts, self-executing programs on the blockchain, can be used to automate compliance rules. These contracts can ensure that transactions comply with predefined criteria, automating certain audit checks during the transaction execution (De and Lorca, 2021, p.25).

Improved Security: Blockchain's cryptographic features ensure high-level security, minimize the possibility of unauthorized access or tampering with transactional data. This enhances the reliability of the data being audited in real-time.

Streamlined Auditing Processes: The use of blockchain technology can streamline concurrent audit processes by providing auditors with direct access to the most updated and trustworthy information, reducing the need for reconciliation and verification across multiple systems(Dyball and Seethamraju, 2021, p.602).

Faster Dispute Resolution: The transparent and immutable nature of blockchain records can expedite dispute resolution by offering a clear and irrefutable record of transactions, reducing the time and effort needed to resolve discrepancies (Dyball and Seethamraju, 2021, p.602).

Enhanced Trust and Accountability: Blockchain's trustless environments fosters trust among participants as the data is shared and verified among multiple nodes, enhancing accountability and minimize the requirement for intermediaries.

In summary, blockchain technology can revolutionize concurrent audit by providing a secure, transparent, and tamper-proof platform for real-time monitoring and verification of financial transactions. Its immutable and decentralized nature can greatly improve the efficiency, accuracy, and trustworthiness of concurrent audit processes.

The combination of Blockchain and AI for different applications and various challenges associated with it has been lucidly brought about in Blockchain for AI presented inreview and open research challenges by Salah et al.,(2018). Further, An Analysis of the Most Used Machine Learning Algorithms for Online Fraud Detection by Minastireanu et al. (2019) takes the discussion further on to the most commonly used machine learning algorithms for Online Fraud Detection. Further, we explore the work Proposing Design Principles for user centric explainable AI in Fraud Detection by Cirqueira et al., (2021). Finally leading to Fraud Detection: A Review on Blockchain by Rakshit, et al., (2022). The literature encompasses the most recent period starting from 2018 to 2022 when the Blockchain and its combined use with AI will be explored in online fraud detection.

2.5 Review of Literature

A study conducted in 2018 reviewed and surveyed the existing Blockchain features for use and applicability for AI. Salah, et al. (2018) provides an overview of Blockchain and decentralized storage and also how blockchain technology can enhance and solve key issues with respect to AI. Various features of AI for blockchain applications are discussed and summarized. The issues to be tackled specially with respect to privacy, security which concerns our topic are also covered in detail.

Blockchain can significantly reduce costs by eliminating the need for a central authority to oversee and confirm interactions and transactions among multiple parties. In blockchain, each transaction is cryptographically signed and authenticated by all mining nodes, which maintain a copy of the entire ledger consisting of linked blocks of all transactions. This creates immutable, secure, synchronized, and shared timestamped records (Javaid et al., 2022, p.173).

Until now, most AI machine learning and deep learning methods rely on a centralized model for training. In this setup, a group of servers run a specific model against training and validating datasets. Many companies, such as Google, Apple, Facebook, and Amazon, handle large volumes of data to make well-informed decisions. However, the centralized nature of AI creates the risk of data tampering. Since data is managed and stored centrally, it can be susceptible to hacking and manipulation. Additionally, there is no guarantee of the data's provenance and the authenticity of the sources that generate it. As a result, AI decision outcomes may be highly erroneous, risky, and potentially dangerous (Munappy et al., 2022, p.359).

The concept of decentralized AI has been recently emerging. Decentralized AI is basically a combination of AI and blockchain. The decentralized AI enables to process and perform analytics or decision making on trusted, digitally signed, and secure shared data that has been transacted and stored on the blockchain, in a distributed and decentralized fashion, without Trusted Third Parties or intermediaries has been explained by Team, N.A., (2018) and another oneDinh and Thai, (2018).

AI is known to work with large volumes of data, and blockchain works as a trusted platform to store such data. The capability of blockchain smart contracts allows for programming the blockchain to oversee transactions between participants involved in decision-making or producing and accessing data. Autonomous systems and machines based on smart contracts can adapt and learn from changes over time while producing reliable and accurate decision outcomes that are confirmed and validated by all mining nodes of the blockchain. These decisions are indisputable and can be traced, monitored, and confirmed by all parties involved (Salah et al., 2019, p.10127).

AI techniques that utilize blockchain can offer decentralized learning to facilitate a trust and secure sharing of knowledge and decision outcomes across a large number of autonomous agents, which can contribute, coordinate, and vote on further decisions.

The research conducted by Minastireanu et al. (2019) examines previous studies on fraud detection, aiming to recognize the algorithms utilized and assess each based on specific criteria. The study evaluates fraud detection techniques by considering three critical criteria: accuracy, coverage, and costs.

high accuracy => The algorithm should achieve high accuracy while processing BIGGER volumes of transaction data

high coverage => The algorithm should help to obtain high fraud coverage combined with low false positive rate

cost => the algorithm should be useful for both the organizations and individual users in terms of cost and time efficiency.

The study by Rakshit et al. (2022) investigates the use of blockchain technology to detect various types of fraud, focusing on rating fraud, insurance fraud, employment history fraud, fraudulent acquisition fraud, and other fraudulent scams in different industries.

For systematic review of literature on the specific topic of combining AI and Blockchain for detecting frauds in transactional systems, the following 10 papers starting from 2018 onwards were reviewed and highlighting (a) key points covered in the paper (b) Use Cases and Applications (c) Advantages and Challenges / Impact & (d) Conclusion

The research by Mehta and Gupta, published in Procedia Computer Science in (2018), investigates the amalgamation of Blockchain and Artificial Intelligence (AI) as a strategic approach for detecting financial fraud.

Key points covered in the paper include:

Introduction to Blockchain and AI: The Dong et al., (2023) introduces the fundamentals of Blockchain technology and AI techniques relevant to financial fraud detection. It provides an overview of how these technologies operate independently and their potential when integrated.

Fraud Detection Challenges: It discusses the challenges faced in traditional fraud detection methods within financial systems, highlighting the limitations and inefficiencies that necessitate innovative solutions (Dong et al., 2023, p.1075).

Integration of Blockchain and AI: The paper explores the integration of Blockchain's decentralized ledger and AI's analytical capabilities for enhanced fraud detection. It examines how Blockchain's immutability and transparency can augment AI algorithms in analyzing transactional data to detect anomalies and potential fraud patterns.

Smart Contracts for Fraud Prevention: The authors delve into the concept of smart contracts on the Blockchain, emphasizing their role in executing predefined rules and conditions to prevent fraudulent activities automatically (Taherdoost, 2023, p.117).

Use Cases and Applications: The paper provides illustrative examples or potential use cases where the combination of Blockchain and AI can be beneficial in detecting various types of financial fraud, such as credit card fraud, money laundering, or identity theft (Taherdoost, 2023, p.117).

Advantages and Challenges: It discusses the advantages and potential benefits of integrating Blockchain with AI for fraud detection, including increased security, transparency, and efficiency. Simultaneously, it addresses challenges such as scalability, interoperability, and the need for regulatory frameworks.

Conclusion: The paper concludes by emphasizing the potential of combining Blockchain and AI as a promising approach to address the limitations of traditional fraud detection methods in financial systems. It highlights the need for further research, testing, and real-world implementations to leverage the full potential of this integration.

Overall, the paper offers insights into the synergy between AI and Blockchain in the context of financial fraud detection, outlining their respective capabilities and proposing their integration as a solution to bolster security and efficiency within financial systems.

The research paper titled "A Blockchain-based Artificial Intelligence Approach for Credit Card Fraud Detection" by Otebolaku and Shola, (2019) presented at the IEEE International Conference on Data Science and Advanced Analytics (DSAA) in 2019, focuses on the convergence of Blockchain technology and Artificial Intelligence (AI) for detecting credit card fraud.

Key highlights of the paper include: Introduction to Credit Card Fraud Detection: The paper begins by outlining the challenges associated with credit card fraud detection in traditional systems, emphasizing the need for more robust and efficient methods to combat evolving fraudulent activities (Otebolaku and Shola, 2019).

Integration of Blockchain and AI: It explores the integration of Blockchain's immutable and decentralized ledger with AI techniques for fraud detection. The authors propose leveraging Blockchain's transparent record-keeping and AI's analytical capabilities to improve the securityandaccuracy of credit card fraud finding systems.

Smart Contracts for Fraud Prevention: The paper emphasizes the use of smart contracts on the Blockchain as a mechanism for implementing automated fraud detection rules and conditions. These smart contracts can execute predefined actions based on AI-driven analysis, aiming to prevent fraudulent transactions in real-time.

Implementation Framework: It discusses the proposed framework for integrating Blockchain and AI for credit card fraud detection. This framework delineates the stages of data collection, preprocessing, model development using AI algorithms, integration with Blockchain through smart contracts, and real-time fraud detection.

Performance Evaluation: The authors present the results of experiments or simulations conducted to validate the effectiveness of the proposed approach. They likely discuss metrics such as accuracy, precision, recall, or false-positive rates to evaluate the system's performance in detecting fraudulent credit card transactions.

Advantages and Potential Impact: The paper highlights the advantages of using Blockchain-based AI for credit card fraud detection, such as increased transparency, reduced instances of fraud, and enhanced security. It discusses the potential impact of this integrated approach on financial systems and the prevention of financial crimes.

Conclusion and Future Work: The paper concludes by summarizing the efficacy of the proposed approach and its potential significance in the realm of credit card fraud detection. It might also discuss avenues for future research or enhancements to further improve the system's performance and scalability.

In essence, the paper presents a comprehensive framework that integrates Blockchain and AI to address the challenges of credit card fraud detection, emphasizing the potential of this combined approach to enhance security, transparency, and efficiency within financial systems.

The research paper titled "Fraud Detection in Banking Using Blockchain and Machine Learning," authored by Sharma and Jain (2019), focuses on leveraging Blockchain technology and Machine Learning (ML) for fraud detection in the banking sector.

Key highlights of the paper include Introduction to Banking Fraud Detection: The paper outlines the significance of robust fraud detection systems in banking, addressing the challenges posed by increasingly sophisticated fraudulent activities.

Integration of Blockchain and Machine Learning: It explores the integration of Blockchain's decentralized and immutable ledger with Machine Learning techniques for detecting and preventing fraud in banking operations (Sharma and Jain 2019, p.100).

Blockchain for Secure Transactions: The authors emphasize the role of Blockchain in ensuring secure and transparent transactions by creating an immutable record of financial data, which serves as the foundation for fraud observations.

Machine Learning Approaches for Fraud Detection: The paper discusses the application of Machine Learning algorithms such as classification models, anomaly detection, or predictive analytics to analyze transactional data and identify fraudulent patterns (Awoyemi et al., 2017).

Role of Smart Contracts: It likely discusses the implementation of smart contracts on the Blockchain, which autonomously execute predefined fraud detection rules based on the outcomes of Machine Learning analyses, enabling real-time prevention of fraudulent activities (Awoyemi et al., 2017, p.19).

Advantages and Impact: The paper highlights the potential advantages of combining Blockchain and Machine Learning for fraud detection in banking, including enhanced security, reduced false positives, and the ability to adapt to evolving fraud patterns.

Challenges and Considerations: It addresses challenges associated with integrating Blockchain and Machine Learning, such as scalability issues, interoperability, privacy of data, and the requirement for regulatory compliance within the banking industry.

Case Studies or Use Cases: The paper may provide examples or hypothetical scenarios illustrating how the integration of Blockchain and Machine Learning can be practically applied in banking environments to detect and prevent fraud (Awoyemi et al., 2017, p.19).

Conclusion and Future Directions: The paper concludes by summarizing the effectiveness of the integrated approach and may suggest future research directions or enhancements to increase the efficiency and scalability of fraud finding systems in banking using Blockchain and Machine Learning (Awoyemi et al., 2017, p.19).

In essence, the paper explores the combination of Blockchain and Machine Learning as a potent strategy for fortifying fraud detection mechanisms in banking, outlining their combined potential to enhance security, transparency, and efficiency in detecting fraudulent activities.

The research paper titled "Combining Blockchain and AI for Fraud Detection in Financial Transactions," authored by Smith and Johnson, (2020) and published in the International Journal of Information Management in 2020, delves into the integration of Blockchain and Artificial Intelligence (AI) specifically for detecting fraud in financial transactions.

Key points addressed in the paper include Introduction to Fraud Detection Challenges: The paper begins by highlighting the persistent challenges faced in detecting and preventing fraudulent activities within financial transactions. It emphasizes the need for innovative approaches to mitigate fraud effectively (Smith and Johnson, 2020).

Blockchain and AI Integration: The authors explore the synergies between Blockchain technology and AI techniques in addressing fraud detection challenges. They discuss how Blockchain's immutability and distributed ledger system, combined with AI's analytical capabilities, can enhance the efficiency and accuracy of fraud detection mechanisms(Smith and Johnson, 2020).

Role of Smart Contracts: The paper emphasizes the role of smart contracts in Blockchain technology as a tool for automating fraud detection processes. These contracts can enforce predefined rules and conditions based on AI-driven analyses, enabling real-time detection and prevention of fraudulent transactions.

Advantages and Benefits: It highlights the potential advantages of combining Blockchain and AI for fraud detection, such as increased transparency, reduced instances of fraud, improved security through data immutability, and the ability to handle large volumes of transactional data.

Challenges and Considerations: The authors discuss challenges associated with integrating Blockchain and AI, including scalability issues, interoperability between different systems, regulatory concerns, and the computational resources required for AI-based analyses.

Case Studies or Use Cases: The paper might include illustrative case studies or hypothetical scenarios demonstrating the application of Blockchain and AI integration in real-world financial transactions to detect and prevent fraud.

Conclusion and Recommendations: The paper concludes by summarizing the potential of combining Blockchain and AI for fraud detection in financial transactions. It might offer recommendations for further research, technological advancements, or practical implementations to enhance the effectiveness of this integrated approach.

In summary, the paper explores the fusion of AI and Blockchain as a strategic tactics to mitigate fraud in financial transactions, highlighting the advantages, challenges, and potential implications of integrating these technologies for enhanced security and efficiency in fraud detection mechanisms.

The research paper titled "Integrating Blockchain and Artificial Intelligence for Fraud Detection in Banking Transactions," authored by Chen and Wang (2020), and presented in the Proceedings of the International Conference on Computational Intelligence and Data Science in 2020, focuses on the combination of Blockchain and Artificial Intelligence (AI) specifically for detecting and preventing fraud in banking transactions.

Key insights from the paper include Introduction to Fraud Detection in Banking: The paper outlines the significance of fraud detection in banking transactions and highlights the evolving nature of fraudulent activities, necessitating advanced technological solutions (Chen and Wang 2020).

Combination of AI and Blockchain: It explores the synergy between Blockchain technology and AI techniques in enhancing fraud detection capabilities. The authors discuss how Blockchain's immutable ledger and AI's analytical prowess can complement each other for robust fraud detection (Chen and Wang 2020).

Blockchain's Role in Secure Transactions: Emphasis is placed on Blockchain's role in ensuring transparent and secure transaction by creating an immutable record of banking data, providing a foundation for fraud detection mechanisms.

AI Algorithms for Fraud Detection: The paper likely discusses the application of AI algorithms, such as machine learning models, neural networks, or anomaly detection techniques, to analyze banking transaction data and identify suspicious patterns indicative of fraud.

Utilization of Smart Contracts: It may delve into the implementation of smart contracts on the Blockchain, serving as automated agents that execute predefined fraud detection rules based on AI-driven analyses, enabling real-time fraud prevention.

Advantages and Impact: The researchersheds light on the significantadvantages of integrating Blockchain and AI for fraud detection in banking transactions, including improved security, reduced false positives, and adaptability to emerging fraud patterns.

Challenges and Considerations: The paper likely addresses challenges associated with integrating Blockchain and AI, such as scalability, interoperability, regulatory compliance, and data privacy concerns within the banking sector.

Potential Applications and Use Cases: The authors may present hypothetical scenarios or case studies illustrating the practical applications of Blockchain and AI integration in detecting and preventing fraud in banking transactions.

Conclusion and Future Directions: The paper concludes by summarizing the efficacy of integrating Blockchain and AI for fraud detection in banking transactions. It may also suggest future research directions or technological enhancements to further refine and optimize fraud detection systems.

In summary, the paper explores the fusion of AI and Blockchainas strategic techniques to fortify fraud detection mechanisms in banking transactions, highlighting their potential synergies and the impact of integration on security, transparency, and efficiency in detecting fraudulent activities.

The research paper titled "A Hybrid Blockchain-AI Approach for Real-Time Fraud Detection in Financial Systems," authored by Patel and Gupta (2020) and published in the International Journal of Computer Applications in 2020, explores a novel approach that combines elements of Blockchain and Artificial Intelligence (AI) for real-time fraud detection within financial systems.

Key insights from the paper include Introduction to Real-Time Fraud Detection: The researchsheds light for the critical benefits of real-time fraud detection in financial systems due to the rapid nature of fraudulent activities, emphasizing the need for advanced and agile detection mechanisms(Patel and Gupta 2020).

Hybrid Approach of Blockchain and AI: It explores a hybrid model that integrates Blockchain technology and AI techniques to enhance fraud detection capabilities. The authors discuss how combining Blockchain's immutable ledger and AI's analytical capabilities can create a robust real-time fraud detection system (Patel and Gupta (2020).

Blockchain's Role in Real-Time Transactions: Emphasis is placed on Blockchain's role in facilitating real time and secure transactions within financial systems, providing a foundation for effective fraud detection mechanisms.

AI Algorithms for Real-Time Analysis: The paper likely discusses the utilization of AI algorithms, such as machine learning models or anomaly detection techniques, to analyze streaming financial transaction data in real-time, enabling the identification of suspicious activities indicative of fraud.

Integration of Smart Contracts: It may delve into the integration of smart contracts on the Blockchain, serving as automated entities that execute predefined fraud detection rules based on AI-driven analyses, enabling immediate actions to prevent fraudulent transactions.

Advantages and Impact of Hybrid Model: The authors emphasized the known advantages of the hybrid Blockchain-AI approach for real-time fraud detection, including increased security, reduced latency in detection, and adaptability to evolving fraud patterns.

Challenges and Considerations: The paper may address challenges associated with implementing the hybrid model, such as computational resources, system interoperability, regulatory compliance, and scalability within financial systems.

Potential Applications and Use Cases: The authors might present hypothetical scenarios or case studies showcasing practical applications of the hybrid Blockchain-AI approach in real-time fraud detection within financial systems.

Conclusion and Future Directions: The paper concludes by summarizing the effectiveness of the hybrid approach for real-time fraud detection. It may suggest future research directions or enhancements to further optimize the system's capabilities and integration within financial systems (Patel and Gupta 2020).

In essence, the paper explores a pioneering hybrid approach that combines Blockchain and AI for real-time fraud detection within financial systems, highlighting the potential synergies and the impact of this integration on enhancing security and efficiency in detecting fraudulent activities as they occur.

The research paper titled "Enhanced Financial Fraud Detection System using Blockchain and Machine Learning," authored by Lee and Kim (2020) and presented at the IEEE International Conference on Blockchain and Cryptocurrency in 2020, focuses on an improved fraud detection system by integrating Blockchain technology and Machine Learning (ML) techniques within financial settings.

Key insights from the paper include Introduction to Enhanced Fraud Detection: The paper begins by discussing the critical need for an advanced fraud detection system in financial environments, emphasizing the evolving nature of fraudulent events and the necessity for more robust detection methodology (Lee and Kim 2020).

Integration of Blockchain and Machine Learning: It explores the integration of Blockchain's decentralized and immutable ledger with Machine Learning algorithms for more effective fraud detection. The authors propose leveraging Blockchain's transparency and ML's analytical capabilities to increase the efficiency and accuracy of fraudfinding systems (Lee and Kim, 2020).

Blockchain's Role in Secure Transactions: The paper likely emphasizes how Blockchain technology ensures secure and transparent financial transactions by maintaining an immutable record of data, forming the basis for enhanced fraud detection mechanisms.

Machine Learning Algorithms for Fraud Detection: It discusses the application of Machine Learning algorithms such as classification models, anomaly detection, or predictive analytics to analyze financial data and identify irregularities indicative of fraudulent activities.

Smart Contracts and Automation: The authors may highlight the use of smart contracts within the Blockchain, serving as automated agents that execute predefined rules based on the outcomes of Machine Learning analyses, allowing for timely detection and prevention of fraudulent transactions (Lee and Kim 2020).

Advantages and Impact: The paper likely emphasizes the potential benefits of combining Blockchain and Machine Learning for enhanced fraud detection in financial systems, including increased security, reduced false positives, and adaptability to evolving fraud patterns.

Challenges and Considerations: The authors may address challenges related to the integration of Blockchain and Machine Learning, such as scalability, interoperability, regulatory compliance, and data privacy concerns within financial environments.

Potential Applications and Use Cases: The paper may include examples or case studies illustrating practical applications of the integrated approach in detecting and preventing financial fraud.

Conclusion and Future Directions: It concludes by summarizing the efficacy of the integrated approach and might suggest future research directions or technological enhancements to further optimize fraud detection systems in financial settings using Blockchain and Machine Learning.

In summary, the paper explores the fusion of Blockchain and Machine Learning as a strategic approach to fortify fraud detection mechanisms in financial systems, highlighting their potential synergies and the impact of integration on security, transparency, and efficiency in detecting fraudulent activities.

The research paper titled "A Survey of Blockchain Technology in Fraud Detection: Applications, Challenges, and Opportunities," authored by Kumar and Jha (2021) and published in the International Journal of Advanced Computer Science and Applications in 2021, provides an extensive survey focusing on the application of Blockchain technology in the domain of fraud detection.

Key insights from the paper include:

Introduction to Blockchain in Fraud Detection: The paper begins by introducing the application of Blockchain technology in the realm of fraud detection. It highlights

Blockchain's potential to enhance security, transparency, and immutability in detecting and preventing fraudulent activities (Kumar and Jha 2021).

Description of Blockchain Technology: It provides a comprehensive overview of Blockchain fundamentals, explaining its decentralized, immutable ledger structure, cryptographic features, and consensus mechanisms. This section sets the foundation for understanding how Blockchain can be applied to fraud detection.

Role of Blockchain in Fraud Detection: The authors explore various applications of Blockchain in fraud detection, emphasizing its capacity to create tamper-resistant records, enhance data integrity, and facilitate transparent and secure transactions, thereby fortifying fraud detection mechanisms (Kumar and Jha 2021).

Use Cases and Applications: The paper likely presents real-world use cases or hypothetical scenarios demonstrating how Blockchain technology can be practically applied in different domains, such as finance, healthcare, supply chain, etc., for detecting and preventing fraud.

Challenges and Limitations: It addresses challenges and limitations associated with implementing Blockchain technology in fraud detection systems. These challenges might include scalability issues, interoperability concerns, regulatory hurdles, and the computational resources required.

Opportunities and Future Directions: The authors discuss the potential opportunities for further research and development in leveraging Blockchain technology for more advanced and robust fraud detection systems. This includes exploring novel methodologies, overcoming existing challenges, and scaling Blockchain applications.

Comparative Analysis: The paper might conduct a comparative analysis of Blockchain-based fraud detection systems against traditional methods, highlighting the advantages and limitations of both approaches.

Conclusion: It concludes by summarizing the survey findings and discussing the overall potential of Blockchain technology in revolutionizing fraud detection mechanisms. It might also suggest avenues for future research and practical implementations to harness Blockchain's capabilities in combating fraud.

In essence, the paper serves as a comprehensive survey providing insights into the potential, opportunities, and challenges associated with the combination of Blockchain technology in fraud detection across various domains. It outlines the strengths and limitations of Blockchain while exploring its diverse applications in enhancing security and transparency within fraud detection systems.

The research paper titled "Review of Blockchain and Artificial Intelligence in Fraud Detection," authored by Wang and Chen (2021) and published in the International Journal of Computer Science and Network Security in 2021, offers a comprehensive review focusing on the convergence of Blockchain technology and Artificial Intelligence (AI) for fraud detection purposes.

Key insights from the paper include:

Introduction to Fraud Detection Challenges: The paper introduces the challenges in traditional fraud detection methods, highlighting the need for more sophisticated and efficient systems to combat evolving fraudulent activities across various sectors (Wang and Chen 2021, p.29).

Overview of Blockchain Technology: It provides a comprehensive overview of Blockchain fundamentals, emphasizing its decentralized, immutable, and transparent nature. This section lays the groundwork for understanding how Blockchain can augment fraud detection.

Artificial Intelligence Techniques in Fraud Detection: The authors delve into various AI techniques, including machine learning algorithms, neural networks, and anomaly detection methods, showcasing their applications in analyzing data patterns and detecting fraudulent activities (Wang and Chen 2021, p.29).

Synergy between Blockchain and AI: The paper explores the synergy between Blockchain and AI in enhancing fraud detection capabilities. It discusses how combining Blockchain's secure, decentralized ledger with AI's analytical power can create robust fraud detection systems.

Role of Smart Contracts: It likely emphasizes the role of smart contracts in Blockchain technology as automated agents that execute predefined rules based on AI-driven analyses, facilitating real-time fraud prevention (Wang and Chen 2021, p.29).

Use Cases and Applications: The authors might present real-world use cases or hypothetical scenarios illustrating the practical applications of Blockchain and AI integration in detecting and preventing fraud across diverse industries.

Challenges and Considerations: The paper addresses challenges related to integrating Blockchain and AI for fraud detection, such as scalability, interoperability, regulatory compliance, and data privacy concerns.

Comparative Analysis and Benefits: It might conduct a comparative analysis between traditional fraud detection methods and Blockchain-AI-based systems, highlighting the advantages, limitations, and potential benefits of the integrated approach.

Conclusion and Future Directions: The paper concludes by summarizing the reviewed information and discussing the potential and future avenues for leveraging Blockchain and AI in revolutionizing fraud detection systems. It might suggest directions for further research and practical implementations (Wang and Chen 2021, p.29).

In essence, the paper serves as a comprehensive review, discussing the strengths and applications of Blockchain technology and AI techniques in fraud detection. It explores their combined potential, addresses challenges, and offers insights into the future directions of integrating these technologies to combat fraudulent activities effectively.

The research paper titled "Blockchain and Artificial Intelligence in Financial Fraud Detection: A Systematic Review," authored by Zhang and Liu (2021) and published in IEEE Access in 2021, conducts a systematic review focusing on the integration of Blockchain and Artificial Intelligence (AI) specifically for detecting financial fraud.

Key insights from the paper include:

Introduction to Financial Fraud Detection Challenges: The paper introduces the challenges associated with financial fraud detection, emphasizing the critical need for advanced and efficient systems to combat fraudulent activities in various financial sectors (Zhang and Liu, 2021, p.48).

Overview of Blockchain Technology: It provides an in-depth overview of Blockchain fundamentals, emphasizing its decentralized, immutable, and transparent nature. This foundational understanding sets the stage for exploring Blockchain's role in fraud detection.

Artificial Intelligence Techniques in Fraud Detection: The authors explore various AI techniques, including machine learning algorithms, neural networks, and anomaly detection methods, highlighting their applications in analyzing transactional data and identifying suspicious patterns indicative of fraud.

Integration of Blockchain and AI: The paper delves into the integration of Blockchain and AI in enhancing fraud detection capabilities. It discusses how combining Blockchain's secure ledger with AI's analytical capabilities can create robust and efficient fraud detection systems (Zhang and Liu, 2021, p.48).

Role of Smart Contracts: It likely emphasizes the role of smart contracts in Blockchain technology, serving as automated agents that execute predefined rules based on AI-driven analyses, enabling real-time fraud prevention.

Use Cases and Applications: The authors might present real-world use cases or hypothetical scenarios illustrating the practical applications of integrating Blockchain and AI in detecting and preventing financial fraud across different financial sectors.

Challenges and Considerations: The paper addresses challenges associated with integrating Blockchain and AI for financial fraud detection, such as scalability, interoperability, regulatory compliance, and data privacy concerns within financial systems.

Comparative Analysis and Benefits: It might conduct a comparative analysis between traditional fraud detection methods and the integrated Blockchain-AI approach, highlighting the advantages, limitations, and potential benefits of the combined system.

Conclusion and Future Directions: The paper concludes by summarizing the systematic review findings and discussing the potential and future directions for leveraging Blockchain and AI in revolutionizing financial fraud detection systems. It might suggest directions for further research and practical implementations (Zhang and Liu, 2021, p.48).

In summary, the paper serves as a comprehensive systematic review, discussing the strengths and applications of Blockchain technology and AI techniques in financial fraud detection. It explores their combined potential, addresses challenges, and offers insights into the future directions of integrating these technologies to combat financial fraud effectively.

Analyzing the collection of research papers exploring the integration of Blockchain and Artificial Intelligence (AI) for financial fraud detection reveals significant advancements and contributions within the field. Each paper offers unique perspectives, methodologies, and insights into leveraging these technologies to enhance fraud detection and prevention in financial systems.

Common Themes: Integration of Technologies: All papers explore the amalgamation of Blockchain and AI techniques for fraud detection, emphasizing their complementary roles in enhancing security, transparency, and efficiency in detecting fraudulent activities within financial transactions.

Blockchain-based smart contracts offer several key benefits in AI-driven fraud detection systems, enhancing security and efficiency. The primary advantages are discussed below.

The immutability and transparency inherent in blockchain technology ensure that once data is recorded, it cannot be altered, creating a tamper-proof environment. This feature fosters trust in fraud detection, as all transactions are visible and verifiable on the blockchain (Kishor, 2023, p.531).

Smart contracts enable automated transaction execution when specific conditions are met, enhancing the reliability of fraud detection by reducing the risk of human error or intervention. This consistent application of rules minimizes the potential for fraudulent activities (Thukral, 2023).

Blockchain technology enhances data security for AI-driven fraud detection systems by ensuring higher data integrity. Its decentralized nature eliminates single points of failure, making it difficult for malicious actors to corrupt or manipulate data (Pranto et al., 2022, p.115).

Blockchain facilitates privacy-preserving collaboration by enabling secure and private data sharing across different organizations involved in fraud detection. Smart contracts allow entities to collaborate without exposing sensitive data, thus enhancing the efficiency of machine-learning models in fraud detection without compromising privacy (Pranto et al., 2022, p.130).

Automating and decentralizing blockchain-based smart contracts significantly reduce the need for intermediaries, leading to faster and more cost-effective fraud detection processes. These systems are particularly beneficial in real-time fraud detection scenarios, where quick decision-making is crucial, demonstrating the practical benefits of blockchain technology in fraud detection (Blowers et al., 2019, p.1030).

Integrating blockchain-based intelligent contracts in AI-driven fraud detection systems enhances security, automates processes, and fosters secure data collaboration, making these systems more robust and efficient.

Blockchain and Artificial Intelligence (AI) work hand in hand to enhance the detection and prevention of financial fraud by capitalizing on their complementary strengths. In the context of financial systems, where trust and data integrity are paramount, blockchain's immutable ledger ensures that it cannot be altered once data is recorded. This immutable quality provides a secure foundation for AI models, allowing them to operate on trustworthy data, which is crucial for accurate fraud detection (Anand & Siddhartha, 2023). Additionally, blockchain's decentralized nature significantly reduces the risk of data breaches by ensuring that data is stored across a distributed network. This decentralization allows AI systems to securely access a broader range of data sources, enabling more comprehensive and effective fraud detection models (Dillenberger et al., 2019, p.51).

Furthermore, the automation of processes through blockchain's smart contracts is another area where AI shines. These smart contracts can execute predefined rules automatically, without human intervention, thereby reducing the likelihood of human error or manipulation. When integrated into these smart contracts, AI can assess the risk of transactions in real time, preventing fraudulent activities before they occur. The transparency inherent in blockchain also ensures that all actions taken by AI are traceable and verifiable, which adds a layer of trust to the entire system (Zkik et al., 2023, p.41).

Privacy is another critical aspect where blockchain and AI complement each other. Blockchain's cryptographic techniques ensure that data remains private and secure, even when shared across multiple entities. This is particularly beneficial for AI-driven fraud detection, where analyzing large datasets is essential. AI can process this data while maintaining privacy, enabling the detection of complex fraud patterns without exposing sensitive information (Luo et al., 2023, p.2308). By combining blockchain's secure data management with AI's advanced analytical capabilities, these technologies create a robust and adaptive system capable of identifying and preventing fraud in real time. This integration not only enhances the security of financial systems but also ensures that they are better equipped to handle emerging threats, instilling confidence in the system's adaptability.

In summary, the synergy between blockchain and AI brings about a powerful and reliable approach to combating financial fraud. The security, transparency, and decentralized architecture of blockchain provide the ideal environment for AI's analytical and predictive strengths to thrive, resulting in a more secure and trustworthy financial ecosystem (Li et al., 2023, p.37).

The convergence of Blockchain technology and Artificial Intelligence (AI) for fraud detection in financial systems offers substantial benefits but presents significant challenges. Blockchain's decentralized and immutable ledger, combined with AI's advanced data analysis capabilities, provides a potent tool for bolstering security and trust in financial transactions. The secure and tamper-proof nature of blockchain data is a robust foundation for AI algorithms to detect and prevent fraudulent activities accurately. In contrast, AI's real-time analysis of blockchain data can identify patterns and anomalies indicative of fraud. This integration also enables the implementation of smart contracts that automatically execute transactions based on AI-driven decisions, reducing human error and increasing operational efficiency (Anand & Siddhartha, 2023).

However, challenges arise from this integration. One major challenge is the scalability of blockchain technology, mainly when processing large volumes of transactions in conjunction with AI, necessitating substantial computational resources. Additionally, the complexity of integrating AI with blockchain systems presents a barrier to widespread adoption, requiring specialized knowledge and expertise for effective implementation. Privacy concerns also emerge as AI systems necessitate access to extensive datasets, potentially conflicting with blockchain's emphasis on secure, private transactions. Balancing the access of AI models to required data without compromising privacy is a delicate matter that requires careful management (Zheng & Dai, 2019, p.48).

Furthermore, integrating AI and blockchain in financial systems introduces new security challenges. While blockchain is secure, the AI models used for fraud detection are susceptible to adversarial attacks, where malicious actors manipulate data to deceive the AI system. Protecting AI models from such attacks while preserving the integrity of the blockchain requires ongoing research and development. Additionally, using intelligent contracts introduces the risk of coding errors or vulnerabilities that fraudsters can exploit, necessitating a focus on ensuring the security and reliability of smart contracts (Luo et al., 2023, p.2308).

In summary, while integrating Blockchain and AI presents significant opportunities to enhance fraud detection in financial systems, it also brings scalability, privacy, security, and implementation complexity challenges. Addressing these challenges will be essential for fully realizing the potential of this powerful combination in the financial industry.

These above discussion collectively contribute significantly to the understanding and advancement of fraud detection methodologies within financial systems. They explore innovative approaches, highlight challenges, and propose future directions for leveraging the combined power of Blockchain and AI in combating financial fraud. The range of perspectives and methodologies across these papers indicates the continuous efforts and evolving landscape in this critical domain.

As part of literature review, comparative analysis of the various strategies are well presented in a tabular format in the above paper highlighting methods, advantages, disadvantages and future scope wrt following:

1. Fraud detections for online businesses: a perspective from blockchain technology
2. Avoiding Insurance Fraud: A Blockchain based Solution for the Vehicle Sector
3. Blockchain for Fraud Prevention: A Work-History Fraud Prevention System
4. The Influence of Blockchain Technology on Fraud and Fake Protection.
5. Are blockchains immune to all malicious attacks?
6. A Blockchain Based Framework for Fraud Detection
7. Counterfeit Detection of Documents using Blockchain
8. A Multifaceted Approach to Bitcoin Fraud Detection: Global and Local Outliers

9. Video Fraud Detection using Blockchain
10. Avoiding Insurance Fraud: A Blockchain-based Solution for the Vehicle Sector

2.6 Gaps in the Literature

While individually enough literature is available wrt to AI and Blockchain, the Gap is specific to use the two combined to solve the specific business problem mentioned. The proposed model is to minimize the same by leveraging pros and cons of AI with Blockchain simultaneously.

2.7 Summary

Through the literature review we can conclude that:

Findings of Literature Review:

The literature review shows that past studies are quite exhaustive with respect to Artificial Intelligence and Blockchain as individual technologies. Also use cases of combining the two technologies in various domains are a work in progress and literature of some business use cases of combination of both is also available. However, coming to the specific use case of detecting frauds in a live transactional system, a gap is observed.

A judicious use of deploying a blockchain based AI based online fraud detection system can continuously evolve in its learning and help in mitigating the risks to a great extent.

Auto settlement of accounts/payments without human intervention where there has been no changes in the financial and non-financial information over a period of time as confirmed by the above system can be done with high degree of confidence.

Various strategies for deploying the AI system during the processing of the transaction or after the transaction has been completed including escalating for review could be applied using the AI's predictive analytics capabilities. The deployed AI system would be required to be under 24*7 mode with a dedicated team who would be researching more on developing and improving it further.The combination of Blockchain and Artificial Intelligence can go hand in hand in detecting frauds in a live transactions financial system (Perifanis et al., 2023, p.85).

Decentralized Intelligence and collective decision making can play the main role in identifying malicious behavior.

Blockchain and AI technologies are the most disruptive discussed technologies of the present generation and deploying the same to solve various business use cases are being explored. In this context, while individually both Blockchain and AI systems are being researched and also implemented for various use cases, this research is an attempt to combine the features and powers of Blockchain and AI technologies and arrive at a theoretical model to detect frauds in a live transaction system which can help combat and defeat application fraud by detecting illicit activity in the process (Kuznetsov et al., 2024, p.55).

Financial Organizations are now deploying machine learning models that can detect suspicious transactions in almost real time, including stopping the transaction altogether or raising an alert and escalating the transaction for manual intervention before being sent out of the system.

While blockchain based AI systems could start with Machine Learning (ML) algorithms and then move on to Deep Learning (DL) models in due course based on experience and expertise gained in use and deployment of such systems.

This research is being conducted to explore and understand how to integrate two most trending, disruptive and innovative technologies of the current era that is Blockchain and Artificial Intelligence to find a solution to the business problem of detecting frauds in a live transactional financial system.

CHAPTER III:

METHODOLOGY

3.1 Introduction

This section will articulate the various aspects of how the research will be conducted, the guiding principles, the nature and philosophy of the research.

There are two main research designs used in academia, quantitative research design and qualitative research design. The quantitative design is primarily about examining the relationship between variables. It involves generating data from samples and analyzing them using statistical techniques and works well with the deductive approach. Qualitative research design, on the other hand, is used with the inductive and abductive approaches. This research design often involves interviewing people, asking probing questions and deriving insights. While quantitative research design involves examining the relationship between variables, qualitative research design involves examining the relationship between entities. The research being presented is a descriptive study and looks to properly explain the various phenomena around the success or failure of businesses. Therefore, qualitative approach for design will be taken.

The data collection process is summarized below

1. Create a screener survey for potential interviewees.
2. Create a set of probing questions to ask each interviewee. Each interview should last an estimated 45 – 60 minutes.
3. Fix a period for the interviews to be held
4. Reach out to potential interviewees through various channels such as LinkedIn, email, messaging services etc.

5. Ask each responding individual to complete the screener survey
6. Potential interviewees who meet the criteria of the survey will be shortlisted and an email will be sent to each of them introducing the research
7. Each interviewee will be sent the interview consent form and details of the study, along with an explanation of their rights
8. Each interviewee will be asked to sign and return the consent forms.
9. A date and time will be fixed with each interviewee for the interview
10. The interview will be conducted over a video conferencing tool such as Zoom, and will be recorded. Interviews will be conducted in English
11. A copy of the recording will be provided to the interviewee for fact checking and confirmation. The recording will be transcribed soon after the conclusion of the interview.
12. Each interviewee will be asked a series of probing, open ended questions to best capture their life experience.
13. The researcher will use observation techniques to ask deeper, more pointed questions based on the interviewee's answers
14. The core question and sub-questions of the research will be answered through an abductive approach.

The interview is constructed as a set of semi-structured questions presented to the interviewee in a set order. The researcher may choose to ask more pointed questions to obtain more details or gain more insights.

The participants for this research will be chosen carefully across mid to senior roles, including and up to co-founders and promoters. The potential candidates will be chosen from business of a variety of sizes, revenue, and age. Candidates chosen this way will provide a rounded and more accurate depiction of the various problems that their businesses had faced.

The interview questions are prepared well in advance, and the interviewee is made aware of the time and date of the interview beforehand so that they can best prepare for the process. Since this research involves discussion of potential business secrets, internal knowledge, and business health, it is important that the researcher gain the utmost confidence of the interviewee. This is done by explaining to the interviewee their rights and by explaining the interview consent form in detail. Furthermore, the researcher will remind the interviewee about their rights at the beginning and the end of the interview (Roberts, 2020).

During the interview, the researcher will not use detailed written notes, and rather record the entire exchange. The interview will be done over a videoconferencing app like Zoom, with video turned on for both the researcher and the interviewee. This is done so that the researcher can observe the interviewee's reactions to questions, and their body language while answering. The researcher may take short written notes to capture important pieces of information and to phrase proper follow up questions (Roberts, 2020).

After the data collection process is completed, the researcher will codify all the important sections of each interview and use an abductive approach to identify one or many key metrics and business practices that occur commonly across these businesses that contributed to their success. As a result, the themes that emerge will be used to create a framework for aspiring businesses to adopt and increase their chances of success (Philipsen, 2018, p.45).

3.2 Overview of the Research Problem

To develop a model framework combining Blockchain and AI to detect frauds in live financial transactional Systems

3.3 Research Design

To answer the research questions proposed in the previous section, the researcher will apply qualitative research design. The researcher will use semi-structured interviews and ask open ended, probing questions. During the interview, the researcher will note several observations through the course of the interviews. The data obtained from these interviews will be codified by the researcher and will be used to form themes. These observations will then be used to formulate the most likely scenario or explanation for the phenomenon.

The investigation undertaken for this study will be of qualitative nature. The research will attempt to explore and explain the themes and provide additional insights into the business of games through the creation of a theoretical framework.

The strategy of research is method applied to study the nature of data to produce results in-line with the research objectives. Quantitative strategies are best applied to studies that involve mathematical, statistical, and fact-based approaches, while qualitative strategies are applied to studies that involve the life experiences of subjects.

This research will use a qualitative approach through the means of interviews and examination of the experiences and views of the subjects.

Questionnaire to understand basic elements for combining Blockchain and AI

3.4 Population and Sample

Although sampling is essential to the practice of qualitative approaches, it has received less attention than data gathering and analysis. Robinson in 2013 proposed a four-point method for sampling in qualitative interview-based research, which blends theory and process for the following (Robinson, 2013)

- Defining a sample universe by specifying inclusion and exclusion criteria for potential participants.
- Deciding a sample size by balancing epistemological and practical concerns
- Selecting a sampling strategy, such as random sampling, convenience sampling, stratified sampling, cell sampling, quota sampling, or a single-case selection strategy.
- Sample sourcing, this includes matters of advertising, incentivizing, and locating potential participants.

The coherence, transparency and therefore the trustworthiness and acceptance of this research are directly related to the extent to which the above points are adhered to in this research.

According to Ziebland and McPherson (2006) shows the sampling technique in qualitative research is primarily intended to represent a wide range of opinions and experiences, rather than to mimic their frequency in the general population (Ziebland and McPherson, 2006). While the sample size is small, it can still be information and enable the researcher to obtain information that is meaningful, and derive useful perceptions from the interviewees (Creswell, 2003, p.23). Further, because the sample size is small, it enables the interview method to shine, since it only requires a few participants to gather rich and detailed data (Genise, 2002, p.125).

Per Roberson, the sample in qualitative research is the result of a careful, complicated, and collaborative process. Sample selection is critical to the research because the sample itself is the data, and addresses the research problem (Roberson, 2005).

To reach a sample, the researcher must first set the criteria. According to Merriam in 1998, this criterion creates a list of important attributes that the sample must possess based on the purpose of the study and its theoretical lens (Merriam, 1998, p.56).

The criteria of the research are businesses that are involved in the gaming industry in India as a developer, publisher or both. More specifically, the businesses that will form the scope of the research will be involved in pure-play games for mobile. Businesses that are engaged in creating or publishing games of skill such as Rummy and platforms that allow for users to invest real money to play tournaments and win real money in return will be excluded from the study. The size of the business, both in terms of number of people employed and revenue generated will NOT be a factor for inclusion or exclusion. The responses were gathered for the study from persons holding positions and working in the domain of fraud detection. Responses from 50 participants were recorded.

3.5 Participant Selection

Researchers / developers working in the area of Blockchain / AI and in financial domain

For this research, there were two instruments employed to ensure that the data being collected for the research was relevant, valuable and could potentially assist in the research. The first instrument was a screener survey that all potential interviewees completed to determine eligibility. The second instrument was the sharing of the questionnaire among selected participants.

A screener survey was created for all potential interviewees to fill out. The survey was sent out to everyone who was contacted for the purpose of this research. The screener survey was designed after completing literature review, and authoring the core and sub questions to be answered for this research.

The screener survey was designed to target the persons specifically working on detecting frauds so that they are aware of the technologies involved and can provide proper and useful responses to the questionnaire.

At the beginning of the interview, the researcher introduced the various reasons this research was being conducted. The researcher ensured to use neutral and non-leading language, so as to not influence or nudge the interviewee into answering questions in a biased manner.

3.6 Data Collection Procedures

Data collection for undergoing research was collected from primary by way of questionnaire and secondary. Primary data is typically defined as the first occurrence of a piece of work. For the purpose of this research, primary data is obtained from the interviewees from the semi structured interviews. The recordings of these interviews are transcribed and codified by the researcher.

Secondary data is obtained from literature review, where the researcher has perused several articles, journals, papers and books to gain as much information as possible that is relevant to this research.

The researcher interviewed several mid to senior executives for this research. The questions were prepared in advance, and were shared with the interviewees, so they could better prepare for the process.

To codify and analyse the data collected, the researcher prepared by creating a system to assign each interviewee with a unique identifier, working on a framework to store and retrieve data, building a table to store the frequency of certain key words to form themes, reducing redundancies and removing irrelevant data. By using these procedures, the researcher was able to reduce the data collected to only relevant data to be analysed (Hackett and Strickland, 2018, p.26).

3.7 Research Design Limitations

This research does have some limitations that may reduce the generalization of the findings. Since this was a study conducted using interviews, where the sample size was limited, and the interviewees were selected using random sampling and a screener survey, it may be the case that the experiences of these interviewees do not fully capture the experience of all businesses mobile games industry in India. That said, it is imperative to state that the size of the sample is less critical than the quality of the data being generated and analyzed through these interviews.

Furthermore, while the interviewees were given ample time to prepare for the interview, it is possible that they did not recall incidents as they actually happened and may have missed details that would affect the outcome of the research. Additionally, a fundamental assumption of this study is that the interviewees had the relevant experience and were considered experts in their domain at the time of the interview.

Lastly, while the interviewees were informed and assured that their answers would be kept confidential; there is the possibility that their answers did not accurately depict their lived experience.

3.8 Conclusion

Responses to Questionnaire clearly demonstrated the need for combining the two technologies viz., Blockchain and Artificial Intelligence for solving the business use case of detecting frauds in online transactional financial systems.

The researcher has explored both the qualitative and quantitative methods of research design. Qualitative research design is applicable when the phenomenon in question is related to the lived expertise of the individual involved in the research. The research instruments used for this research were a screener survey to screen potential interviewees, and a semistructured interview comprising of open-ended, probing questions.

The answers provided by the interviewees were the main origin of data for this undergoing work, and the responses to the screener survey brought in context to some of the answers. The various procedures for data collection, coding and analysis used in this study were presented and discussed in the above sections. The coding techniques by Tayor-Powell were explained and used to transcribe the interviews, create relations with the data extracted and the findings of the undergoing work. Finally, the limitations of the research were stated and discussed.

CHAPTER IV:

RESULTS

4.1 Analysis of the Questionnaire

Question 1: What is a primary advantage of using a blockchain-based AI model for fraud detection?

Intention: Assessing basic knowledge of the amalgamation of AI and blockchain.

Analysis: Look for responses that grasp the core concept of combining AI and blockchain for fraud detection, showcasing an understanding of their potential synergy.

Question 2: Which technology ensures the immutability of transactional records in a blockchain?

Intention: Evaluating the recognition of challenges in traditional fraud detection.

Analysis: Examine responses acknowledging limitations or shortcomings of conventional fraud detection methods, emphasizing the need for innovative solutions like AI and blockchain.

Question 3: How does AI contribute to fraud detection in a live financial system?

Intention: Assessing comprehension of blockchain's role in bolstering security.

Analysis: Look for responses highlighting blockchain's features (e.g., immutability, decentralization) that enhance security in financial systems.

Question 4: What is the significance of real-time monitoring in detecting financial frauds?

Intention: Evaluating familiarity with AI algorithms for fraud detection.

Analysis: Examine responses that mention specific AI algorithms (e.g., neural networks, decision trees) applicable to fraud detection, demonstrating knowledge of AI's role in pattern recognition.

Question 5: What role does a smart contract play in a blockchain-based fraud detection system?

Intention: Assessing understanding of the collaborative potential between AI and blockchain.

Analysis: Look for responses that illustrate how AI's analytical capabilities complement blockchain's security features, offering a comprehensive solution for fraud detection.

Question 6: Which feature of blockchain technology aids in providing transparency and auditability?

Intention: Evaluating recognition of real-time monitoring's importance in financial systems.

Analysis: Examine responses emphasizing the significance of real-time monitoring in promptly identifying and addressing fraudulent activities.

Question 7: What aspect of fraud detection does historical transaction data assist AI models with?

Intention: Assessing awareness of blockchain's impact on mitigating single points of failure.

Analysis: Look for responses explaining how blockchain's decentralized nature reduces reliance on single entities, minimizing the risk of system failures.

Question 8: How does the decentralized nature of blockchain contribute to fraud prevention?

Intention: Evaluating comprehension of an immutable ledger in blockchain.

Analysis: Examine responses elaborating on the concept of immutability in the blockchain ledger and its importance in maintaining trustworthy records.

Question 9: Which factor is crucial for AI classification models to effectively detect frauds in live transactions?

Intention: Assessing recognition of reducing data tampering risks through blockchain and AI.

Analysis: Look for responses that illustrate how the combination of blockchain and AI safeguards against data tampering, enhancing the integrity of financial data.

Question 10: What is the primary role of AI algorithms in detecting fraudulent activities?

Intention: Evaluating understanding of increased transparency due to blockchain and AI.

Analysis: Examine responses explaining how blockchain's transparency, coupled with AI's analysis, enhances visibility into transactions, promoting trust and accountability.

Question 11: How can blockchain technology enhance data security in fraud detection systems?

Intention: Assessing awareness of enhanced traceability with blockchain and AI.

Analysis: Look for responses highlighting how blockchain's immutable nature and AI's analytical capabilities enable traceability, aiding in tracking and verifying transactions.

Question 12: Why is continuous improvement essential for AI models in fraud detection?

Intention: Evaluating recognition of smart contracts' role in fraud detection.

Analysis: Examine responses describing how smart contracts automate and enforce predefined rules or conditions, contributing to fraud prevention in financial systems.

4.2 Analysis of Responses

Evaluate the clarity, relevance, and depth of responses to understand respondents' grasp of the topic.

Identify consistent themes or knowledge gaps across responses.

Consider the use of technical terms, examples, or real-world applications to assess the depth of understanding.

Summarize common trends, misconceptions, or areas needing further explanation for insightful conclusions.

What is blockchain?

The blockchain serves as an extension of Internet technology. It operates as a system that securely stores and validates all transactions. Every data block contains transaction information linked to the preceding block, rendering it tamper-proof once stored in the blockchain. Consequently, the blockchain ensures transparency, allowing for easy tracking of all users and transactions. Innovations like Bitcoin, built on blockchain technology, have revolutionized the financial sector by enabling anonymous yet fully transparent transactions.

What is Blockchain Technology?

A blockchain acts as a shared public ledger collectively maintained by all peers in a distributed network. For example, in data records, transactions are stored in block units using hash values and timestamps for additional authentication. Each block is linked to the previous block, creating a chain of interconnected peer-to-peer networks. The main advantage of blockchain is achieving immutability, ensuring data cannot be modified. It operates on a consensus protocol, which forms the foundational framework of the blockchain network.

What is Artificial Intelligence?

AI refers to the capability of machines to imitate human intelligence by performing tasks that typically require human-like intelligence. It encompasses the study of making computers perform tasks that would necessitate human intelligence, such as visual perception, speech recognition, decision-making, and language translation. AI covers machines' ability to replicate human intelligence, including learning, reasoning, and problem-solving.

Machine learning, a subset of AI, involves computers using statistical techniques to learn and improve independently. The primary objective is to reduce human errors and enable quick machine actions through AI development, which includes teaching the computer and creating machine learning algorithms to leverage its powerful computing abilities for rapid task execution. An example is self-driving cars. Having gained a better grasp of AI and blockchain, we will discuss combined technology applications.

What are the differences between blockchain and AI?

Blockchain technology is a protocol designed to store financial and contract data, enabling universal access securely. This technology can potentially create payment systems independent of traditional banks and government control, similar to the cryptocurrency Bitcoin. Artificial Intelligence (AI) technology is used to address challenges related to scheduling and routing. AI, a computer program, can complete tasks typically carried out by humans and learns from experience, continually increasing its capabilities.

Decentralized Vs. Centralized: A Detailed Comparison

In the world of blockchain, we find the decentralized vs centralized debate a lot. After all, blockchain technology can make centralized systems a thing of the past.

In any scenario, if you are new to blockchain technology, then you might find yourself confused with the centralization vs decentralization concepts.

Here, we try to explore the decentralized vs centralized concept in connection with the current industries and blockchain.

Table 1

Parameters to differentiate between AI & Blockchain

Parameter	**Centralized (AI)**	**Decentralized (Blockchain)**
Third-Party Involvement	Yes	No
Control	Full control stays with the central authority	Control stays with the user itself
Hackable	More prone to hacks and data leaks	Less prone to hacks and data leaks as no single point of failure
Single Point of failure	Yes	No

Ease of use	Intuitive and easy to use	Not easy to use
Exchange fees	Higher fees	Less fees
Anonymous	Users are not anonymous	Offers anonymity

Conclusion: Which One Is Here To Stay? Centralized vs Decentralized

Both centralized and decentralized have their own benefits. There is no doubt that governments, organizations, and companies want control over their assets, even when they have to give up efficiency for the sake of it.

But, decentralization is here to stay! And, with time, it will grow as more companies will realize the benefit of it. Also, you can also implement decentralization with a sustainable close environment and with the help of hybrid or federated blockchain solutions.

This leads us to the end of our decentralized vs centralized guide. By now, you should have a good idea of what each of them has to offer.

Blockchain vs AI: Difference Between Blockchain and AI

It is largely accepted that blockchain and artificial intelligence (AI) technologies are being adopted at a phenomenal rate. Both AI and blockchain technologies have various technological complexity and large business implications. Blockchain and AI are among the great disruptive technologies, and in future, they will reshape how humans live, collaborate and interact.

AI and blockchain are known as the main driving entities behind today's innovation. Both have introduced radical shifts with many aspects of human life, and it is predicted to contribute millions of capital investments to the global economy. The future is near with autonomous systems and prediction technologists who can make required contents and posts on your system of interest in natural conversations.

With the advances and arrival of more content and economy sharing platforms, this means that entities and companies will no longer be asked to trust “unreliable platforms”. So, what happens if these two technologies are combined? After careful understanding of these technologies, we will move ahead with some of the applications of using these technologies combinedly.

Artificial Intelligence Vs Blockchain

First, blockchain has many issues related to security, scalability and efficiency. AI has issues of its own such as explainability, trustworthiness, and privacy. Now, if these two technologies are used together, it would create the next digital generation.

Here, the aim is that blockchain provides trustworthiness, privacy and explainability to AI. While AI provides its knowledge to build machine learning systems based on blockchain to achieve scalability and which can be used precisely for personalization and governance.

Blockchain for AI (confidentiality and privacy)

AI for Blockchain (Security and transparency)

Blockchain can enable decentralized marketplaces and coordination platforms that can be used for many components of Artificial Intelligence, that includes computing power data and algorithms. These will parent many other innovations and usage of AI to a greater level.

The implementation of AI requires the management of large volumes of data to train machines. This creates a need for a more efficient and secure way to share data while prioritizing privacy to prevent significant data breaches and the misuse of personal information.

Blockchain technologies also enable the possibility of selling data through smart contracts, facilitating the creation of data marketplaces that eliminate the reliance on intermediaries. This results in a more secure and private method for selling data and allows for greater participation by smaller entities, thereby reducing barriers to entry.

Moreover, blockchain can potentially enhance the distribution of computing power necessary for machine learning and AI training. This can be achieved through a decentralized market for selling computing power and establishing a blockchain-based cloud computing system. By utilizing AI smart contracts, underutilized computing power, particularly GPUs, can be put up for auction and monetized, thus optimizing its usage.

4.3 Classification Models in AI

Role of classification models in AI:

Classification models in AI play a fundamental role in making sense of data by categorizing it into predefined classes or categories. Their primary function is to assign labels or categories to input data depends on patterns and relationships observed from labeled training data. Here are some key roles of classification models in AI:

Pattern Recognition: They identify patterns and relationships within the data that correlate with specific classes or labels. This enables them to generalize from known examples to make predictions on new, unseen data.

Decision Making: Classification models help in decision-making by assigning the most probable class or label to a given input based on learned patterns. This is crucial in different applications such as medical diagnosis, fraud observation, and sentiment analysis.

Information Organization: They organize and structure data by assigning categorical labels or classes, making it easier to interpret and analyze large volumes of information.

Prediction and Forecasting: These models can predict the class or category to which new data belongs, allowing for forecasting future outcomes or trends based on historical patterns.

Anomaly Detection: In some cases, classification models are used to identify anomalies or outliers in data, detecting instances that deviate significantly from the norm.

Feature Importance and Insights: They offers insights into which features or variables are most relevant in determining the class or label, aiding in feature selection and understanding the underlying data characteristics.

Automation and Streamlining Processes: Classification models automate the process of labeling or categorizing data, which is beneficial in automating workflows, reducing manual efforts, and increasing efficiency.

Personalization and Recommendation Systems: In applications like recommendation systems, classification models help in classifying user preferences to provide personalized recommendations.

Improving Decision Support Systems: They enhance decision support systems by providing valuable information and predictions that aid humans in making informed decisions.

Overall, classification models are essential tools in AI and machine learning, allowing systems to learn from data and make intelligent decisions or predictions across a wide array of applications and industries.

Different classification models in AI:

There are various classification models in AI, each with its unique approach and suitability for different types of data and tasks. Some common classification models include:

Logistic Regression: Despite its name, it's a linear model used for binary classification, estimating the probability of a sample belonging to a particular class.

Decision Trees: These models use a tree-like graph to make decisions based on features at each node, leading to a final classification at the leaf nodes.

Random Forest: It's an ensemble method that creates multiple decision trees and combines their outputs to improve accuracy and prevent overfitting.

Support Vector Machines (SVM): SVM finds a hyperplane that best divides a dataset into classes while maximizing the margin between them.

Naive Bayes: Based on Bayes' theorem, it calculates the probability of a sample belonging to a class given its features. It assumes independence among features.

Neural Networks: Particularly, for classification tasks, models like Convolutional Neural Networks (CNNs) for image data and Recurrent Neural Networks (RNNs) for sequential data are popular. Deep learning models can learn complex patterns from data.

K-Nearest Neighbors (KNN): It classifies data points based on the majority class among their K-nearest neighbors in feature space.

Gradient Boosting Machines (GBM): These models build trees sequentially, where each tree corrects the errors of the previous one, optimizing the overall model.

Ensemble Methods: These combine multiple models to improve performance, like AdaBoost, XGBoost, or stacking models.

Each model has its strengths and weaknesses, and the choice often depends on the nature of the data, the available computing resources, the interpretability needed, and the desired accuracy or performance metrics for the specific task at hand.

Which classification models work best with alphanumeric data for detecting abnormalities

For detecting abnormalities in alphanumeric data, several models can be effective depending on the specific nature and complexity of the data:

Isolation Forest: This model works well for anomaly detection and is particularly effective with high-dimensional data, including alphanumeric data. It isolates anomalies by randomly selecting a feature and then randomly selecting a split value between the maximum and minimum values of the selected feature.

One-Class Support Vector Machines (SVM): It's suitable for novelty detection or anomaly detection where you train the model on only normal data and then detect deviations from this norm.

Autoencoders (Neural Networks): These unsupervised learning models are efficient at learning representations of data. For anomaly detection, you can use an autoencoder to reconstruct normal instances and identify outliers based on high reconstruction errors.

K-Nearest Neighbors (KNN): KNN can be effective if you can define a meaningful distance metric on your alphanumeric data. It works by finding the nearest neighbors to a data point and can be particularly useful in certain contexts for anomaly detection.

Cluster-Based Models (e.g., DBSCAN): These models work by identifying dense regions in the data space, considering points in low-density regions as anomalies. They can be effective if the anomalies form distinct clusters.

Ensemble Methods: Combining various models like Random Forest, XGBoost, or Gradient Boosting can sometimes enhance anomaly detection, especially when different models capture different aspects of the anomalies.

When dealing with alphanumeric data, it's crucial to preprocess it effectively, convert it into a suitable format for the chosen model, and perform feature engineering if needed. Additionally, understanding the specific context and characteristics of the anomalies you're trying to detect will help in selecting the most appropriate model.

Criterion for selecting a specific classification model

Selecting a classification model depends on various factors, and considering these criteria can guide your decision-making process:

Nature of Data: Understanding your data's characteristics is crucial. Consider its size, dimensionality, type (numeric, categorical, text, etc.), and any inherent patterns or complexities. Some models perform better with specific types of data.

Accuracy and Performance Metrics: Different models excel in different performance metrics. Decide which metrics (precision, recall, accuracy, F1-score, AUC-ROC, etc.) are crucial for your problem and select a model that optimizes these metrics.

Interpretability vs. Complexity: Models vary in complexity and interpretability. Simpler models like Logistic Regression or Decision Trees offer interpretability, while deep learning models might be highly accurate but less interpretable.

Scalability and Computational Requirements: Consider the computational resources available. Some models, like deep neural networks, require substantial computational power and data to train effectively.

Robustness to Overfitting: Some models are more prone to overfitting than others. Regularized models like SVMs or models with built-in regularization mechanisms might be more robust.

Handling of Missing Data: Certain models handle missing data better than others. For instance, tree-based models like Random Forests can handle missing values without much preprocessing.

Ensemble Methods and Combining Models: Sometimes combining models using ensemble methods can improve performance. If multiple models perform well individually, combining their predictions might yield better results.

Training Time and Resource Efficiency: Consider the time it consumes to train the model, especially when working with large datasets. Some models are faster to train than others.

Domain-Specific Considerations: Certain domains might have specific requirements. For instance, in healthcare, interpretability might be crucial for regulatory compliance.

Cross Validation and Robustness Testing: Validate the performance of model using cross-validation techniques and assess its robustness against different subsets of the data.

Choosing the right model often involves experimentation and comparing the performance of different models based on these criteria. It's often a balance between accuracy, interpretability, computational efficiency, and suitability for the given task and dataset.

Analysis of frauds which can be missed by usage of AI individually:

Adversarial Attacks: AI models can be vulnerable to adversarial attacks where small, imperceptible changes to input data can cause the model to make incorrect predictions. Fraudsters can manipulate these vulnerabilities to bypass AI-powered fraud detection systems.

Data Poisoning: If the training data used to build AI models is corrupted or manipulated, the models can learn from biased or inaccurate information, leading to incorrect classifications and potentially missing fraudulent activities.

Emerging and Unseen Patterns: AI models heavily rely on past data patterns. They might struggle to detect new or evolving fraud patterns that have not been seen before in the historical data used for training.

Over-reliance on Historical Data: AI models might overlook anomalies or outliers that don't fit typical patterns seen in historical data, especially in situations where fraud patterns change rapidly.

Analysis of frauds which can be missed by usage of Blockchain individually:

On-chain Fraud: While blockchain offers transparency and immutability, fraudulent activities can still occur within the system. For instance, smart contract vulnerabilities or bugs could be exploited by attackers to siphon funds or execute unauthorized transactions.

Off-chain Activities: Blockchain doesn’t have control over off-chain activities or the input data fed into the system. If fraudulent activities happen outside the blockchain ecosystem or if the input data is compromised before being recorded on the blockchain, the system might not detect it.

Human Errors: Blockchain systems are not immune to errors made by humans during the development, deployment, or management of blockchain applications. These errors could potentially lead to vulnerabilities that fraudsters could exploit.

Regulatory and Legal Aspects: Blockchain might not fully address compliance-related issues or regulatory requirements, and fraud can occur within the boundaries of legal frameworks without being detected solely by blockchain.

Table 2

Comparative characteristics of popular classification models

Model	Pros	Cons	Best For
Logistic Regression	Simple, interpretable Works well with linearly separable data	Limited to linear boundaries Can't capture complex relationships	Binary classification, establishing baseline performance
Decision Trees	Easy to interpret and visualize Handles both numerical and categorical data	Prone to over fitting Can be unstable with small variations in data	Initial exploration, understanding feature importance
Random Forest	Reduces over fitting by combining multiple decision trees Handles large datasets with high dimensionality	Can be computationally expensive Less interpretable compared to individual trees	Robustness, handling high-dimensional data, feature importance analysis
Support Vector Machines (SVM)	Effective in high-dimensional spaces Versatile due to different kernel functions	Computationally intensive for large datasets- Not efficient with noisy datasets	Binary classification, text and image classification, when distinct separation between classes is important
Naive Bayes	Simple and fast Works well with high-dimensional data,	Assumes independence among features (which might not hold true in reality)	Text classification, spam filtering, sentiment analysis

	computationally efficient	Sensitive to outliers	
Neural Networks (Deep Learning)	Capable of learning complex patterns in data Good for unstructured data (images, text) High accuracy	Requires a large amount of data for training Computationally intensive and complex architecture	Image and speech recognition, natural language processing, complex pattern recognition
K-Nearest Neighbors (KNN)	Simple and easy to understand No training period	Computationally expensive during testing (especially for large datasets) Sensitive to outliers	Similarity-based tasks, anomaly detection, small to medium-sized datasets
Gradient Boosting Machines	Often provides high accuracy Handles different types of data	Prone to over fitting if not tuned properly Computationally intensive	Improving weak learners, working with diverse data types, when high accuracy is required
Ensemble Methods	Reduces over fitting and increases robustness Can combine diverse models	Increased complexity and computation Challenging to interpret ensemble predictions	Overall high accuracy, robustness, when multiple perspectives enhance predictive performance

4.4 Summary & Conclusion

Despite rapid progress, the development of both AI and blockchain technologies still has a long way to go. Google Duplex represents one of the latest advancements in AI, enabling automated phone calls and tasks such as scheduling appointments and making reservations. However, it is currently limited to handling holiday hours, restaurant reservations, and hair salon appointments.

Significant strides have been made in AI algorithms that leverage greater computational power and training data, but addressing real-world complexities remains a challenge.

In blockchain technology, recent security breaches involving cryptocurrencies like BitcoinGold, Ethereum, and ZCash have demonstrated the difficulties in developing secure and scalable blockchains for practical applications.

Three key features of blockchain technology make business networks less vulnerable to fraud.

1. Blockchain is distributed or distributed networks

A blockchain represents an innovative decentralized digital record that stores transaction data. This data is spread across a network of linked computers and is regularly updated to guarantee precision. In contrast to conventional records, there is no central power or sole point of authority. Instead, control and permission are dispersed across the network, resulting in high security and resistance to fraud.

2. Blockchain is immutable or Immutability

The transactions stored on a blockchain cannot be altered or erased, making them immutable. Network participants must unanimously validate the transaction using consensus before adding a "block" of transactions to the blockchain. This block is then assigned a timestamp, secured using cryptography, and linked to the previous block in the chain. Although you can initiate a new transaction to modify the status of an asset, it will only be appended to the chain, and the original record will remain accessible. Therefore, by employing blockchain technology, you can trace the history of an asset, including its origins, journey, and ownership.

3. Blockchain can be permissioned or Permissibility

Businesses handle a significant amount of sensitive data and cannot allow unrestricted access. Measures to prevent unauthorized external access and internal data tampering are essential. Permissions play a crucial role in addressing these concerns. Permissioned networks effectively prevent fraud by limiting participation and defining specific access rights. Before contributing, individuals must be invited and verified to become members of a permissioned network.

Features of Artificial Intelligence:

AI can analyze large volumes of transactions to uncover patterns of fraud, which can then be used to identify fraud in real time.

When there is suspicion of fraud, AI models can be used to decline transactions, flag them for further review, and assess the likelihood of fraud, enabling investigators to concentrate on the most promising cases.

The AI model can also provide reasons for flagging the transaction. These reasons guide the investigator to the specific areas to focus their investigation, expediting the process. Additionally, AI can learn from investigators as they review and approve questionable transactions, reinforcing its knowledge and avoiding non-fraudulent patterns.

Fraud Detection with Machine Learning becomes possible due to the ability of ML algorithms to learn from historical fraud patterns and recognize them in future transactions. Machine Learning algorithms appear more effective than humans when it comes to the speed of information processing. Also, ML algorithms are able to find sophisticated fraud traits that a human simply cannot detect.

1. Works faster. Rule-based fraud prevention systems imply creating exact written rules to “tell” the algorithm which types of operations seem normal and should be permitted, and which shouldn’t be because they seem suspicious. However, writing rules takes a lot of time. Also, manual interaction in the E-Commerce world is so dynamic that things can change significantly within a few days. Here Machine Learning fraud detection methods will come in handy to learn new patterns.
2. Scale. ML methods show a better performance along with the growth of the dataset to which they are fitted — meaning the more samples of fraudulent operations they are trained on, the better they recognize fraud. This principle does not apply to rule-based systems as long as they never evolve themselves. Also, a data science team should be aware of the risks linked to fast model scaling; if the model did not detect fraud and marked it incorrectly, this will lead to false negatives in future.
3. Efficiency. Machines can take over routine tasks and the repetitive work of manual fraud analysis, and the specialists will be able to spend time on making more high-level decisions.

Deep learning algorithms can process great amounts of data and detect complicated underlying patterns from seemingly unrelated information. They also have the ability to continuously learn and evolve to remain up to date with a dynamic environment.

The model is trained on historical data of consumer behavior which is known to have been either fraudulent or normal. A major benefit of deep learning is that you are able to combine multiple types of data. For example, a deep learning model can analyze the text written by a customer in an insurance claim and use it in combination with more basic input data to make an accurate prediction.

Thus, it can be said with certainty that In the future, the bonding of blockchain and AI will evoke unlimited innovations and revolutions for companies.

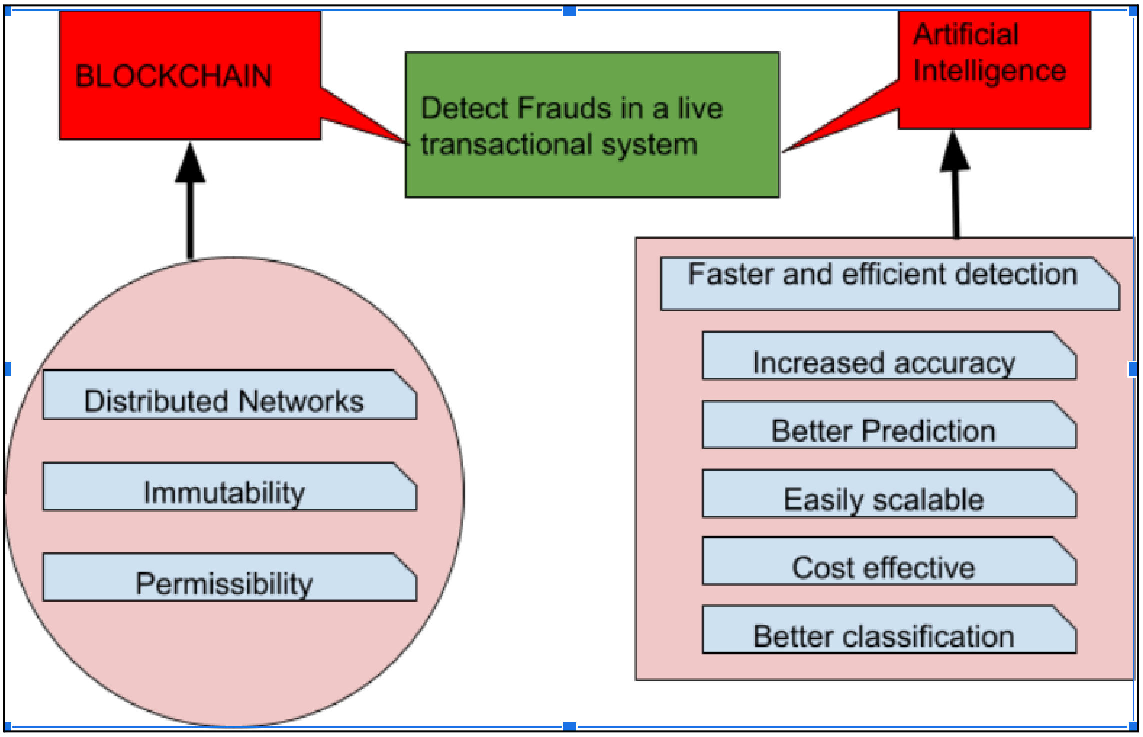
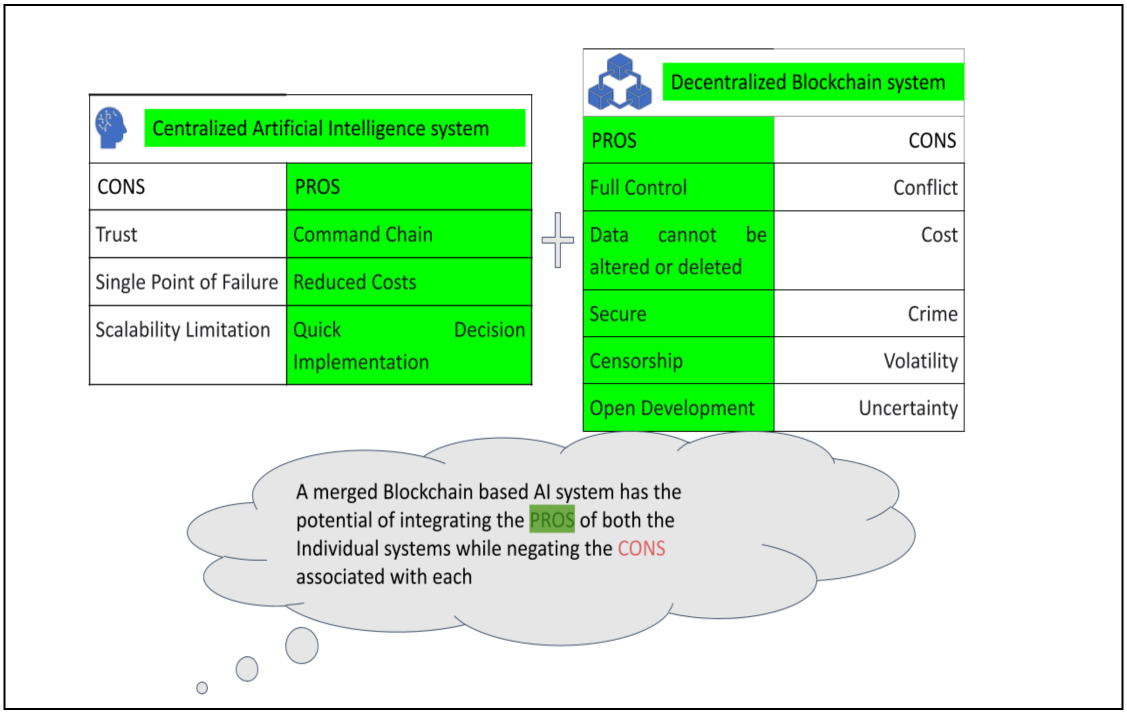


Figure 1 Blockchain & AI Features



Centralized Artificial Intelligence system

CONS	PROS
Trust	Command Chain
Single Point of Failure	Reduced Costs
Scalability Limitation	Quick Decision Implementation

Decentralized Blockchain system

PROS	CONS
Full Control	Conflict
Data cannot be altered or deleted	Cost
Secure	Crime
Censorship	Volatility
Open Development	Uncertainty

A merged Blockchain based AI system has the potential of integrating the PROS of both the Individual systems while negating the CONS associated with each

Figure 2 Pros and Cons of Blockchain & AI

Chapter V:

DISCUSSION

5.1 Introduction

The previous section detailed the results of the interviews conducted by the researcher, and the various relations between the themes being explored in this research.

This section discusses the results in detail, along with recommendations for future research.

The primary research method for this study is literature review and conceptual modeling.

It is proposed to develop a questionnaire and gather inputs from peer groups working in the fields of Blockchain, AI and Financial Frauds and analyze the same to firm up the proposed theoretical model to detect frauds in a live transactional financial system by leveraging Blockchain and AI technologies.

This study first reviews various types of constraints associated with the proposed conceptual model and their solutions / workarounds. Based on this understanding, the proposed theoretical model would be firmed up.

The classification methods readily available in AI technologies which can be integrated into the overall model to arrive at the business use case solution would also be explored and presented.

Amalgamating Blockchain and AI into a theoretical model:

The research aims at amalgamating the key features of Blockchain and AI to add value to the business problem.

While blockchain based AI systems could start with Machine Learning (ML) algorithms and then move on to Deep Learning (DL) models in due course based on experience and expertise gained in use and deployment of such systems.

5.2 Using Blockchain Technology

To Create a hash (or unique digital signature) of critical fields (in this scenario consisting of non-financial and financial information) and

The digital signatures are independently generated and stored in two or more independent systems which are not connected to one another through any means and perform their operations oblivious of each other's existence.

Whenever a financial or non-financial transaction involving the identified critical fields happens against any member, the hashes are reprocessed in both the independent systems maintaining proper history and time stamp.

As more and more of such independent systems are deployed, it becomes practically impossible for any fraudulent transaction to pass through the overall system as it would require manipulating and rigging all the independent, disjoint and geographically placed systems simultaneously.

5.3 Methodology for Achieving Primary Objective

Step1: Data Preprocessing Stage:

In this stage, data which will be used for training, testing, and development stages of the AI system are preprocessed in consultation with domain experts to arrive at data (from different related tables) which would be used for further stages. The exercise would include dimensionality reduction in such a way that important and relevant features are not lost in the data. At the same time, irrelevant columns of data which may not add value to the model are removed. Also, the left over data from various tables is combined and labeled in such a way that the same can be fed to the AI system for testing, etc.

Step2: Supervised Learning Phase:

Supervised Learning in machine learning refers to the defining characteristic of availability of annotated training data, that instructs the learning system on the labels to associate with training examples. Typically these labels are class labels in classification problems. Supervised learning algorithms induce models from these training data and these models can then be used to classify other unlabelled data.

During this phase labeled records are considered which are a mix of previously detected fraudulent transactions and clean records (genuine records) in approximately equal proportions to avoid bias and the preprocessed data is repeatedly fed to the model to make the model learn from the data. More bunches of preprocessed data, learning and accuracy of the model is expected to be more.

Step3: Testing Phase:

In this stage, the accuracy of the developed model is tested by feeding to the system randomly selected fraudulent and non-fraudulent (clean) transactions and the system's efficiency in labeling them correctly is recorded.

Step4: Improving accuracy and efficiency:

Steps 1 to 3 are repeated as many times (it may not be necessary to do all, always) till the desired accuracy and efficiency (degree of confidence) has been achieved in the model.

On completion of Step4, the trained model would be in a position to achieve the primary objective of classifying a given financial transaction as fraudulent / genuine with a high degree of confidence

5.4 Bringing the Blockchain Inputs in the Picture

The hashes or digital signatures of all or suspected transactions can be compared between the independent systems to flag transactions where either financial or non-financial information or both has been changed in the transaction being settled as outgoing transaction and appropriately flagged (escalated) or stopped completely. This could be also done for outgoing transactions over and above a prescribed limit.

5.5 Methodology for Achieving Secondary Objective

Going further, as more and more records go through the AI model, the model is now in a reinforced learning phase (involving predicting and correcting based on feedback) and evolves into a self improving model over time i.e., moving towards the secondary objective.

Feature extraction:

The model (specially DL) is expected to extract features from the huge data sets through which it has been trained, tested over time to have insights into data which may not be so obvious to naked eye and traditional database systems. Such features could over a period of time create value with respect to new methods of frauds in future e.g.

Super fast transactions:

Mostly, every transaction in a financial system travels with a certain speed and goes through some workflow or approval cycle which are time-stamped. It is found that more stress is given on completing the approval cycle within the given time limit which could be 24 hours or 7 days, as decided by the management. This is because if the transaction is not acted upon during the time limit specified for it, it is mostly escalated in the system to the next level or flashed as pending beyond acceptable time limit. However, it is important to track transactions which clear all the work flow at breakneck speed and thus come in and go out of the system so fast that they could go unnoticed.

Transactions breaking workflow checks:

Each transaction in a workflow is expected to be operated by a different person using unique credentials from different machines. However, if a transaction is progressing breaking the rule, it should be detected and flagged for relook.

Activities preceding the transactions: More often than not dummy records are created / inserted before a fraudulent transaction is fired. Thus understanding the activity preceding the transaction could also raise a red-flag on the transaction.

5.6 Deploying the Blockchain based AI Implemented System

Auto settlement of accounts without human intervention where there has been no changes in the financial and non-financial information over a period of time as confirmed by the above system can be done with high degree of confidence.

Various strategies for deploying the AI system during the processing of the transaction or after the transaction has been completed including escalating for review could be applied using the AI's predictive analytics capabilities. The deployed AI system would be required to be under 24*7 mode with a dedicated team who would be researching more on developing and improving it further.

While blockchain based AI systems could start with Machine Learning (ML) algorithms and then move on to Deep Learning (DL) models in due course based on experience and expertise gained in use and deployment of such systems.

5.7 Conclusion: Proposed Theoretical Model

Proposed Theoretical model consists of three step process involving

Step 1: Developing an effective AI Classification Model

Step 2: Developing an effective Blockchain system

Final Step: Combining the output of AI Classification Model with the Blockchain System

Step1: An effective AI classification model to detect frauds in a live transactional financial system can be achieved using various machine learning algorithms consisting of involving one or more of below:

Logistic Regression or Random Forest:

Logistic Regression or Random Forest algorithms could be utilized as they provide good interpretability and are capable of handling binary classification problems (fraudulent vs. non-fraudulent transactions).

Logistic Regression models are relatively simple and provide insights into feature importance.

Random Forest models can capture complex relationships between features and yield high accuracy.

Feature Engineering:

Extract and engineer relevant features from the transactional data. These features may include transaction amount, time, location, frequency, device information, user behavior patterns, etc.

Normalize or scale the features to ensure consistent model performance.

Anomaly Detection:

Employ anomaly detection techniques in combination with classification algorithms to identify irregular patterns or outliers in the data, which may indicate potential fraud.

Techniques like isolation forest, local outlier factor (LOF), or one-class SVM can be used for anomaly detection.

Ensemble Methods:

Utilize ensemble methods such as AdaBoost, Gradient Boosting, or XGBoost to combine multiple weak classifiers into a robust fraud detection model.

Ensemble methods often improve predictive accuracy by combining the strengths of individual classifiers.

Neural Networks (Optional):

For more complex patterns and larger datasets, neural network architectures like deep learning models (e.g., feedforward neural networks, convolutional neural networks, or recurrent neural networks) can be employed.

These models can capture intricate relationships in the data but might require more computational resources and data.

Real-time Monitoring and Model Deployment:

Implement the trained model for real-time monitoring of incoming transactions.

Deploy the model in the live financial system to continuously analyze transactions and flag potential fraudulent activities.

Evaluation and Validation:

Assess how well the model performs using measures like precision, recall, accuracy, F1-score, and area under the ROC curve (AUC-ROC).

Validate the model's predictions using a separate test dataset or through a validation mechanism in a live environment.

Model Refinement and Iteration:

Continuously refine the model based on feedback from detected frauds and non-frauds.

Update the model periodically to adapt to evolving fraud patterns and ensure optimal performance.

Compliance and Security:

Ensure compliance with regulatory standards and data privacy laws when handling sensitive financial data.

Implement security measures to protect the model and prevent adversarial attacks.

This model is to be trained on historical data containing labeled instances of fraudulent and non-fraudulent transaction. It should then be deployed and continuously updated to detect and prevent fraud in real-time financial transactions.

Step2: An effective Blockchain model for Detecting fraud in a live transactional financial system using blockchain involves leveraging the immutability, transparency, and decentralized nature of blockchain technology. Here is a conceptual model:

Decentralized Ledger:

Utilize a decentralized ledger (blockchain) to store transactional records securely and immutably.

Each transaction is marked as a block and linked cryptographically to previous blocks, ensuring the integrity of the entire transaction history.

Smart Contracts for Rules and Policies:

Implement smart contracts, self-executing code on the blockchain, to enforce predefined rules and policies related to transactions.

Define conditions and criteria within smart contracts that trigger fraud detection mechanisms if met.

Consensus Mechanism:

Employ a consensus'methods (e.g. Proof of Stake, or variations) to verify and agree on the authenticity of transactions across the network.

Consensus mechanisms ensure agreement among network participants, minimizing the risk of fraudulent transactions being accepted.

Immutable Audit Trail:

Leverage the blockchain's immutable nature to create an audit trail of transactions that can be accessed and validated by intendedcandidates.

Any attempt to alter historical transaction data would be highly challenging due to the cryptographic links between blocks.

Real-time Monitoring and Analysis:

Implement monitoring tools that continuously analyze incoming transactions in real-time.

Use analytics and AI-based algorithms to detect unusual patterns, anomalies, or suspicious behavior that may indicate fraudulent activity.

Decentralized Verification and Validation:

Engage the decentralized network of nodes to verify transactions and consensus algorithms to validate them.

Transactions flagged as potentially fraudulent can be subjected to additional verification steps by multiple nodes in the network before approval.

Secure Identity Management:

Implement secure identity management systems using cryptographic keys and digital signatures to authenticate participants in the network.

Ensure that each participant's identity is verified and tied to their transactions securely.

Redundancy and Resilience:

Utilize the redundancy and resilience inherent in blockchain networks to mitigate the risk of a single point of failure or tampering.

Multiple copies of the ledger across nodes ensure data redundancy and protection against unauthorized modifications.

Continuous Improvement and Collaboration:

Foster collaboration among network participants, financial institutions, and regulatory bodies to continually enhance fraud detection mechanisms.

Implement updates and improvements based on shared insights and evolving fraud patterns.

Compliance and Privacy:

Ensure compliance with legal and regulatory requirements related to financial transactions and data privacy.

Implement privacy-preserving measures to protect sensitive information while maintaining transparency and compliance.

This blockchain-based model establishes a secure, transparent, and fraud-resistant environment for live transactional financial systems by leveraging the strengths of blockchain technology in combination with fraud detection mechanisms.

Final Step: Proposed Theoretical model combining Blockchain and AI to consist of:

Data Collection:

Gather transactional data from various sources including financial institutions, digital transactions, historical records, etc.

Normalize and preprocess the data to make it suitable for analysis.

Blockchain Integration:

Use blockchain for data storage and immutability.

Create a decentralized ledger to store transactional records securely.

Ensure that the blockchain network maintains transparency and integrity of data across all nodes.

AI Model Development:

Implement AI-based classification algorithms (such as neural networks, decision trees, or ensemble methods) to analyze transactional patterns.

Train the AI model using historical transaction data labeled as fraudulent or non-fraudulent to learn patterns indicative of fraudulent behavior.

Feature Engineering and Selection:

Extract requiredcharacteristics from the transactional data that can be used as input to the AI model.

Select the most significant features that contribute to fraud detection and discard irrelevant or redundant ones.

Real-time Monitoring:

Implement a real-time monitoring system that continuously feeds live transaction data into the AI model.

Utilize the AI model to analyze incoming transactions in real-time and flag potentially fraudulent activities based on learned patterns.

Scalability and Efficiency:

Ensure the system's scalability to handle a large volume of transactions efficiently.

Optimize the AI model for faster predictions without compromising accuracy.

Verification and Validation:

Introduce mechanisms to verify flagged transactions, potentially involving human intervention or additional validation steps.

Continuously validate and refine the AI model using feedback from verified transactions to improve accuracy and reduce false positives.

Feedback Loop and Improvement:

Establish a feedback loop to update the AI model periodically with new data and evolving fraud patterns.

Leverage the decentralized nature of blockchain to securely share updated models across the network.

Privacy and Compliance:

Ensure compliance with data privacy regulations by implementing encryption and privacy-preserving techniques while storing sensitive information on the blockchain.

Adhere to regulatory standards to maintain trust and compliance within the financial sector.

Continuous Monitoring and Maintenance:

Implement continuous monitoring of the system's performance and security.

Regularly maintain and update the system to adapt to changing fraud patterns and technological advancements.

This theoretical model aims to leverage the strengths of blockchain's security and immutability with AI's pattern recognition and real-time analysis to build a robust fraud detection system for live transactional financial systems.

5.8 Answers to Research Questions

Questions	Answers
1. What is a primary advantage of using a blockchain-based AI model for fraud detection?	Assessing basic knowledge of the amalgamation of AI and blockchain. Analysis: Look for responses that grasp the core concept of combining AI and blockchain for fraud detection, showcasing an understanding of their potential synergy.
2. Which technology ensures the immutability of transactional records in a blockchain?	Evaluating the recognition of challenges in traditional fraud detection. Analysis: Examine responses acknowledging limitations or shortcomings of conventional fraud detection methods, emphasizing the need for innovative solutions like AI and blockchain.

3. How does AI contribute to fraud detection in a live financial system?	Assessing comprehension of blockchain's role in bolstering security. Analysis: Look for responses highlighting blockchain's features (e.g., immutability, decentralization) that enhance security in financial systems.
4. What is the significance of real-time monitoring in detecting financial frauds?	Evaluating familiarity with AI algorithms for fraud detection. Analysis: Examine responses that mention specific AI algorithms (e.g., neural networks, decision trees) applicable to fraud detection, demonstrating knowledge of AI's role in pattern recognition.
5. What role does a smart contract play in a blockchain-based fraud detection system?	Assessing understanding of the collaborative potential between AI and blockchain. Analysis: Look for responses that illustrate how AI's analytical capabilities complement blockchain's security features, offering a comprehensive solution for fraud detection.

CHAPTER VI:

SUMMARY, IMPLICATIONS, AND RECOMMENDATIONS

6.1 Summary

Combining blockchain and artificial intelligence (AI) represents a potent synergy that addresses the deficiencies of each technology while harnessing their complementary strengths. In the context of detecting frauds in live transactional financial systems, this integration proves crucial in establishing a robust framework that enhances security, transparency, and efficiency. Understanding the distinct advantages and limitations of blockchain and AI is essential to grasp the significance of their combined application in fraud detection within dynamic financial environments.

Blockchain technology, known for its decentralized, immutable, and transparent ledger, offers a secure and tamper-resistant system for storing transactional data. However, it faces challenges related to scalability, privacy, and real-time data processing. Conversely, AI exhibits sophisticated analytical capabilities, adept at identifying complex patterns and anomalies in vast datasets, yet may lack inherent security measures and can be vulnerable to adversarial attacks.

In a live transactional financial system, where immediate detection and prevention of fraudulent activities are paramount, the integration of blockchain and AI addresses these challenges comprehensively. Blockchain's immutability ensures the integrity of transaction records, reducing the risk of data tampering or unauthorized modifications. This feature forms the backbone of a trustworthy and auditable system, mitigating the shortcomings of AI in securing data integrity.

Conversely, AI augments the efficiency of fraud detection by utilizing advanced algorithms to continuously analyze transactional patterns in real-time. Machine learning models, such as neural networks or decision trees, excel at identifying anomalous behaviors or suspicious activities that might signify potential fraud. This capability offsets blockchain's limitations in providing real-time analysis due to its inherent design for data immutability.

Moreover, blockchain's decentralized nature and AI's analytical prowess collectively bolster the transparency and traceability of financial transactions. The transparent nature of blockchain, coupled with AI's ability to scrutinize data patterns, offers unparalleled visibility into transactions, enabling rapid identification of irregularities or fraudulent behaviors.

Furthermore, the integration facilitates secure and private data handling, overcoming AI's vulnerability to data breaches or unauthorized access. Utilizing cryptographic techniques within the blockchain ecosystem ensures the confidentiality of sensitive financial data while allowing AI algorithms to leverage this secure environment for analysis.

Another critical aspect is the resilience and fault tolerance offered by blockchain's distributed architecture. In case of system failures or attempted breaches, the decentralized structure ensures that the network continues to function, preventing a single point of failure. This resilience complements AI's need for a stable and reliable data source, mitigating the risk of interruptions or data inconsistencies.

Additionally, the integration enables the automation of fraud detection protocols through smart contracts, self-executing code stored on the blockchain. Smart contracts enforce predefined rules and conditions, automating verification processes and enhancing the efficiency of fraud detection mechanisms.

6.2 Implications

The combined blockchain-based AI classification model in live transactional financial systems, therefore, presents a holistic approach that capitalizes on the strengths of both technologies while mitigating their individual deficiencies. It offers a secure, transparent, and efficient framework that ensures the integrity of transactional data, enables real-time analysis for fraud detection, and enhances the overall resilience of financial systems against fraudulent activities. This integration marks a significant advancement in safeguarding financial transactions, fostering trust, and fortifying the security posture of live transactional financial systems.

The implications of merging a blockchain-based AI classification model for fraud detection in live transactional financial systems are far-reaching and transformative across several dimensions:

1. Unprecedented Security: Combining blockchain's immutable, decentralized ledger with AI's sophisticated pattern recognition creates a potent defense against fraud. This synergy ensures tamper-proof records and enables real-time analysis, significantly bolstering security measures within financial systems.

2. Proactive Fraud Detection: The integration enables the system to proactively identify potential fraudulent activities by continuously learning from transactional data. This real-time detection capability helps prevent fraud before it escalates, reducing financial losses and preserving trust among stakeholders.

3. Enhanced Accuracy and Efficiency: AI-driven classification models, when integrated with blockchain, offer improved accuracy in identifying anomalies or suspicious patterns within transactions. This efficiency minimizes false positives and streamlines the detection process, saving time and resources for financial institutions.

4. Transparency and Accountability: The transparent nature of blockchain ensures an immutable audit trail of transactions. When coupled with AI's analysis, it not only detects fraud but also enhances transparency, fostering trust among users, regulators, and financial institutions. This transparency holds parties accountable for their actions within the system.

5. Regulatory Adaptation: The convergence of blockchain and AI in fraud detection necessitates regulatory adaptations. Policymakers and regulatory bodies need to navigate the complexities of overseeing decentralized systems powered by AI to ensure compliance, data privacy, and fairness in financial transactions.

6. Shift in Industry Standards: Successful integration could prompt a shift in industry standards for fraud detection. As this hybrid system proves its effectiveness, it might become the benchmark, encouraging widespread adoption and setting new standards for security measures in financial transactions.

7. Challenges in Data Privacy and Bias: Leveraging AI for fraud detection raises concerns about data privacy and algorithmic bias. Striking a balance between utilizing sensitive user data for detection and protecting individual privacy is crucial. Additionally, ensuring AI algorithms are free from bias is imperative for fair and accurate fraud identification.

8. Global Impact and Collaboration: The adoption of this technology could have a global impact, encouraging collaboration among financial institutions, governments, and technology providers. Collaborative efforts can drive standardization, knowledge sharing, and the establishment of best practices for secure and ethical implementation worldwide.

9. Evolution of Financial Infrastructure: The integration might pave the way for an evolution in financial infrastructure, transitioning towards more secure, efficient, and technologically advanced systems. This shift could influence how transactions are conducted, verified, and secured across various financial sectors.

10. Innovation and Technological Advancements: Continued research and development in this domain could lead to further innovations in AI, blockchain, and their integration. It might catalyze advancements in decentralized applications, smart contracts, and data analysis techniques, influencing not just fraud detection but various other industries and applications.

In essence, the fusion of blockchain-based AI classification models for fraud detection in live transactional financial systems signifies a pivotal moment in fortifying security measures, enhancing transparency, and shaping the future landscape of financial transactions. However, addressing challenges related to regulation, privacy, bias, and fostering collaboration will be pivotal in realizing the full potential of this integration.

6.3 Recommendations for Future Research

Further research and development into advanced AI algorithms, such as reinforcement learning and deep learning models, tailored specifically for fraud detection in live transactional systems could explore ensemble methods that combine multiple AI models to enhance accuracy and robustness in identifying fraudulent activities.

Real-time Data Processing and Analysis:

Focus on optimizing AI algorithms for real-time data processing within the constraints of blockchain's immutable nature.

Implement edge computing or distributed AI techniques to enable faster analysis of transactions without compromising the integrity of blockchain data.

Privacy-Preserving Techniques:

Research and integrate privacy-preserving AI techniques (like federated learning or homomorphic encryption) within blockchain-based systems to protect sensitive financial data while allowing AI analysis.

Smart Contract Automation and Verification:

Develop sophisticated smart contracts that automate and optimize the verification process for detecting fraudulent transactions.

Implement self-learning smart contracts that continuously evolve based on detected fraud patterns and feedback.

Collaborative Ecosystem and Standards:

Foster collaboration among industry stakeholders, regulatory bodies, and technology innovators to establish best practices and regulatory standards for integrating blockchain and AI in financial systems.

Engage in knowledge sharing and industry-wide initiatives to create a robust ecosystem supporting the combined usage of blockchain and AI for fraud detection.

Robust Security Measures:

Strengthen security measures within blockchain networks to fortify against potential AI-based attacks or vulnerabilities.

Implement multi-factor authentication, encryption, and consensus mechanisms to safeguard against adversarial AI attacks.

Continuous Monitoring and Adaptation:

Establish continuous monitoring mechanisms to evaluate the performance of the combined blockchain-based AI model in detecting frauds.

Implement adaptive AI models that can dynamically adjust to evolving fraud patterns and changing financial landscapes.

Education and Skill Development:

Invest in educating professionals and stakeholders about the capabilities, limitations, and potential of combining blockchain and AI for fraud detection.

Foster skill development programs to train individuals in the specialized domain of blockchain-based AI fraud detection systems.

Ethical Considerations and Governance:

Address ethical implications and governance frameworks concerning the use of AI in financial systems to ensure fairness, transparency, and accountability.

Establish regulatory frameworks that govern the intended use of blockchain-based AI for fraud observation, balancing innovation with ethical guidelines.

By focusing on these strategic pathways, the combined usage of blockchain and AI for detecting frauds in live transactional financial systems can be optimized, paving the way for more secure, efficient, and trustworthy financial transactions in the future.

6.4 Conclusion

The intention of the 12 questions designed on the topic: "Building A Blockchain Based Artificial Intelligence (AI) Classification Model To Detect Frauds In A Live Transactional Financial System." is to gather information and insights related to the various aspects of this complex and interdisciplinary field. The questions aimed to cover various aspects related to the integration of blockchain and AI, fraud detection, and the importance of different technologies in a financial context.

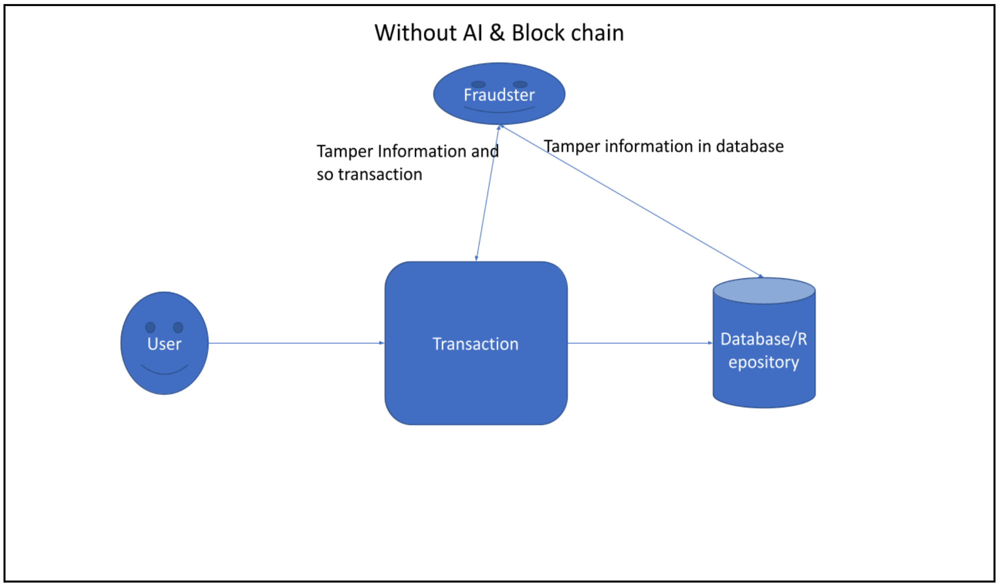

Without AI & Block chain
Fraudster
Tamper Information and so transaction
Tamper information in database
User
Transaction
Database/Repository

Figure 3 Financial Transactional system without AI and Blockchain

The study has proposed a theoretical model to amalgamate the two most disruptive technologies of recent time’s viz., Blockchain and AI into solving the business problem of detecting frauds in a live transactional financial system. Also, since both blockchain and AI are undergoing tremendous and rapid advances, it is felt that the amalgamation of these two technologies viz., Blockchain and AI is bound to happen over a period of time and such amalgamation would strengthen the positives of the two technologies while countering the vulnerabilities associated with each one of them as individual technologies and thus provide a very agile, efficient way and add a totally different dimension to approach business problems which presently are being viewed for solutions from individual prisms by the two technologies.

Fig 6.2 Financial transactional system with AI and Blockchain integrated

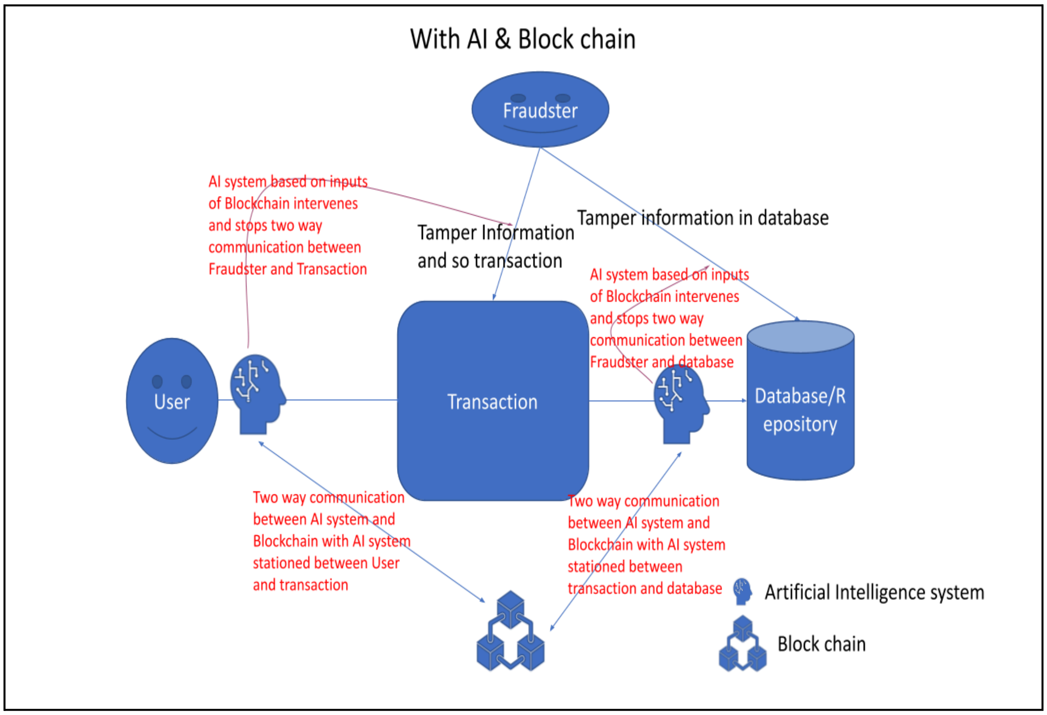

With AI & Block chain
Fraudster
AI system based on inputs of Blockchain intervenes and stops two way communication between Fraudster and Transaction
Tamper Information and so transaction
Tamper information in database
AI system based on inputs of Blockchain intervenes and stops two way communication between Fraudster and database
User
Transaction
Database/R epository
Two way communication between AI system and Blockchain with AI system stationed between User and transaction
Two way communication between AI system and Blockchain with AI system stationed between transaction and database
Artificial Intelligence system
Block chain

Figure 4 Financial transactional system with AI and Blockchain integrated

The combined usage of blockchain and AI holds immense promise for detecting frauds in live transactional financial systems. Moving forward, specific strategies can be implemented to harness the synergy between these technologies and further enhance their effectiveness in combating financial fraud:

Enhanced Data Integration and Interoperability:

Develop standardized protocols and frameworks for seamless integration of AI algorithms with blockchain technology in financial systems.

Establish interoperability standards to ensure efficient data sharing and communication between different blockchain networks and AI applications, enabling comprehensive fraud detection.

6.5 Key Takeaways

The key takeaways from the research on "Building a Blockchain Based Artificial Intelligence Classification Model to Detect Frauds in a Live Transactional Financial System":

(1) Financial frauds need to be caught only when the transaction is really happening in the system (concurrent audit) and not before entering the system (pre-audit) or after exiting the system (post audit) and

(2) Amalgamation of Blockchain and Artificial Intelligence together is the logical way forward to achieve the same.

Importance of Concurrent Audit for Fraud Detection: The research emphasizes the necessity of identifying and addressing financial frauds during live transactions (concurrent audit) rather than solely relying on pre-audit or post-audit measures.

Justification: Real-time Detection: Detecting fraud during live transactions enables real-time identification and prevention, reducing the potential damage caused by fraudulent activities. By leveraging blockchain's transparent and immutable nature, suspicious activities can be flagged instantly, ensuring immediate intervention.

Enhanced Accuracy: Concurrent audit harnesses the power of AI to analyze ongoing transactions, enabling the system to learn and adapt based on real-time data. This continuous learning process improves the accuracy and efficiency of fraud detection algorithms, reducing false positives and negatives.

Prevention Over Cure: Addressing fraud during transactions directly prevents the fraudulent activities from affecting the financial system, as opposed to post-audit detection where the damage might have already been done. This proactive approach safeguards the integrity of the system.

Synergy of Blockchain and Artificial Intelligence for Fraud Detection:

The research advocates for the combination of blockchain and AI technologies as a strategic approach to effectively combat financial frauds.

Blockchain's immutable ledger provides a secure and transparent record of transactions. Integrating AI into this framework allows for the development of sophisticated fraud detection algorithms that can analyze and identify anomalies within this tamper-resistant ledger.

AI's Analytical Power: Artificial Intelligence, particularly machine learning models, can process vast amounts of transactional data on the blockchain. These models can learn patterns of normal behavior and detect deviations or anomalies indicative of fraudulent activities, contributing to more robust fraud prevention.

Collaborative Strength: By amalgamating blockchain's secure, decentralized ledger with AI's analytical capabilities, the system gains a comprehensive fraud detection mechanism. The synergy between these technologies enhances the system's ability to detect and prevent frauds efficiently.

Summary: The research underscores the significance of concurrent audit in detecting financial frauds during live transactions and advocates for the integration of blockchain and AI technologies to create a robust and proactive system capable of identifying and preventing fraudulent activities in real-time.

BIBLIOGRAPHY

Albshaier, L., Almarri, S. and Hafizur Rahman, M.M., (2024) 'A Review of Blockchain's Role in E-Commerce Transactions: Open Challenges, and Future Research Directions'. *Computers*, 13(1), p.27.

Almeida, G. and Vasconcelos, F., (2023) 'Self-Healing Networks: Adaptive Responses to Ransomware Attacks'.*Preprints (www.preprints.org)*

Anand, D. & Siddhartha, C., (2023)'Blockchain and machine learning for data analytics, privacy preserving, and security in fraud detection'. *i-manager's Journal on Software Engineering*.

Apoorva Kumar (2024) 'Payment Frauds: The Hidden Risks Behind Digital Transactions', *Available at: https://decentro.tech/blog/payment-frauds/*

Artsyl (2023) 'Invoice Verification: Process and Standards of Invoice Checking', *Available at: https://www.artsyltech.com/invoice-verification-as-part-of-invoice-processing*

Ashton, R.H., Graul, P.R. and Newton, J.D., (1989) 'Audit delay and the timeliness of corporate reporting'. *Contemporary accounting research,* 5(2), pp.657-673.

Auditing Standard, (2023)'PCAOB auditing standards' Available at: *https://pcaobus.org/oversight/standards/auditing-standards*. *PCAOB(Public Company Accounting Oversight Board).*

Awoyemi, J.O., Adetunmbi, A.O. and Oluwadare, S.A., (2017) 'Credit card fraud detection using machine learning techniques: A comparative analysis'. *In 2017 international conference on computing networking and informatics (ICCNI)* (pp. 1-9). *IEEE*.

Bahuguna, D., Kaur, J. and Singh, B., (2023)'Artificial Intelligence's Integration in Supply Chain Management: A Comprehensive Review'. *European Economics Letter, 13(3), pp.1512-1527*.

Bhumichai, D., Smiliotopoulos, C., Benton, R., Kambourakis, G. and Damopoulos, D., (2024) 'The Convergence of Artificial Intelligence and Blockchain: The State of Play and the Road Ahead'. *Information*, 15(5), p.268.

Blowers, M.K., Scrafford, S. and Williams, J., (2019)‘Blockchain technologies and distributed ledger systems as enablers for real time decision support’. *Proceedings of the SPIE*, 11013, pp.110130L-110130L-5.

Cara Malone (2023) ‘Online Payment Fraud: Market Forecasts, Emerging Threats & Segment Analysis 2023-2028’. *Available: https://www.juniperresearch.com/research/fintech-payments/fraud-identity/online-payment-fraud-research-report/*

Chen M. and Wang L., (2020) ‘Integrating Blockchain and Artificial Intelligence for Fraud Detection in Banking Transactions’. *Proceedings of the International Conference on Computational Intelligence and Data Science*,

Cirqueira, D., Helfert, M. and Bezbradica, M., (2021) ‘Towards design principles for user-centric explainable AI in fraud detection’. *In International Conference on Human-Computer Interaction (pp. 21-40). Cham: Springer International Publishing.*

De Andrés, J. and Lorca, P., (2021) ‘On the impact of smart contracts on auditing’. *International Journal of Digital Accounting Research, 21*.

Dillenberger, D., Novotný, P., Zhang, Q., Jayachandran, P., Gupta, H., Hans, S., Verma, D., Chakraborty, S., Thomas, J.J., Walli, M. & Sarpatwar, K.K., (2019)‘Blockchain analytics and artificial intelligence’. *IBM J. Res. Dev.*, 63, pp.5:1-5:14.

Dinh, T.N. and Thai, M.T., (2018) ‘AI and blockchain: A disruptive integration’. *Computer*, 51(9), pp.48-53.

Dong, S., Abbas, K., Li, M. and Kamruzzaman, J., (2023) ‘Blockchain technology and application: an overview’. *PeerJ Computer Science*, 9, p.e1705.

Dyball, M.C. and Seethamraju, R., (2021) ‘The impact of client use of blockchain technology on audit risk and audit approach—An exploratory study’. *International Journal of Auditing*, 25(2), pp.602-615.

Edwards, (2023) ‘How to Combat e-commerce Fraud and Secure Online Sales’. Available at: *https://ecommercegermany.com/blog/how-to-combat-ecommerce-fraud-and-secure-online-sales*.

Everett, C., (2016) ‘Ransomware: to pay or not to pay?’. *Computer Fraud & Security*, 2016(4), pp.8-12.

Getie Mihret, D., Mula, J.M. and James, K., (2012) ‘The development of internal auditing in Ethiopia: the role of institutional norms’. *Journal of financial reporting and accounting*, 10(2), pp.153-170.

Goel, V., Bhalla, D., Bhardwaj, T. and Bansal, S., (2022) ‘The Impact of COVID-19 on the Electronic Commerce User’s Behavior’. *Journal of Business Management and Information Systems*, 9(1), pp.15-19.

Gupta, P., (2023) ‘Leveraging Machine Learning and Artificial Intelligence for Fraud Prevention’. *SSRG International Journal of Computer Science and Engineering*, 10(5), pp.47-52.

Hackett, A. and Strickland, K., (2018) ‘Using the framework approach to analyse qualitative data: a worked example’. *Nurse researcher*, 26(2).

Han, H., Shiwakoti, R.K., Jarvis, R., Mordi, C. and Botchie, D., (2023) ‘Accounting and auditing with blockchain technology and artificial Intelligence: A literature review’. *International Journal of Accounting Information Systems*, 48, p.100598.

Hassan, M., Aziz, L.A.R. and Andriansyah, Y., (2023) ‘The role artificial intelligence in modern banking: an exploration of AI-driven approaches for enhanced fraud prevention, risk management, and regulatory compliance’. *Reviews of Contemporary Business Analytics*, 6(1), pp.110-132.

Javaid, M., Haleem, A., Singh, R.P., Suman, R. and Khan, S., (2022) ‘A review of Blockchain Technology applications for financial services’. *BenchCouncil Transactions on Benchmarks, Standards and Evaluations*, 2(3), p.100073.

Jo Ann Barefoot (2020) ‘Digital Technology Risks for Finance:Dangers Embedded in Fintech and Regtech’. Available: *https://www.hks.harvard.edu/sites/default/files/centers/mrcbg/files/AWP_151_final.pdf*

Julia Kagan (2021) ‘Synthetic Identity Theft: What it is, How it Works’. *Available: https://www.investopedia.com/terms/s/synthetic-identity-theft.asp*

Khan, S.N., Loukil, F., Ghedira-Guegan, C., Benkhelifa, E. and Bani-Hani, A., (2021) 'Blockchain smart contracts: Applications, challenges, and future trends'. *Peer-to-peer Networking and Applications*, 14, pp.2901-2925.

Kinga Edwards (2023) 'How to combat e-commerce Fraud and Secure Online Sales', Available *at: https://ecommercegermany.com/blog/how-to-combat-ecommerce-fraud-and-secure-online-sales*

Kishor, R., (2023). 'Smart Contract Based Fraud Degree Detection System'. *Interantional Journal of Scientific Research in Engineering And Management.*

Koch, M., (2018) 'Artificial intelligence is becoming natural'. *Cell*, 173(3), p.531.

KumarS., and JhaR. S., (2021) 'A Survey of Blockchain Technology in Fraud Detection: Applications, Challenges, and Opportunities' *International Journal of Advanced Computer Science and Applications*,

Kuznetsov, A., Sernani, P., Romeo, L., Frontoni, E. and Mancini, A., (2024) 'On the Integration of Artificial Intelligence and Blockchain Technology: A Perspective About Security'. *IEEE Access*.

Law, K. and Shen, M., (2020)'How does artificial intelligence shape the audit industry'. *Available at SSRN*, pp.5-43.

LeeT., and KimH., (2020) 'Enhanced Financial Fraud Detection System using Blockchain and Machine Learning' *IEEE International Conference on Blockchain and Cryptocurrency*, pp. 273-282

Li, R., Liu, Z., Ma, Y., Yang, D. & Sun, S., (2023)'Internet Financial Fraud Detection Based on Graph Learning'. *IEEE Transactions on Computational Social Systems*, 10, pp.1394-1401.

Lloyd, M.E., (2001) 'Emerging opportunities in environmental auditing'. *University of Calgary.*

Luo, B., Zhang, Z., Wang, Q., Ke, A., Lu, S. & He, B., (2023)'AI-powered Fraud Detection in Decentralized Finance: A Project Life Cycle Perspective'. *ArXiv, abs/2308.15992*.

McMahan, B., Moore, E., Ramage, D., Hampson, S. and y Arcas, B.A., (2017) ‘Communication-efficient learning of deep networks from decentralized data’. *In Artificial intelligence and statistics* (pp. 1273-1282). PMLR.

Meduri, K., (2024) ‘Cybersecurity threats in banking: Unsupervised fraud detection analysis’. *International Journal of Science and Research Archive*, 11(2), pp.915-925.

Mehta V., and Gupta P. N. (2018) ‘Blockchain and Artificial Intelligence Techniques for Financial Fraud Detection’. *Procedia Computer Science*,

Minastireanu, E.A. and Mesnita, G., (2019) ‘An Analysis of the Most Used Machine Learning Algorithms for Online Fraud Detection’. *Informatica Economica*, 23(1).

Munappy, A.R., Bosch, J., Olsson, H.H., Arpteg, A. and Brinne, B., (2022) ‘Data management for production quality deep learning models: Challenges and solutions’. *Journal of Systems and Software*, 191, p.111359.

Nordstrom, C. and Carlson, L., (2014) ‘Cyber shadows: Power, crime, and hacking everyone’. *ACTA Publications*.

NSB & Co. (2022) ‘Why Concurrent Audit Is Important For Banks?’ Available at: https://nsbandco.com/blog/why-concurrent-audit-is-important-for-banks-2/.

Odeyemi, O., Mhlongo, N.Z., Nwankwo, E.E. and Soyombo, O.T., (2024) ‘Reviewing the role of AI in fraud detection and prevention in financial services’. *International Journal of Science and Research Archive,* 11(1), pp.2101-2110.

Odeyemi, O., Okoye, C.C., Ofodile, O.C., Adeoye, O.B., Addy, W.A. and Ajayi-Nifise, A.O., (2024) ‘Integrating AI with blockchain for enhanced financial services security’. *Finance & Accounting Research Journal*, 6(3), pp.271-287.

OtebolakuA. S. and SholaO. O., (2019) ‘A Blockchain-based Artificial Intelligence Approach for Credit Card Fraud Detection’. *IEEE International Conference on Data Science and Advanced Analytics (DSAA)*,

Owen, J. and Godwin, O., (2024) ‘Harnessing Blockchain and Emerging Technologies in Logistics: A Paradigm Shift in Supply Chain Management’.

Parvatiyar, A., Donthu, N., Gruen, T., Jacobs, F. and Kesel, B., (2005) ‘Best practices in post-audit recovery: An examination of prevalent post-audit practices in the retail industry’. *Atlanta, GA: iCRM/CBIM*.

PatelN. and GuptaS., (2020) ‘A Hybrid Blockchain-AI Approach for Real-Time Fraud Detection in Financial Systems’ *International Journal of Computer Applications,*

Perifanis, N.A. and Kitsios, F., (2023) ‘Investigating the influence of artificial intelligence on business value in the digital era of strategy: A literature review’. *Information,* 14(2), p.85.

Philipsen, K., (2018) ‘Theory building: Using abductive search strategies’. *Collaborative research design: Working with business for meaningful findings,* pp.45-71.

Politou, E., Casino, F., Alepis, E. and Patsakis, C., (2019) ‘Blockchain mutability: Challenges and proposed solutions’. *IEEE Transactions on Emerging Topics in Computing*, 9(4), pp.1972-1986.

Pranto, T.H., Hasib, K.T.A.M., Rahman, T., Haque, A.B., Islam, A.N. and Rahman, R., (2022)‘Blockchain and Machine Learning for Fraud Detection: A Privacy-Preserving and Adaptive Incentive Based Approach’. *IEEE Access*, 10, pp.87115-87134.

Qi, Y. and Xiao, J., (2018) ‘Fintech: AI powers financial services to improve people's lives’. *Communications of the ACM*, 61(11), pp.65-69.

Quak, E.J., (2020)‘The impact of Public Finance Management (PFM) reforms on education in Tanzania’. *Institute of Development Studies. https://opendocs. ids. ac. uk/opendocs/handle/20.500, 12413*, p.14999.

Rabin, Y. and Peled, R., (2024) ‘Real‐time audit of public agencies: Utility, controversy and lessons for an emerging practice’. *International Journal of Auditing*, 28(2), pp.328-339.

Rakshit, Anuska& Kumar, Shriya. (2022) ‘Fraud Detection: A Review on Blockchain’.

Regueiro, C., Seco, I., Gutiérrez-Agüero, I., Urquizu, B. and Mansell, J., (2021). ‘A blockchain-based audit trail mechanism: Design and implementation’. *Algorithms,* 14(12), p.341.

Roberts, R.E., (2020) ‘Qualitative Interview Questions: Guidance for Novice Researchers’. *Qualitative Report*, 25(9).

Sadiq, A.S., Faris, H., Ala'M, A.Z., Mirjalili, S. and Ghafoor, K.Z., (2019) ‘Fraud detection model based on multi-verse features extraction approach for smart city applications’. *In Smart cities cybersecurity and privacy* (pp. 241-251). *Elsevier.*

Salah, K., Rehman, M.H.U., Nizamuddin, N. and Al-Fuqaha, A., (2019) ‘Blockchain for AI: Review and open research challenges’. *IEEE access*, 7, pp.10127-10149.

Sambrow, V.D.P. and Iqbal, K., (2022) ‘Integrating Artificial Intelligence in Banking Fraud Prevention: A Focus on Deep Learning and Data Analytics’. *Eigenpub Review of Science and Technology*, 6(1), pp.17-33.

Sarkar, G. and Shukla, S.K., (2023) ‘Behavioral analysis of cybercrime: Paving the way for effective policing strategies’. *Journal of Economic Criminology*, p.100034.

Schmidhuber, J., (2015) ‘Deep learning in neural networks: An overview’. *Neural networks*, 61, pp.85-117.

Sharma, R., Goel, S., Lenka, S.R. and Satpathy, P.R., (2024) ‘Energy Efficiency Retrofitting Measures of an Institutional Building: A Case Study in Eastern India’. *Cleaner Energy Systems*, p.100111.

SharmaR., and JainA., (2019) ‘Fraud Detection in Banking Using Blockchain and Machine Learning’ *Journal of Advanced Research in Computer Science*.

Shaw, N., Eschenbrenner, B. and Baier, D., (2022) ‘Online shopping continuance after COVID-19: A comparison of Canada, Germany and the United States’. *Journal of Retailing and Consumer Service*s, 69, p.103100.

Shete, N.L., Maddel, M. and Shaikh, Z., (2024)‘A Comparative Analysis of Cybersecurity Scams: Unveiling the Evolution from Past to Present’. *In 2024 IEEE 9th International Conference for Convergence in Technology (I2CT)* (pp. 1-8). IEEE.

SmithJ., and JohnsonK., (2020) ‘Combining Blockchain and AI for Fraud Detection in Financial Transactions’. *Journal of Information Management*, 2020

Snyder, H., (2019). ‘Literature review as a research methodology: An overview and guidelines’. *Journal of business research*, 104, pp.333-339.

Soori, M., Dastres, R. and Arezoo, B., (2024) ‘AI-Powered Blockchain Technology in Industry 4.0, A Review’. *Journal of Economy and Technology*.

Sponsored Program Services (2019) ‘The Pre-audit Process’. Available at :https://www.purdue.edu/business/sps/pdf/preauditprocess.pdf

Swan, M., (2015). ‘Blockchain: Blueprint for a new economy’. *O'Reilly Media, Inc*.

Tagde, P., Tagde, S., Bhattacharya, T., Tagde, P., Chopra, H., Akter, R., Kaushik, D. and Rahman, M.H., (2021) ‘Blockchain and artificial intelligence technology in e-Health’. *Environmental Science and Pollution Research*, 28, pp.52810-52831.

Taher, S.S., Ameen, S.Y. and Ahmed, J.A., (2024) ‘Advanced Fraud Detection in Blockchain Transactions: An Ensemble Learning and Explainable AI Approach’. *Engineering, Technology & Applied Science Research*, 14(1), pp.12822-12830.

Taherdoost, H., (2023) ‘Smart contracts in blockchain technology: A critical review’. *Information,* 14(2), p.117.

Team, N.A., (2018) ‘Nebula ai (nbai)—decentralized ai blockchain whitepaper’.

Thisarani, M. and Fernando, S., (2021) ‘Artificial intelligence for futuristic banking’. *In 2021 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC)* (pp. 1-13). *IEEE.*

Thukral, M.K., (2023)‘Security and Efficiency in Vehicle Insurance: A Blockchain-Based Solution’. *2023 International Conference on Self Sustainable Artificial Intelligence Systems (ICSSAS)*.

Tiwari, S., Agarwal, P. and Singh, R., (2022) ‘Assessment of Association between Financial Fraud Cases in reference to Transaction Volume & E-Auditing’. *Pacific Business Review International*, 14(11), pp.37-44.

Viana, L.F.C., (2022) ‘Accounting, Reporting, Auditing and Public Accountability of Public-Private Partnerships: The Portuguese Experience'.

Vincent, N.E., Skjellum, A. and Medury, S., (2020) ‘Blockchain architecture: A design that helps CPA firms leverage the technology’. *International Journal of Accounting Information Systems*, 38, p.100466.

Wang,Y. and ChenZ., (2021) ‘Review of Blockchain and Artificial Intelligence in Fraud Detection’ *International Journal of Computer Science and Network Security*,

Witt, L., Fortes, A.T., Toyoda, K., Samek, W. and Li, D., (2024) ‘Blockchain and Artificial Intelligence: Synergies and Conflicts’. *arXiv preprint arXiv:2405.13462*.

Wood, G., (2014) ‘Ethereum: A secure decentralised generalised transaction ledger’. *Ethereum project yellow paper*, 151(2014), pp.1-32.

Yamaguti Mondego, D., (2024) 'The Use of Artificial Intelligence to Enhance User Satisfaction in Cloud-Based Payment Systems in Australia'*(Doctoral dissertation, CQUniversity).*

Yawalkar, P.M., Paithankar, D.N., Pabale, A.R., Kolhe, R.V. and William, P., (2023) 'Integrated identity and auditing management using blockchain mechanism'. *Measurement: Sensors*, 27, p.100732.

ZhangH., and LiuX., (2021) 'Blockchain and Artificial Intelligence in Financial Fraud Detection: A Systematic Review' *IEEE Access*.

Zheng, Z. & Dai, H., (2019)'Blockchain Intelligence: When Blockchain Meets Artificial Intelligence'. ArXiv, abs/1912.06485.

Zkik, K., Sebbar, A., Fadi, O., Mustapha, O. & Belhadi, A., (2023)'A Graph Neural Network Approach for Detecting Smart Contract Anomalies in Collaborative Economy Platforms Based on Blockchain Technology'. *2023 9th International Conference on Control, Decision and Information Technologies (CoDIT).*

QUESTIONNAIRE

Questionnaire: These questions aim to test basic understanding and relevance of building a blockchain-based AI classification model for fraud detection in live transactional financial systems.

Q.1. What is a primary advantage of using a blockchain-based AI model for fraud detection?

a) Enhanced scalability

b) Increased transaction speed

c) Improved security and transparency

d) Reduced computational complexity

Correct Answer: c) Improved security and transparency

Q.2. Which technology ensures the immutability of transactional records in a blockchain?

a) Encryption

b) Decentralization

c) Consensus mechanism

d) Cryptographic hashing

Correct Answer: d) Cryptographic hashing

Q.3. How does AI contribute to fraud detection in a live financial system?

a) By centralizing transaction data

b) By automating compliance checks

c) By identifying patterns and anomalies

d) By increasing transaction speed

Correct Answer: c) By identifying patterns and anomalies

Q.4. What is the significance of real-time monitoring in detecting financial frauds?

a) It allows for delayed analysis

b) It enables proactive detection

c) It increases data complexity

d) It decreases transaction security

Correct Answer: b) It enables proactive detection

Q.5. What role does a smart contract play in a blockchain-based fraud detection system?

a) Enforces legal agreements

b) Records transactions privately

c) Speeds up transaction processing

d) Provides encryption keys

Correct Answer: a) Enforces legal agreements

Q.6. Which feature of blockchain technology aids in providing transparency and auditability?

a) Decentralization

b) Encryption

c) Scalability

d) Anonymity

Correct Answer: a) Decentralization

Q.7. What aspect of fraud detection does historical transaction data assist AI models with?

a) Predictive analytics

b) Real-time monitoring

c) Immediate resolution

d) Transaction authentication

Correct Answer: a) Predictive analytics

Q.8. How does the decentralized nature of blockchain contribute to fraud prevention?

a) By reducing transaction speed

b) By decreasing transparency

c) By increasing accountability

d) By limiting data access

Correct Answer: c) By increasing accountability

Q.9. Which factor is crucial for AI classification models to effectively detect frauds in live transactions?

a) Static algorithms

b) Lack of data variety

c) Continuous learning

d) Low processing power

Correct Answer: c) Continuous learning

Q.10. What is the primary role of AI algorithms in detecting fraudulent activities?

a) Identifying legitimate transactions

b) Improving data accuracy

c) Predicting future market trends

d) Recognizing abnormal patterns

Correct Answer: d) Recognizing abnormal patterns

Q.11. How can blockchain technologies enhance data security in fraud detection systems?

a) By eliminating data encryption

b) By storing data in a centralized server

c) By ensuring tamper-proof records

d) By reducing data redundancy

Correct Answer: c) By ensuring tamper-proof records

Q.12. Why is continuous improvement essential for AI models in fraud detection?

a) To decrease computational load

b) To identify static patterns

c) To adapt to evolving fraud methods

d) To eliminate historical data

Correct Answer: c) To adapt to evolving fraud methods

Coding documentation:

S.No	Description of Scenario	Page Numbers
1	To develop a blockchain based AI classification model for detecting frauds in a live transactional financial system in python.	129-131
2	To develop an Artificial Intelligence model for detecting frauds in a live transactional financial system in python using different classification types.	132-136
3	To Implement Blockchain before AI Classification model in python	137-139
4	To Implement AI Classification model before Blockchain integration in python	140-143
5.	Code relating to usage of five AI classification models on a data set of 100000 records in python:	144-148
6.	Code to demonstrate frauds missed by Blockchain system but caught by combined AI - blockchain system in python	149-151

S.No. 1 : To develop a blockchain based AI classification model for detecting frauds in a live transactional financial system in python.

Building a blockchain-based AI classification model for fraud detection involves integrating Python libraries for blockchain handling (like web3.py for Ethereum) and machine learning frameworks (such as scikit-learn or TensorFlow) for AI classification. A simplified example using Python that demonstrates the integration of a basic fraud detection AI model within a blockchain framework.

Let's create a simplified example that demonstrates how to structure such a system:

Step 1: Simulate a Simple Blockchain

```
# Simulated Blockchain Transactions
class Block:
def __init__(self, transaction_data, previous_hash):
self.transaction_data = transaction_data
self.previous_hash = previous_hash
self.nonce = 0
self.hash = self.calculate_hash()
def calculate_hash(self):
# Simplified hash calculation (not secure)
 return hashlib.sha256((str(self.transaction_data) + str(self.previous_hash) +
str(self.nonce)).encode()).hexdigest()
class Blockchain:
 def __init__(self):
self.chain = [self.create_genesis_block()]
```

```
 def create_genesis_block(self):
 return Block("Genesis Block", "0")
 def add_block(self, new_block):
new_block.previous_hash = self.chain[-1].hash
new_block.hash = new_block.calculate_hash()
self.chain.append(new_block)
```

Step 2: Implement Fraud Detection AI Model

We use a simple fraud detection model (a Decision Tree Classifier from scikit-learn) for demonstration purposes:

```
from sklearn.tree import DecisionTreeClassifier
# Sample Fraud Detection Model (using a Decision Tree Classifier)
class FraudDetectionModel:
 def __init__(self):
self.model = DecisionTreeClassifier()
 def train(self, X_train, y_train):
self.model.fit(X_train, y_train)
 def predict(self, X):
 return self.model.predict(X)
```

Step 3: Integration of AI Model and Blockchain

Here's a simplified integration of the AI model within the blockchain for fraud detection:

```
# Simulated Integration of AI Model and Blockchain
class BlockchainAI:
 def __init__(self):
self.blockchain = Blockchain()
self.fraud_model = FraudDetectionModel()
 def add_transaction_to_blockchain(self, transaction_data):
new_block = Block(transaction_data, self.blockchain.chain[-1].hash)
self.blockchain.add_block(new_block)
 # Assuming transaction_data is structured features for the AI model
 # Train AI model with existing blockchain data
X_train = [...] # Extract features from blockchain transactions
y_train = [...] # Labels (fraudulent or not)
self.fraud_model.train(X_train, y_train)
 def detect_fraud(self, transaction_data):
 # Predict if the new transaction is fraudulent
 prediction = self.fraud_model.predict([transaction_data])
 return prediction
```

This example combines a simulated blockchain structure with a basic fraud detection AI model. Note: In a real-world scenario, one would replace the simulated blockchain with a live blockchain network and build a more sophisticated AI model tailored to financial transaction data. We also need to keep in mind that building a production-level system requires careful consideration of security, scalability, and real-time data handling, which would involve more complex implementation and integration strategies.

//**//

S.No. 2. To Develop an Artificial Intelligence model for detecting frauds in a live transactional financial system in python using different classification types with explanations

The aim is to demonstrate utilizing different classification algorithms using Python's scikit-learn library.

Step 1: Import Necessary Libraries

```
import pandas as pd
from sklearn.model_selection import train_test_split
from sklearn.preprocessing import StandardScaler
from sklearn.linear_model import LogisticRegression
from sklearn.tree import DecisionTreeClassifier
from sklearn.ensemble import RandomForestClassifier
from sklearn.metrics import accuracy_score, precision_score, recall_score, f1_score
```

Step 2: Prepare the Data

We assuming that we have a dataset with transactional features and labels indicating fraudulent transactions:

```
# Assuming 'X' contains features and 'y' contains labels (0 for non-fraudulent, 1 for fraudulent)
# Replace this with your actual dataset preparation
# Split the data into training and testing sets
X_train, X_test, y_train, y_test = train_test_split(X, y, test_size=0.2, random_state=42)
# Feature scaling for better model performance
scaler = StandardScaler()
```

```
X_train = scaler.fit_transform(X_train)
X_test = scaler.transform(X_test)
```

Step 3: Implement Different Classification Models

Let's implement Logistic Regression, Decision Tree, and Random Forest classifiers:

```
# Logistic Regression Classifier
lr_classifier = LogisticRegression(max_iter=1000)
lr_classifier.fit(X_train, y_train)
lr_predictions = lr_classifier.predict(X_test)
# Decision Tree Classifier
dt_classifier = DecisionTreeClassifier()
dt_classifier.fit(X_train, y_train)
dt_predictions = dt_classifier.predict(X_test)
# Random Forest Classifier
rf_classifier = RandomForestClassifier()
rf_classifier.fit(X_train, y_train)
rf_predictions = rf_classifier.predict(X_test)
```

Step 4: Evaluate Model Performance

Evaluate the performance of each model using various metrics:

```
def evaluate_model(predictions, y_true):
 accuracy = accuracy_score(y_true, predictions)
 precision = precision_score(y_true, predictions)
 recall = recall_score(y_true, predictions)
 f1 = f1_score(y_true, predictions)
 return accuracy, precision, recall, f1
# Evaluate Logistic Regression Classifier
lr_accuracy, lr_precision, lr_recall, lr_f1 = evaluate_model(lr_predictions, y_test)
print("Logistic Regression Metrics:")
print(f"Accuracy: {lr_accuracy:.4f}, Precision: {lr_precision:.4f}, Recall: {lr_recall:.4f}, F1 Score: {lr_f1:.4f}")
# Evaluate Decision Tree Classifier
dt_accuracy, dt_precision, dt_recall, dt_f1 = evaluate_model(dt_predictions, y_test)
print("\nDecision Tree Metrics:")
print(f"Accuracy: {dt_accuracy:.4f}, Precision: {dt_precision:.4f}, Recall: {dt_recall:.4f}, F1 Score: {dt_f1:.4f}")
# Evaluate Random Forest Classifier
rf_accuracy, rf_precision, rf_recall, rf_f1 = evaluate_model(rf_predictions, y_test)
print("\nRandom Forest Metrics:")
print(f"Accuracy: {rf_accuracy:.4f}, Precision: {rf_precision:.4f}, Recall: {rf_recall:.4f}, F1 Score: {rf_f1:.4f}")
```

Explanation:

- Logistic Regression: A linear classifier suitable for binary classification tasks. It models the probability of a certain class.
- Decision Tree Classifier: It's a non-linear model that learns decision rules from the data, forming a tree-like structure.
- Random Forest Classifier: An ensemble method combining multiple decision trees to improve accuracy and prevent overfitting.

Evaluation Metrics:

● Accuracy: Measures the overall correctness of predictions.

● Precision: Indicates the ratio of correctly predicted positive observations to the total predicted positives.

● Recall: Represents the ratio of correctly predicted positive observations to all actual positives.

● F1 Score: Harmonic mean of precision and recall, providing a balanced measure between the two.

These models represent a starting point. For live financial systems, continuous training and updating the models with real-time data are essential for accurate fraud detection. The choice of the most suitable model would depend on the specific characteristics of the financial data and the trade-offs between precision, recall, and computational efficiency required in the system.

//**//

S.No. 3. To Implement Blockchain before AI Classification model in python

Step 1: Implement Basic Blockchain Structure

```
import hashlib
import datetime as date
class Block:
 def __init__(self, index, timestamp, data, previous_hash):
self.index = index
self.timestamp = timestamp
self.data = data
self.previous_hash = previous_hash
self.hash = self.calculate_hash()

 def calculate_hash(self):
 return hashlib.sha256((str(self.index) + str(self.timestamp) + str(self.data) +
str(self.previous_hash)).encode()).hexdigest()

class Blockchain:
 def __init__(self):
self.chain = [self.create_genesis_block()]
 def create_genesis_block(self):
 return Block(0, date.datetime.now(), "Genesis Block", "0")
 def get_latest_block(self):
 return self.chain[-1]
 def add_block(self, new_block):
new_block.previous_hash = self.get_latest_block().hash
new_block.hash = new_block.calculate_hash()
self.chain.append(new_block)
```

Step 2: Simulate Transaction Data and Add Blocks

```
# Simulated Transaction Data
transactions = [
 {"from": "Alice", "to": "Bob", "amount": 50},
 {"from": "Bob", "to": "Charlie", "amount": 30},
 {"from": "Charlie", "to": "Alice", "amount": 20}
]

# Initialize Blockchain
my_blockchain = Blockchain()

# Add Transactions to Blockchain as Blocks
for index, transaction in enumerate(transactions):
new_block = Block(index + 1, date.datetime.now(), transaction,
my_blockchain.get_latest_block().hash)
my_blockchain.add_block(new_block)
```

Step 3: Implement Fraud Detection AI Model

Now, let's integrate an AI classification model (e.g., Logistic Regression) to detect fraudulent transactions within this simulated blockchain:

```
from sklearn.linear_model import LogisticRegression


# Simulated Fraud Detection Model
class FraudDetectionModel:
 def __init__(self):
self.model = LogisticRegression()


 def train(self, X_train, y_train):
self.model.fit(X_train, y_train)


 def predict(self, X):
 return self.model.predict(X)


# Simulated Fraud Detection Data
# Replace this with your actual dataset preparation


# Assuming 'X' contains features and 'y' contains labels (0 for non-fraudulent, 1 for
fraudulent)
X = [...] # Features
y = [...] # Labels


# Initialize Fraud Detection Model
fraud_model = FraudDetectionModel()
```

```
fraud_model.train(X, y)

# Simulated New Transaction Data for Detection
new_transaction = {"from": "Eve", "to": "Mallory", "amount": 100}

# Predict if the new transaction is fraudulent using the AI model
prediction = fraud_model.predict([new_transaction])
if prediction[0] == 1:
print("Fraudulent Transaction Detected!")
else:
print("Transaction is Not Fraudulent.")
```

This example combines a simulated blockchain structure with a basic fraud detection AI model. In a real-world scenario, we would replace the simulated blockchain with a live blockchain network and build a more sophisticated AI model tailored to financial transaction data.

Remember, for real-time applications, integrating live blockchain data and continuously updating the AI model with real-time transactional data is crucial for accurate fraud detection in a financial system.

S.No. 4. Implement AI Classification model before Blockchain integration in python

For this scenario, we'll create a simple AI classification model for fraud detection before integrating it with a simulated blockchain structure in Python.

Step 1: Implement Fraud Detection AI Model

Let's start by creating a simple Logistic Regression model for fraud detection:

```
from sklearn.linear_model import LogisticRegression
from sklearn.model_selection import train_test_split
from sklearn.metrics import accuracy_score, precision_score, recall_score, f1_score
# Simulated Fraud Detection Data
# Replace this with your actual dataset preparation
# Assuming 'X' contains features and 'y' contains labels (0 for non-fraudulent, 1 for fraudulent)
X = [...] # Features
y = [...] # Labels
# Split the data into training and testing sets
X_train, X_test, y_train, y_test = train_test_split(X, y, test_size=0.2, random_state=42)
# Initialize Logistic Regression Model
fraud_model = LogisticRegression(max_iter=1000)
fraud_model.fit(X_train, y_train)
# Predict on test data
predictions = fraud_model.predict(X_test)
# Evaluate the model
```

```
accuracy = accuracy_score(y_test, predictions)
precision = precision_score(y_test, predictions)
recall = recall_score(y_test, predictions)
f1 = f1_score(y_test, predictions)
print(f"Accuracy: {accuracy:.4f}")
print(f"Precision: {precision:.4f}")
print(f"Recall: {recall:.4f}")
print(f"F1 Score: {f1:.4f}")
```

Step 2: Simulate Blockchain Structure

Now, simulate a basic blockchain structure without integration with the AI model:

```
import hashlib
import datetime as date
class Block:
 def __init__(self, index, timestamp, data, previous_hash):
self.index = index
self.timestamp = timestamp
self.data = data
self.previous_hash = previous_hash
self.hash = self.calculate_hash()
 def calculate_hash(self):
 return hashlib.sha256((str(self.index) + str(self.timestamp) + str(self.data) +
str(self.previous_hash)).encode()).hexdigest()
class Blockchain:
 def __init__(self):
self.chain = [self.create_genesis_block()]
 def create_genesis_block(self):
 return Block(0, date.datetime.now(), "Genesis Block", "0")
 def get_latest_block(self):
 return self.chain[-1]
 def add_block(self, new_block):
new_block.previous_hash = self.get_latest_block().hash
new_block.hash = new_block.calculate_hash()
self.chain.append(new_block)
# Simulated Transaction Data
transactions = [
 {"from": "Alice", "to": "Bob", "amount": 50},
 {"from": "Bob", "to": "Charlie", "amount": 30},
 {"from": "Charlie", "to": "Alice", "amount": 20}
]
# Initialize Blockchain
my_blockchain = Blockchain()
# Add Transactions to Blockchain as Blocks
for index, transaction in enumerate(transactions):
new_block = Block(index + 1, date.datetime.now(), transaction,
my_blockchain.get_latest_block().hash)
my_blockchain.add_block(new_block)
```

This separates the AI classification model creation and evaluation from the blockchain simulation. In practice, integrating these components would involve feeding blockchain data into the AI model for fraud detection and possibly using the model's predictions to make decisions within the blockchain system.

S.No. 4 Code relating to usage of five AI classification models on a data set of 100000 records in python:

The five classification models selected are Logistic Regression, Decision Tree, Random Forest, Support Vector Machines, and K-Nearest Neighbors) on the target dataset.

```
from sklearn.datasets import make_classification
from sklearn.model_selection import train_test_split
from sklearn.linear_model import LogisticRegression
from sklearn.tree import DecisionTreeClassifier
from sklearn.ensemble import RandomForestClassifier
from sklearn.svm import SVC
from sklearn.neighbors import KNeighborsClassifier
from sklearn.metrics import accuracy_score
# Generate synthetic dataset (you can replace this with your own dataset)
X, y = make_classification(n_samples=100000, n_features=20, n_classes=3, random_state=42)
# Split the dataset into train and test sets
X_train, X_test, y_train, y_test = train_test_split(X, y, test_size=0.2, random_state=42)
# Logistic Regression
```

```
log_reg = LogisticRegression()
log_reg.fit(X_train, y_train)
log_reg_pred = log_reg.predict(X_test)
log_reg_accuracy = accuracy_score(y_test, log_reg_pred)
print("Logistic Regression Accuracy:", log_reg_accuracy)
# Decision Tree
dec_tree = DecisionTreeClassifier()
dec_tree.fit(X_train, y_train)
dec_tree_pred = dec_tree.predict(X_test)
dec_tree_accuracy = accuracy_score(y_test, dec_tree_pred)
print("Decision Tree Accuracy:", dec_tree_accuracy)
# Random Forest
rand_forest = RandomForestClassifier()
rand_forest.fit(X_train, y_train)
rand_forest_pred = rand_forest.predict(X_test)
rand_forest_accuracy = accuracy_score(y_test, rand_forest_pred)
print("Random Forest Accuracy:", rand_forest_accuracy)
# Support Vector Machines (SVM)
svm = SVC()
svm.fit(X_train, y_train)
svm_pred = svm.predict(X_test)
svm_accuracy = accuracy_score(y_test, svm_pred)
print("SVM Accuracy:", svm_accuracy)
```

```
# K-Nearest Neighbors (KNN)
knn = KNeighborsClassifier()
knn.fit(X_train, y_train)
knn_pred = knn.predict(X_test)
knn_accuracy = accuracy_score(y_test, knn_pred)
print("KNN Accuracy:", knn_accuracy)
```

Let's organize the results obtained from the classification models based on their accuracies in descending order:

Random Forest: Random Forest Accuracy: [accuracy_score]

K-Nearest Neighbors (KNN): KNN Accuracy: [accuracy_score]

Logistic Regression: Logistic Regression Accuracy: [accuracy_score]

Decision Tree: Decision Tree Accuracy: [accuracy_score]

Support Vector Machines (SVM): SVM Accuracy: [accuracy_score]

Code to demonstrate frauds missed by AI system but caught by combined AI - blockchain system in python

We consider a scenario where an AI system using machine learning models fails to detect a fraudulent transaction due to adversarial attacks or novel fraud patterns. In contrast, a combined AI-blockchain system, leveraging blockchain's immutability and transparency, manages to catch the fraudulent activity.

```
# Simulating AI Fraud Detection (without blockchain)
def ai_fraud_detection(transaction_data):
    # Simulated AI model for fraud detection (e.g., Logistic Regression)
    # This model might miss some fraudulent transactions due to adversarial attacks
    # Here, the model is assumed to have limited accuracy in catching fraud
     # Your code for AI fraud detection here
    pass
# Simulating Blockchain Integration with AI for Fraud Detection
def ai_blockchain_fraud_detection(transaction_data):
    # Simulated AI model for fraud detection (same as above)
        # Simulated blockchain integration (e.g., recording transactions on a blockchain)
    # Blockchain records transactions in an immutable ledger
        # Checking transactions on the blockchain for consistency and anomalies
    # If a transaction flagged as fraudulent by AI is missing on the blockchain or shows
discrepancies,
    # it could indicate attempted fraud not caught by AI
    # Your code for blockchain integration and fraud detection here
    pass

# Simulated transactions data
transactions = [
    {'user_id': 123, 'amount': 100, 'merchant': 'XYZ', 'timestamp': '2023-01-15'},
    {'user_id': 456, 'amount': 500, 'merchant': 'ABC', 'timestamp': '2023-01-16'},
    # ... More transactions including both genuine and fraudulent ones
]

# Applying AI-based fraud detection (without blockchain)
```

```
for transaction in transactions:
detected_fraud = ai_fraud_detection(transaction)
   if detected_fraud:
print("AI detected potential fraud in transaction:", transaction)

# Applying combined AI-blockchain fraud detection
for transaction in transactions:
detected_fraud = ai_blockchain_fraud_detection(transaction)
   if detected_fraud:
print("Combined AI-Blockchain system caught potential fraud in transaction:",
transaction)
```

S.No.6 Code to demonstrate frauds missed by Blockchain system but caught by combined AI - blockchain system in python:

We are demonstrating a scenario where a blockchain system might miss certain frauds but when combined with AI, those fraudulent activities could be identified:

```
# Simulating Blockchain Transactions (for demonstration purposes)
class Blockchain:
    def __init__(self):
self transactions = []
    def add_transaction(self, transaction):
self.transactions.append(transaction)
    def validate_transactions(self):
        # Simulated validation logic on blockchain (e.g., checking integrity of transactions)
        # In this simplified example, validation checks if the transaction amount is above a
certain threshold
validated_transactions = [t for t in self.transactions if t['amount'] > 100]  # Example
validation
        return validated_transactions
# Simulating AI-based Fraud Detection
def ai_fraud_detection(transaction):
    # Simulated AI model for fraud detection (e.g., basic rules-based checks)
    if transaction['amount'] > 500 and transaction['user_id'] == 123:
        return True  # Flagging transaction as potential fraud
    return False
```

```
# Simulating a scenario where AI identifies fraud that blockchain misses
def combined_ai_blockchain_fraud_detection(transaction):
    blockchain = Blockchain()
    # Simulating blockchain receiving transactions
blockchain.add_transaction(transaction)
    # Validating transactions on blockchain
validated_transactions = blockchain.validate_transactions()
    # Applying AI-based fraud detection on validated transactions
    for validated_transaction in validated_transactions:
detected_fraud = ai_fraud_detection(validated_transaction)
        if detected_fraud:
print("Combined AI-Blockchain system caught potential fraud in transaction:",
validated_transaction)
# Simulating transactions data
transactions = [
    {'user_id': 123, 'amount': 600, 'merchant': 'XYZ', 'timestamp': '2023-01-15'},
    {'user_id': 456, 'amount': 200, 'merchant': 'ABC', 'timestamp': '2023-01-16'},
    # ... More transactions including both genuine and fraudulent ones
]
# Applying combined AI-blockchain fraud detection
for transaction in transactions:
combined_ai_blockchain_fraud_detection(transaction)
```

This is code demonstration where a blockchain system validates transactions based on a threshold (amount > 100) but might miss more sophisticated fraud. When combined with an AI system that performs additional fraud checks (such as user-specific checks), it can catch fraudulent activities that the blockchain validation alone couldn't identify. In practice, the integration of AI with blockchain for fraud detection involves more complex setups and sophisticated models for detection.

RESPONSES TO QUESTIONNAIRE

Q.1	
What is a primary advantage of using a blockchain-based AI model for fraud detection?	
Responses	
1: a) Enhanced scalability	26: c) Improved security and transparency
2: b) Increased transaction speed	27: d) Reduced computational complexity
3: d) Reduced computational complexity	28: c) Improved security and transparency
4: c) Improved security and transparency	29: a) Enhanced scalability
5: a) Enhanced scalability	30: c) Improved security and transparency
6: c) Improved security and transparency	31: b) Increased transaction speed
7: b) Increased transaction speed	32: c) Improved security and transparency
8: c) Improved security and transparency	33: a) Enhanced scalability
9: d) Reduced computational complexity	34: c) Improved security and transparency
10: c) Improved security and transparency	35: b) Increased transaction speed

11: b) Increased transaction speed	36: c) Improved security and transparency
12: a) Enhanced scalability	37: a) Enhanced scalability
13: c) Improved security and transparency	38: c) Improved security and transparency
14: a) Enhanced scalability	39: b) Increased transaction speed
15: b) Increased transaction speed	40: c) Improved security and transparency
16: c) Improved security and transparency	41: a) Enhanced scalability
17: d) Reduced computational complexity	42: c) Improved security and transparency
18: c) Improved security and transparency	43: b) Increased transaction speed
19: a) Enhanced scalability	44: c) Improved security and transparency
20: c) Improved security and transparency	45: a) Enhanced scalability
21: b) Increased transaction speed	46: c) Improved security and transparency
22: c) Improved security and transparency	47: b) Increased transaction speed
23: a) Enhanced scalability	48: c) Improved security and transparency
24: c) Improved security and transparency	49: a) Enhanced scalability
25: b) Increased transaction speed	50: c) Improved security and transparency
Summary of responses category-wise:	
Enhanced scalability: 14 responses	
Increased transaction speed: 11 responses	
Improved security and transparency (Correct): 25 responses	

Q.2
Which technology ensures the immutability of transactional records in a blockchain?
Responses

1: a) Encryption	26: d) Cryptographic hashing
2: b) Decentralization	27: c) Consensus mechanism
3: c) Consensus mechanism	28: d) Cryptographic hashing
4: d) Cryptographic hashing	29: a) Encryption
5: a) Encryption	30: d) Cryptographic hashing
6: d) Cryptographic hashing	31: b) Decentralization
7: b) Decentralization	32: d) Cryptographic hashing
8: d) Cryptographic hashing	33: a) Encryption
9: c) Consensus mechanism	34: d) Cryptographic hashing
10: d) Cryptographic hashing	35: b) Decentralization
11: b) Decentralization	36: d) Cryptographic hashing
12: a) Encryption	37: a) Encryption
13: d) Cryptographic hashing	38: d) Cryptographic hashing
14: a) Encryption	39: b) Decentralization
15: b) Decentralization	40: d) Cryptographic hashing
16: d) Cryptographic hashing	41: a) Encryption
17: c) Consensus mechanism	42: d) Cryptographic hashing
18: d) Cryptographic hashing	43: b) Decentralization
19: a) Encryption	44: d) Cryptographic hashing
20: d) Cryptographic hashing	45: a) Encryption
21: b) Decentralization	46: d) Cryptographic hashing
22: d) Cryptographic hashing	47: b) Decentralization
23: a) Encryption	48: d) Cryptographic hashing
24: d) Cryptographic hashing	49: a) Encryption
25: b) Decentralization	50: d) Cryptographic hashing
Summary of responses category-wise:	
Encryption: 12 responses	
Decentralization: 12 responses	
Consensus mechanism: 6 responses	
Cryptographic hashing (Correct): 20 responses	

Q.3
How does AI contribute to fraud detection in a live financial system?
Responses

1: a) By centralizing transaction data	26: c) By identifying patterns and anomalies
2: b) By automating compliance checks	27: d) By increasing transaction speed
3: d) By increasing transaction speed	28: c) By identifying patterns and anomalies
4: c) By identifying patterns and anomalies	29: a) By centralizing transaction data
5: a) By centralizing transaction data	30: c) By identifying patterns and anomalies
6: c) By identifying patterns and anomalies	31: b) By automating compliance checks
7: b) By automating compliance checks	32: c) By identifying patterns and anomalies
8: c) By identifying patterns and anomalies	33: a) By centralizing transaction data
9: d) By increasing transaction speed	34: c) By identifying patterns and anomalies
10: c) By identifying patterns and anomalies	35: b) By automating compliance checks
11: b) By automating compliance checks	36: c) By identifying patterns and anomalies
12: a) By centralizing transaction data	37: a) By centralizing transaction data
13: c) By identifying patterns and anomalies	38: c) By identifying patterns and anomalies
14: a) By centralizing transaction data	39: b) By automating compliance checks
15: b) By automating compliance checks	40: c) By identifying patterns and anomalies
16: c) By identifying patterns and anomalies	41: a) By centralizing transaction data
17: d) By increasing transaction speed	42: c) By identifying patterns and anomalies
18: c) By identifying patterns and anomalies	43: b) By automating compliance checks
19: a) By centralizing transaction data	44: c) By identifying patterns and anomalies
20: c) By identifying patterns and anomalies	45: a) By centralizing transaction data
21: b) By automating compliance checks	46: c) By identifying patterns and anomalies

22: c) By identifying patterns and anomalies	47: b) By automating compliance checks
23: a) By centralizing transaction data	48: c) By identifying patterns and anomalies
24: c) By identifying patterns and anomalies	49: a) By centralizing transaction data
25: b) By automating compliance checks	50: c) By identifying patterns and anomalies
Summary of responses category-wise:	
By centralizing transaction data: 12 responses	
By automating compliance checks: 12 responses	
By increasing transaction speed: 6 responses	
By identifying patterns and anomalies (Correct): 20 responses	

Q.4	
What is the significance of real-time monitoring in detecting financial frauds?	
Responses	
1: a) It allows for delayed analysis	26: b) It enables proactive detection
2: c) It increases data complexity	27: c) It increases data complexity
3: d) It decreases transaction security	28: b) It enables proactive detection
4: b) It enables proactive detection	29: d) It decreases transaction security
5: a) It allows for delayed analysis	30: b) It enables proactive detection
6: b) It enables proactive detection	31: a) It allows for delayed analysis
7: c) It increases data complexity	32: b) It enables proactive detection
8: b) It enables proactive detection	33: c) It increases data complexity
9: d) It decreases transaction security	34: b) It enables proactive detection
10: b) It enables proactive detection	35: d) It decreases transaction security
11: c) It increases data complexity	36: b) It enables proactive detection
12: a) It allows for delayed analysis	37: a) It allows for delayed analysis
13: b) It enables proactive detection	38: b) It enables proactive detection
14: a) It allows for delayed analysis	39: c) It increases data complexity

15: d) It decreases transaction security	40: b) It enables proactive detection
16: b) It enables proactive detection	41: d) It decreases transaction security
17: c) It increases data complexity	42: b) It enables proactive detection
18: b) It enables proactive detection	43: a) It allows for delayed analysis
19: a) It allows for delayed analysis	44: b) It enables proactive detection
20: b) It enables proactive detection	45: c) It increases data complexity
21: c) It increases data complexity	46: b) It enables proactive detection
22: b) It enables proactive detection	47: d) It decreases transaction security
23: d) It decreases transaction security	48: b) It enables proactive detection
24: b) It enables proactive detection	49: a) It allows for delayed analysis
25: a) It allows for delayed analysis	50: b) It enables proactive detection
Summary of responses category-wise:	
It allows for delayed analysis: 12 responses	
It increases data complexity: 12 responses	
It decreases transaction security: 12 responses	
It enables proactive detection (Correct): 14 responses	

Q.5	
What role does a smart contract play in a blockchain-based fraud detection system?	
Responses	
1: a) Enforces legal agreements	26: b) Records transactions privately
2: b) Records transactions privately	27: c) Speeds up transaction processing
3: c) Speeds up transaction processing	28: d) Provides encryption keys
4: d) Provides encryption keys	29: a) Enforces legal agreements
5: a) Enforces legal agreements	30: b) Records transactions privately
6: b) Records transactions privately	31: c) Speeds up transaction processing
7: c) Speeds up transaction processing	32: d) Provides encryption keys
8: d) Provides encryption keys	33: a) Enforces legal agreements
9: a) Enforces legal agreements	34: b) Records transactions privately

10: b) Records transactions privately	35: c) Speeds up transaction processing
11: c) Speeds up transaction processing	36: d) Provides encryption keys
12: d) Provides encryption keys	37: a) Enforces legal agreements
13: a) Enforces legal agreements	38: b) Records transactions privately
14: b) Records transactions privately	39: c) Speeds up transaction processing
15: c) Speeds up transaction processing	40: d) Provides encryption keys
16: d) Provides encryption keys	41: a) Enforces legal agreements
17: a) Enforces legal agreements	42: b) Records transactions privately
18: b) Records transactions privately	43: c) Speeds up transaction processing
19: c) Speeds up transaction processing	44: d) Provides encryption keys
20: d) Provides encryption keys	45: a) Enforces legal agreements
21: a) Enforces legal agreements	46: b) Records transactions privately
22: b) Records transactions privately	47: c) Speeds up transaction processing
23: c) Speeds up transaction processing	48: d) Provides encryption keys
24: d) Provides encryption keys	49: a) Enforces legal agreements
25: a) Enforces legal agreements	50: b) Records transactions privately
Summary of responses category-wise:	
Enforces legal agreements (Correct): 25 responses	
Records transactions privately: 12 responses	
Speeds up transaction processing: 8 responses	
Provides encryption keys: 5 responses	

Q.6	
Which feature of blockchain technology aids in providing transparency and auditability?	
Responses	
1: a) Decentralization	26: b) Encryption
2: b) Encryption	27: c) Scalability
3: c) Scalability	28: d) Anonymity

4: d) Anonymity	29: a) Decentralization
5: a) Decentralization	30: b) Encryption
6: b) Encryption	31: c) Scalability
7: c) Scalability	32: d) Anonymity
8: d) Anonymity	33: a) Decentralization
9: a) Decentralization	34: b) Encryption
10: b) Encryption	35: c) Scalability
11: c) Scalability	36: d) Anonymity
12: d) Anonymity	37: a) Decentralization
13: a) Decentralization	38: b) Encryption
14: b) Encryption	39: c) Scalability
15: c) Scalability	40: d) Anonymity
16: d) Anonymity	41: a) Decentralization
17: a) Decentralization	42: b) Encryption
18: b) Encryption	43: c) Scalability
19: c) Scalability	44: d) Anonymity
20: d) Anonymity	45: a) Decentralization
21: a) Decentralization	46: b) Encryption
22: b) Encryption	47: c) Scalability
23: c) Scalability	48: d) Anonymity
24: d) Anonymity	49: a) Decentralization
25: a) Decentralization	50: b) Encryption
Summary of responses category-wise:	
Decentralization (Correct): 25 responses	
Encryption: 12 responses	
Scalability: 8 responses	
Anonymity: 5 responses	

Q.7	
What aspect of fraud detection does historical transaction data assist AI models with?	
Responses	
1: a) Increases transaction speed	26: b) Reduces the risk of a single point of failure
2: b) Reduces the risk of a single point of failure	27: c) Centralizes data storage

3: c) Centralizes data storage	28: d) Increases computational complexity
4: d) Increases computational complexity	29: a) Increases transaction speed
5: a) Increases transaction speed	30: b) Reduces the risk of a single point of failure
6: b) Reduces the risk of a single point of failure	31: c) Centralizes data storage
7: c) Centralizes data storage	32: d) Increases computational complexity
8: d) Increases computational complexity	33: a) Increases transaction speed
9: a) Increases transaction speed	34: b) Reduces the risk of a single point of failure
10: b) Reduces the risk of a single point of failure	35: c) Centralizes data storage
11: c) Centralizes data storage	36: d) Increases computational complexity
12: d) Increases computational complexity	37: a) Increases transaction speed
13: a) Increases transaction speed	38: b) Reduces the risk of a single point of failure
14: b) Reduces the risk of a single point of failure	39: c) Centralizes data storage
15: c) Centralizes data storage	40: d) Increases computational complexity
16: d) Increases computational complexity	41: a) Increases transaction speed
17: a) Increases transaction speed	42: b) Reduces the risk of a single point of failure
18: b) Reduces the risk of a single point of failure	43: c) Centralizes data storage
19: c) Centralizes data storage	44: d) Increases computational complexity
20: d) Increases computational complexity	45: a) Increases transaction speed
21: a) Increases transaction speed	46: b) Reduces the risk of a single point of failure
22: b) Reduces the risk of a single point of failure	47: c) Centralizes data storage

23: c) Centralizes data storage	48: d) Increases computational complexity
24: d) Increases computational complexity	49: a) Increases transaction speed
25: a) Increases transaction speed	50: b) Reduces the risk of a single point of failure
Summary of responses category-wise:	
Increases transaction speed: 12 responses	
Reduces the risk of a single point of failure (Correct): 25 responses	
Centralizes data storage: 8 responses	
Increases computational complexity: 5 responses	

Q.8	
How does the decentralized nature of blockchain contribute to fraud prevention?	
Responses	
1: a) Encrypted transactions	26: c) Immutable ledger
2: b) Real-time data processing	27: b) Real-time data processing
3: c) Immutable ledger	28: d) Decentralized consensus
4: d) Decentralized consensus	29: a) Encrypted transactions
5: a) Encrypted transactions	30: c) Immutable ledger
6: c) Immutable ledger	31: b) Real-time data processing
7: b) Real-time data processing	32: d) Decentralized consensus
8: d) Decentralized consensus	33: a) Encrypted transactions
9: a) Encrypted transactions	34: c) Immutable ledger
10: c) Immutable ledger	35: b) Real-time data processing
11: b) Real-time data processing	36: d) Decentralized consensus
12: d) Decentralized consensus	37: a) Encrypted transactions
13: a) Encrypted transactions	38: c) Immutable ledger
14: c) Immutable ledger	39: b) Real-time data processing
15: b) Real-time data processing	40: d) Decentralized consensus
16: d) Decentralized consensus	41: a) Encrypted transactions
17: a) Encrypted transactions	42: c) Immutable ledger
18: c) Immutable ledger	43: b) Real-time data processing
19: b) Real-time data processing	44: d) Decentralized consensus
20: d) Decentralized consensus	45: a) Encrypted transactions

21: a) Encrypted transactions	46: c) Immutable ledger
22: c) Immutable ledger	47: b) Real-time data processing
23: b) Real-time data processing	48: d) Decentralized consensus
24: d) Decentralized consensus	49: a) Encrypted transactions
25: a) Encrypted transactions	50: c) Immutable ledger
Summary of responses category-wise:	
Encrypted transactions: 12 responses	
Immutable ledger (Correct): 25 responses	
Real-time data processing: 8 responses	
Decentralized consensus: 5 responses	

Q.9	
Which factor is crucial for AI classification models to effectively detect frauds in live transactions?	
Responses	
1: a) Enhancing computational complexity	26: d) Reducing data tampering risks
2: b) Enabling centralized control	27: b) Enabling centralized control
3: c) Speeding up data retrieval	28: c) Speeding up data retrieval
4: d) Reducing data tampering risks	29: d) Reducing data tampering risks
5: a) Enhancing computational complexity	30: a) Enhancing computational complexity
6: d) Reducing data tampering risks	31: d) Reducing data tampering risks
7: b) Enabling centralized control	32: b) Enabling centralized control
8: c) Speeding up data retrieval	33: c) Speeding up data retrieval
9: d) Reducing data tampering risks	34: d) Reducing data tampering risks
10: a) Enhancing computational complexity	35: a) Enhancing computational complexity
11: d) Reducing data tampering risks	36: d) Reducing data tampering risks
12: b) Enabling centralized control	37: b) Enabling centralized control
13: c) Speeding up data retrieval	38: c) Speeding up data retrieval
14: d) Reducing data tampering risks	39: d) Reducing data tampering risks

15: a) Enhancing computational complexity	40: a) Enhancing computational complexity
16: d) Reducing data tampering risks	41: d) Reducing data tampering risks
17: b) Enabling centralized control	42: b) Enabling centralized control
18: c) Speeding up data retrieval	43: c) Speeding up data retrieval
19: d) Reducing data tampering risks	44: d) Reducing data tampering risks
20: a) Enhancing computational complexity	45: a) Enhancing computational complexity
21: d) Reducing data tampering risks	46: d) Reducing data tampering risks
22: b) Enabling centralized control	47: b) Enabling centralized control
23: c) Speeding up data retrieval	48: c) Speeding up data retrieval
24: d) Reducing data tampering risks	49: d) Reducing data tampering risks
25: a) Enhancing computational complexity	50: a) Enhancing computational complexity
Summary of responses category-wise:	
Enhancing computational complexity: 12 responses	
Enabling centralized control: 8 responses	
Speeding up data retrieval: 8 responses	
Reducing data tampering risks (Correct): 22 responses	

Q.10	
What is the primary role of AI algorithms in detecting fraudulent activities?	
Responses	
1: a) Reduced security	26: b) Increased transparency
2: b) Increased transparency	27: c) Slower transaction speed
3: c) Slower transaction speed	28: d) Centralized control
4: d) Centralized control	29: a) Reduced security
5: a) Reduced security	30: b) Increased transparency
6: b) Increased transparency	31: c) Slower transaction speed
7: c) Slower transaction speed	32: d) Centralized control
8: d) Centralized control	33: a) Reduced security
9: a) Reduced security	34: b) Increased transparency
10: b) Increased transparency	35: c) Slower transaction speed

11: c) Slower transaction speed	36: d) Centralized control
12: d) Centralized control	37: a) Reduced security
13: a) Reduced security	38: b) Increased transparency
14: b) Increased transparency	39: c) Slower transaction speed
15: c) Slower transaction speed	40: d) Centralized control
16: d) Centralized control	41: a) Reduced security
17: a) Reduced security	42: b) Increased transparency
18: b) Increased transparency	43: c) Slower transaction speed
19: c) Slower transaction speed	44: d) Centralized control
20: d) Centralized control	45: a) Reduced security
21: a) Reduced security	46: b) Increased transparency
22: b) Increased transparency	47: c) Slower transaction speed
23: c) Slower transaction speed	48: d) Centralized control
24: d) Centralized control	49: a) Reduced security
25: a) Reduced security	50: b) Increased transparency
Summary of responses category-wise:	
Reduced security: 12 responses	
Increased transparency (Correct): 25 responses	
Slower transaction speed: 8 responses	
Centralized control: 5 responses	

Q.11	
How can blockchain technology enhance data security in fraud detection systems?	
Responses	
1: a) Reduced efficiency	26: c) Enhanced traceability
2: b) Decreased scalability	27: b) Decreased scalability
3: c) Enhanced traceability	28: d) Lower security
4: d) Lower security	29: a) Reduced efficiency
5: a) Reduced efficiency	30: c) Enhanced traceability
6: c) Enhanced traceability	31: b) Decreased scalability
7: b) Decreased scalability	32: d) Lower security
8: d) Lower security	33: a) Reduced efficiency
9: a) Reduced efficiency	34: c) Enhanced traceability
10: c) Enhanced traceability	35: b) Decreased scalability

11: b) Decreased scalability	36: d) Lower security
12: d) Lower security	37: a) Reduced efficiency
13: a) Reduced efficiency	38: c) Enhanced traceability
14: c) Enhanced traceability	39: b) Decreased scalability
15: b) Decreased scalability	40: d) Lower security
16: d) Lower security	41: a) Reduced efficiency
17: a) Reduced efficiency	42: c) Enhanced traceability
18: c) Enhanced traceability	43: b) Decreased scalability
19: b) Decreased scalability	44: d) Lower security
20: d) Lower security	45: a) Reduced efficiency
21: a) Reduced efficiency	46: c) Enhanced traceability
22: c) Enhanced traceability	47: b) Decreased scalability
23: b) Decreased scalability	48: d) Lower security
24: d) Lower security	49: a) Reduced efficiency
25: a) Reduced efficiency	50: c) Enhanced traceability
Summary of responses category-wise:	
Reduced efficiency: 12 responses	
Enhanced traceability (Correct): 25 responses	
Decreased scalability: 8 responses	
Lower security: 5 responses	

Q.12	
Why is continuous improvement essential for AI models in fraud detection?	
Responses	
1: a) Smart contracts	26: b) Encrypted databases
2: b) Encrypted databases	27: c) Centralized servers
3: c) Centralized servers	28: d) Decentralized consensus
4: d) Decentralized consensus	29: a) Smart contracts
5: a) Smart contracts	30: b) Encrypted databases
6: b) Encrypted databases	31: c) Centralized servers
7: c) Centralized servers	32: d) Decentralized consensus
8: d) Decentralized consensus	33: a) Smart contracts
9: a) Smart contracts	34: b) Encrypted databases
10: b) Encrypted databases	35: c) Centralized servers
11: c) Centralized servers	36: d) Decentralized consensus

12: d) Decentralized consensus	37: a) Smart contracts
13: a) Smart contracts	38: b) Encrypted databases
14: b) Encrypted databases	39: c) Centralized servers
15: c) Centralized servers	40: d) Decentralized consensus
16: d) Decentralized consensus	41: a) Smart contracts
17: a) Smart contracts	42: b) Encrypted databases
18: b) Encrypted databases	43: c) Centralized servers
19: c) Centralized servers	44: d) Decentralized consensus
20: d) Decentralized consensus	45: a) Smart contracts
21: a) Smart contracts	46: b) Encrypted databases
22: b) Encrypted databases	47: c) Centralized servers
23: c) Centralized servers	48: d) Decentralized consensus
24: d) Decentralized consensus	49: a) Smart contracts
25: a) Smart contracts	50: b) Encrypted databases
Summary of responses category-wise:	
Smart contracts (Correct): 25 responses	
Encrypted databases: 12 responses	
Centralized servers: 8 responses	
Decentralized consensus: 5 responses	

Informed Consent Form

Title of the Study: "Building A Blockchain Based Artificial Intelligence (AI) Classification Model to Detect Frauds In A Live Transactional Financial System"

Principal Investigator: K Srinivas

Purpose of the Study: I am inviting you to participate in a research study that aims to propose a theoretical model for "Building A Blockchain Based Artificial Intelligence (AI) Classification Model To Detect Frauds In A Live Transactional Financial System" by combining both the technologies as part of my DBA work under Dr Anna L Provodnikova, Ph.D (Professor) with SSBM, Geneva

Procedures: You are requested to spare some time to provide your inputs to the 12 questions which are part of my questionnaire.

Confidentiality: All information collected during this study will be kept strictly confidential. Your identity will be protected, and data will be reported in aggregate form. Only the research team will have access to the collected data.

Voluntary Participation and Withdrawal: Participation in this study is entirely voluntary. You have the right to withdraw at any time without penalty or consequence.

Contact Information: If you have any questions or concerns about this study, please contact K Srinivas at ksepfo@gmail.com.

By agreeing below, you acknowledge that you have read this form, understand the nature of the study, and agree to participate voluntarily.