Understanding the Security and Privacy Risks in Healthcare and Insurance Records Management

Ms. Jaspreet Kaur
Research Scholar
University Institute of Computing
Chandigarh University,Punjab

Dr.Gagandeep Chawla
Associate Professor
University Institute of Computing
Chandigarh University,Punjab

***Abstract*-Globally, healthcare fraud is a major problem that affects patient confidence, healthcare organizations, and financial stability. Specifically in insurance claims, billing, and medical reporting, the healthcare sector is confronted with formidable obstacles in its fight against fraud. The inability of TFD (Traditional Fraud Detection) techniques to identify complex fraudulent activity frequently results in significant financial losses and impaired health care.Thisstudy applies blockchain technology to improve fraud detection and prevention in the healthcare sector.This study will suggest a NFDS (Novel Fraud Detection Strategy) to spot healthcare fraud by utilizing the concept of Block Chain Technology as the Block Chain has properties of immutability and transparency in conjunction with data analytics integration. Through a detailed analysis of the literature of recent research, case studies, and examples, the report explains the benefits and challenges of using block chain-powered NFDS. Important areas of focus include developing new algorithms, applying data analytics techniques, and integrating block chain technology into the healthcare system. In addition to evaluating how well different fraud detection algorithms and models perform in identifying fraudulent activity in insurance claims, billing procedures, and medical reports, the study will also examine the integration of block chain technology to enhance auditability, security, and data integrity. This study also emphasizes how smart contracts may automate fraud detection procedures, minimize human participation, and guarantee real-time transaction verification. The study investigates the ways in which decentralized identity management can improve patient data security while upholding legal requirements. The results will ultimately support continued efforts to improve privacy and security in the administration of medical and insurance records.**

***Keywords:*Block Chain-Powered Model, Fraud Detection Algorithms, Fraudulent Activity, NFDS,TFD.**

1. INTRODUCTION

In 2008, a single or anonymous group of researchers going by the name of Satoshi Nakamoto created blockchain technology. It was presented as a long-term fix for the double spending issue. Block chain technology has expanded across a wide range of industries, including manufacturing, insurance coverage, energy, health care, educational institutions, technology, Internet of Things, the farming industry, social media, and entertainment, after getting significant interest in the financial sector. Block chain technology is used to provide reliability, effectiveness, anonymity, immutability, ownership, ease of auditability, and other benefits in businesses that may not utilize cryptocurrency[1]. Due to the increase in fraudulent activities, which threaten patient safety and confidence in addition to causing significant financial losses, fraud detection and prevention have taken on a critical importance in the healthcare sector.

Healthcare fraud is a worldwide issue that affects both industrialized and underdeveloped nations. It is particularly harmful to people who get high-quality medical care, particularly those who have health insurance [2][3].The 2015 study on the financial effect of healthcare fraud found that a total of roughly £303.8 million was lost as a result of healthcare fraud. [4]. The £22.9 million for optical charge fraud, the £43.9 million for dental charge fraud, and the £237 million for prescription charge fraud are the three distinct categories for this sum. Similarly, healthcare fraud is predicted to cost Europe and Korea, respectively, €56 billion and 798.2 billion annually, according to Thaifur et al. [5]. Government-sponsored health insurance programs in Africa assist the impoverished by shielding them from having to pay cash for medical services and prescription drug purchases. There is enough proof in the literature to conclude that health insurance systems in Africa are fraudulent. For example, based on the clinical audit report and claim intelligence data gathered, GenKey SOLUTIONS, B.V. estimates that fraud wastes 15% to 20% of healthcare spending[6]. This translates to an estimated $487 billion in fraud losses every year. The monthly medical assistance contributions that participants in South Africa's national health insurance program pay rise from R192 ($14) to R410 ($30) as a result of fraud. The expected sum of these minor healthcare cost overruns is $882 million. Numerous scholars have put out numerous suggestions to address this problem as discussed in Amponsah et al. [2]. The authors proposed an efficient block chain-based data management system and a claims processing system that ensures service

providers are paid on time. Our research includes a module that forecasts and detects fraud in the claims processing system using Blockchain Technology (BC).Stakeholders may utilize block chain technology to develop secure, transparent mechanisms for documenting and approving medical transactions. This reduces the possibility of fraud and guarantees the accuracy of medical data.

According to the report, health insurance companies should employ block chain technology to record medical services provided, legitimate claims that have been settled, and other claim-related data. Proposal of developing cutting-edge algorithms and using data analytics approaches, this paper seeks to investigate the novel uses of blockchain in healthcare fraud detection and prevention. Through an analysis of the convergence of blockchain technology, algorithm development, and data analytics, our goal is to clarify the possible advantages and obstacles associated with using blockchain-driven solutions in the fight against healthcare fraud. This study will show how blockchain technology might improve the effectiveness, precision, and dependability of fraud detection systems in the healthcare industry by a thorough analysis of the body of existing research, case studies, and examples. The benefits of blockchain-powered fraud detection for bettering patient outcomes, lessening the financial strain on healthcare institutions, and promoting increased trust and openness within the healthcare ecosystem will also be covered. This endeavour's primary objective is to prevent resentful and dishonest actors who exist throughout the NHIS claim handling lifecycle from implementing their fraudulent schemes. In addition, it will protect the coverage plan from financial losses caused by manipulating the inefficiencies in the lifetime of claims processing.

I. **Block Chain Technology:** Blockchain is a decentralized, distributed, transparent, immutable, publically verifiable, and genuine technology for managing data and capturing transaction histories [22]. Despite being new, blockchain mostly depends on already-existing technology to offer immutability, secrecy, privacy, and security. These technologies include cryptographic algorithms, consensus processes, distributed ledgers, Merkle trees, and certificates [23]. In 2008, Blockchain (BC) surfaced as a financial application [24], driven by the success of Bitcoin and Ethereum. Rather of keeping every record on a single, weak server, it is dispersed among several PCs throughout the globe. Distributed ledger technology improves privacy controls over sensitive medical data, such as electronic health records (EHRs), and removes single points of failure. Thus, by increasing security, transparency, and efficiency, blockchain technology can enhance healthcare.

II. **Types of Block Chain Technology:** Blockchain technology comes in two primary flavors: permission less and permissioned. Permission less block chains, also known as trustless or public block chains, are open networks where anybody may take part in the consensus process that the blockchain uses to validate transactions and data, according to Helliar et al. [25]. Dispersed among unidentified parties, they are totally decentralized. With a few exceptions, players in permission less blockchain systems remain anonymous at all times, transactional transparency is ensured by open source development, and there is no central regulatory authority. A major component of public blockchain is rewarding users with tokens and other digital assets. Ethereum and Bitcoin are two instances of permission less blockchain platforms[26]. Permissioned block chains, often referred to as private block chains or permissioned sandboxes, are closed networks in which members of a consortium or other previously specified parties interact and take part in consensus-building and data validation. While they are conceivable, tokens and digital assets are not as common as they are in systems without authorization. Hyper ledger Fabric, Corda, Multichain, and other block chains are examples of private block chains [26].The suggested improved NHIS claims procedure is shown in the sequence diagram in Fig. 3 below. To submit claims, the supplier completes the blockchain-based form. Subsequently, the patient who is claiming costs takes over control and verifies the information provided by the provider. The Director/National Scheme thereafter handles administrative duties and audits.

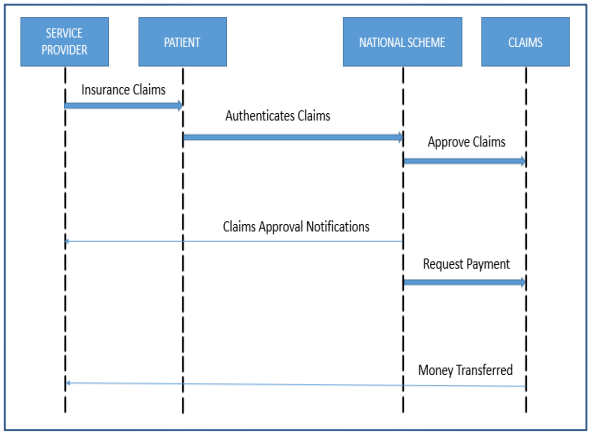

Fig 1. The Sequence Diagram for the Blockchain based system

In addition to initiating or requesting provider reimbursement, participants in the director role can authenticate and approve claims that have been submitted. After the claims are accepted by the director, funds must be transferred by the finance office via the bank into the provider's account. Since the fulfilment officer is only involved in manual claim submission, they are removed from the chain of events. The Director and the Vetting Officer/Supervisor/Accountant entities have combined in order to streamline the claims process's communication channel.

2. BACKGROUND

Worldwide, healthcare fraud is still a major problem that affects patients and healthcare institutions alike. The national health insurance program in South Africa has a significant problem due to the high incidence of fraudulent activities, which can result in negative outcomes including financial losses and poor healthcare delivery. According to a research conducted by The South African Medical Association (SAMA), kickbacks, phantom billing, and charging for services not delivered are examples of fraudulent activities that drive up the expense of healthcare in the nation [7].

Following the enormous success of bitcoin, Interest in block chain technology has grown among scientists and business people. Maintaining transaction records in an anonymous, decentralized, immutable, transparent, and accessible manner is the primary goal of block chain technology. [8]. Each block has a link to the block before it, and the first block is known as the genesis block. [9]. Block chain's special qualities have allowed it to address many of the shortcomings of conventional systems. Blockchain-based solutions create very reliable and safe channels for trade and business instances such as funding venture capital, insurance, and investment transactions [10].Roriz and Pereira, for example, developed a block chain-based defense against auto insurance fraud, which includes the practice of "double-dipping," or holding multiple policies for the same vehicle. [11]. In addition to the financial industry, other industries that have made extensive use of this technology include supply chain management, healthcare, education, and process automation [12][15].

The sectors where block chain applications show the most potential include financial services, public administration, health care, and real estate. [16]. As a result, insurance must be included in this chain as a risk transfer tool to facilitate easier transactions between organizations, the general public, and insurance undertakings.

The observation made in this paper that how patients and physicians behave when it comes to health insurance fraud, accounting for bribery from patients, insurance institution fines and incentives, and moral hazard from physicians and patients. Some fraud behaviours between physicians and patients are mentioned in order to illustrate the behaviour mechanism and make the issue more clear.

Creating cutting-edge algorithms specifically for the healthcare industry is essential to successfully identifying and stopping fraudulent activity. These algorithms can evaluate vast amounts of healthcare data and spot patterns suggestive of fraud by utilizing machine learning, artificial intelligence, and other cutting-edge analytical techniques.

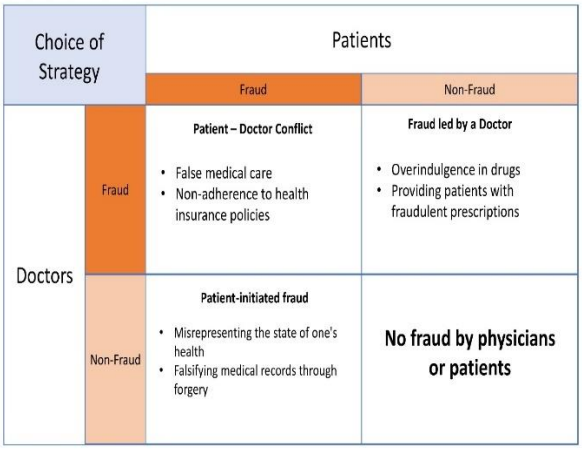

Fig 2. Doctors Patients healthcare Frauds Types.

Fig 2 illustrates that Real-world instances of health insurance fraud fall into three categories: doctor-patient collaboration, patient-led, and patient-led. [17]. These types of fraud are based on the actions of both doctors and patients. Patient-led fraud happens when patients select fraudulent conduct while doctors select non-fraudulent behaviour. Forging and falsifying medical documents, as well as inflating medical problems, are examples of this type of fraud. Fraud guided by doctors occurs when they select dishonest behaviour while the patients opt for honest activity. In these situations, physicians will overprescribe medications and pressure patients to overpay for them. Furthermore, there will be doctor-patient collaboration if both the patients and the physicians decide to engage in fraudulent activity. In order to combat healthcare fraud, patients and physicians will come to an agreement in this method. For instance, physicians and patients may choose to arbitrage medical insurance fees by using fraudulent information to circumvent restrictions governing medical insurance. To get additional health insurance, physicians may treat patients fraudulently and write fictitious prescriptions. Currently, doctors and patients stand to gain

the most from their perspective, in contrast to patient-led and physician-led healthcare fraud.Schemes for health care fraud are as diverse as people's imaginations. The results will ultimately support continued efforts to improve privacy and security in the administration of medical and insurance records. Below are four categories of health care thefts to help you better grasp the fraud threats.

Provider Frauds: All of the frauds included in this category include the provider or a fake provider committing the fraud against a third-party payer, such Medicare, private insurance, or government or private foundations that support health care research. The majority of provider frauds fall under the category of "False Claim Schemes," for which the Federal False Claims Act permits redress. Any invoicing of health insurers for services or procedures that were either not performed or unnecessary and done with the intention of wrongfully earning financial gain is considered a false claim scheme.

Fraud in Quality Data Reporting:A growing area of concern is quality data reporting fraud. Fraud can be committed by failing to provide care or by providing medically unneeded services. When medically inappropriate procedures are carried out, the patient faces needless risks to their health and the individuals who pay are charged for unwarranted expenses. The Centres for Medicare and Medicaid Services (CMS), the Joint Commission, physician quality reporting data, hospital quality data for annual payment updates, medical error and "sentinel event" data, and quality reporting mandated by state law all provide information about these occurrences. The financial component of this kind of fraud stems from the provider's motivation, which comes from an indirect financial interest. Provider and data reporting fraud components are combined in the following types of fraud:

(1) Falsified clinical trial data, drug test results, and research fraud
(2) Despite not having the requisite licensing or certification, unlicensed/uncertified carefacilities and unlicensed physicians offer appropriate services and bill appropriately.

Consumer Fraud: Apart from healthcare providers, individuals also perpetrate frauds against providers and insurers, which often have a lower financial impact than billing or quality frauds. One type of consumer fraud is when someone uses dishonest methods to get health care services for which they are not qualified. Among the instances are: 1) falsely claiming insurance eligibility for dependents; 2) changing prescriptions to get more painkillers or other restricted substances than called for; and 3) obtaining medical care by using a fake or pilfered insurance card.

Fraud in General Business -Physicians and hospitals need to be mindful of the same non-health related scams that affect all businesses, such as those committed against them by staff members, vendors, or contractors. The same kinds of frauds that target any other business can also target health care providers. A few instances are duplicate billings for the same delivery, check kiting, ghost employees in the payroll system, theft of cash co-payments, fake supplier bills for inaccurate quantities, and billing from shell business suppliers.

3. Brief Review of Available Studies

Healthcare fraud can in a variety of forms. Some of the more prevalent types of fraud are conventional schemes executed by shell vendors, ghost workers who obtained access to bill payers, and employees who continue to charge after their licenses expire. [18][19]. Some of the main actors involved in or committing fraud are manufacturers of medical equipment, pharmaceutical companies, organizations licensed to provide specialized services like home healthcare, beneficiaries (those who receive medical or related services), and providers (those who are authorized to provide services to beneficiaries)..

The percentages of incorrect payments in US government programs run by the Health and Human Services (HHS) are shown in Figure 3 for the years 2017 through 2023. Any form of fraud, underpayment, overpayment, or unknown payment are examples of such incorrect payments. The Children's Health Insurance Program (CHIP), Medicaid, Medicare Fee-For-Service (FFS), are the HHS agency programs that are listed in the original data [20] as government healthcare programs Medicare Fee-For-Service (FFS), and the Children's Health Insurance Program (CHIP).

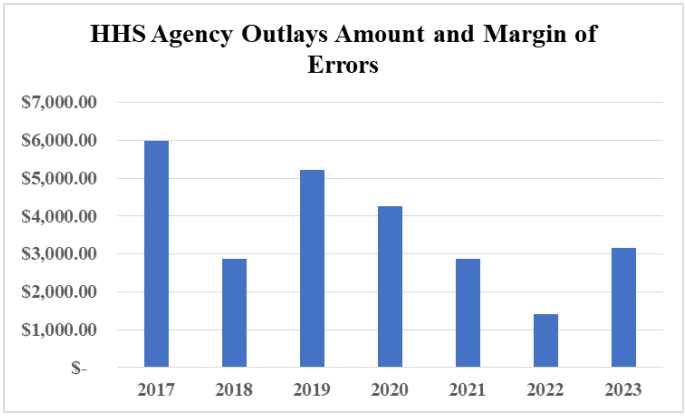

Fig 3 HHS Agency Outlays Amount and Margin of Errors

The rate of inappropriate payments for the HHS agency has typically increased steadily, as shown in Figure 3[21].

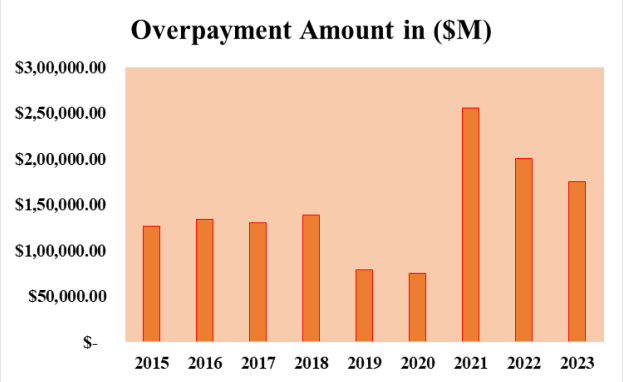

Fig 4Overpayment Amount by Agencies

The agency Health and Human Services (HHS) Federal Financial System (FFS) overpayments in 2023 that were not under the agency's control are displayed in this graph. The single bar shows the $27.5 million in financial terms that are attributed to "Failure to Access Data/Information Needed." The agency's inability to acquire or get the data or information essential for correct payment processing and validation is most likely the reason for this large overpayment. The following graph illustrates a significant problem with the agency's financial operations: difficulties with data accessibility resulted in significant overpayments in the fiscal year 2023.

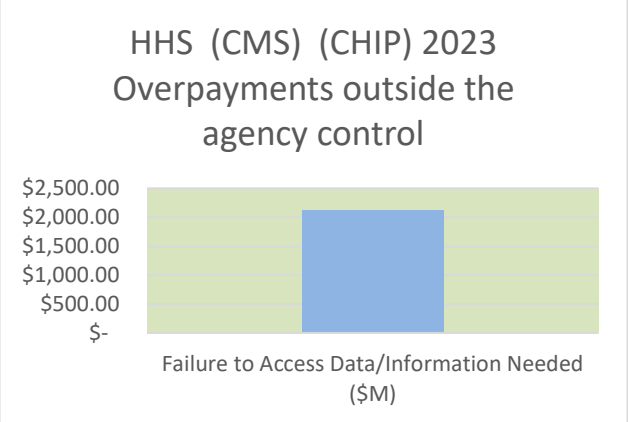

Fig 5 CHIP Failure to Access data/Information need

This graph displays the excess payments made by the Centers for Medicare & Medicaid Services (CMS) in 2023 that were not beyond the agency's control, specifically in the Children's Health Insurance Program (CHIP). A $2,071 million overcharge is shown by the single bar, which is attributed to "Failure to Access Data/Information Needed." Because the agency was unable to acquire or get the necessary data or information for effective payment processing and validation inside the CHIP program, there was a significant overpayment. The graph illustrates a major problem with data accessibility that CMS faced during the 2023 fiscal year, which resulted in large overpayments in the CHIP program.

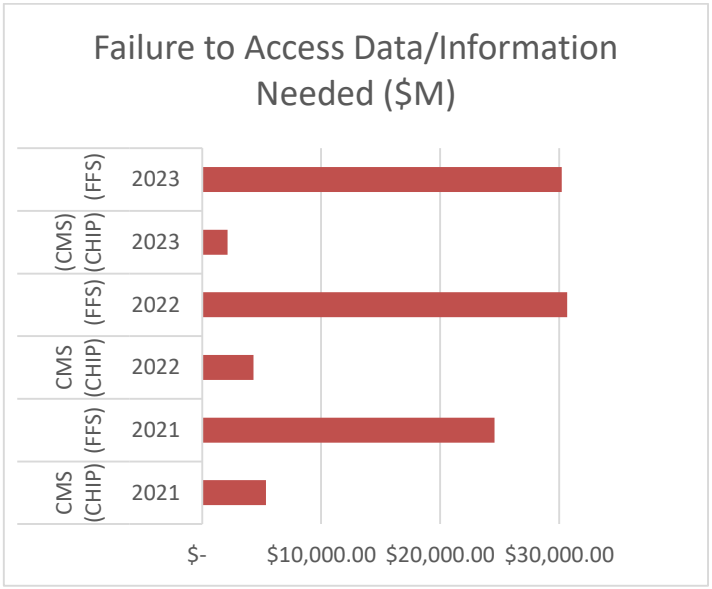

Fig6Comparison Failure to Access data/Information need

In this graph, the Federal Financial System (FFS) and the Centers for Medicare & Medicaid Services Children's Health Insurance Program (CMS CHIP), two Department of Health and Human Services (HHS) programs, are compared for "Failure to Access Data/Information Needed" overpayment amounts over time. The overpayment amount for FFS in 2023 was $27.5 million, a dramatic decrease from the much larger $2,071 million for CMS CHIP. This suggests that data access for the CHIP program was a far bigger problem that year. Nevertheless, in 2022, the pattern was reversed when FFS overpaid by approximately $17.5 million, while CMS CHIP only overpaid by around $4.5 million.

About $15 million for FFS and $2 million for CMS CHIP were overpaid in 2021, which was a comparable but smaller sum for both programs. The recurring problem of data access problems resulting in significant overpayments is seen across both FFS and CMS CHIP, even while the overpayment amounts between the two programs varied over time, with one program routinely outpacing the other in a given year. Overall, our comparison shows that in order to reduce these expensive overpayments in its key programs, HHS must enhance its information management and data access procedures.

4. Conclusions

With an emphasis on health insurance fraud and billing fraud specifically, this research has examined how blockchain technology may transform fraud detection and

prevention in the healthcare industry. Globally, healthcare fraud presents serious problems as it damages faith in healthcare institutions and causes financial losses. Utilizing cutting-edge algorithms, blockchain technology, and data analytics integration presents a potential chance to successfully address these issues. The intrinsic properties of blockchain, including immutability, transparency, and decentralization, provide a safe and impenetrable framework for documenting and verifying medical transactions. In this study, the potential advantages of blockchain-powered fraud detection systems in healthcare have been illustrated.The advantages of this approach encompass enhanced precision, efficacy, and dependability in detecting fraudulent activities, resulting in superior patient outcomes, diminished financial burden on healthcare establishments, and heightened trust throughout the healthcare network.

5. Future Scope

It is crucial to carry out more study into the creation of sophisticated algorithms and data analytics methods for fraud detection. Future studies should concentrate on improving the security and privacy components of healthcare systems that use blockchain technology.This study shows how blockchain technology improves insurance and healthcare organizations' ability to detect and prevent fraud. This entails investigating methods to safeguard private patient data while maintaining data integrity, such as decentralized identity management.

References

[1] Amponsah, A. A., Adebayo, F. A., & WEYORI, B. A. (2021). Blockchain in insurance: Exploratory analysis of prospects and threats. International Journal of Advanced Computer Science and Applications, 12(1).

[2] Amponsah, A. A., Adekoya, A. F., &Weyori, B. A. (2022). Improving the financial security of national health insurance using cloud-based blockchain technology application. International Journal of Information Management Data Insights, 2(1), 100081.

[3] Kirlidog, M., &Asuk, C. (2012). A fraud detection approach with data mining in health insurance. Procedia-Social and Behavioral Sciences, 62, 989-994.

[4] Button, M., Gee, J., & Brooks, G. (2011). Measuring the cost of fraud: an opportunity for the new competitive advantage. Journal of Financial Crime, 19(1), 65-75.

[5]Thaifur, A. Y. B. R., Maidin, M. A., Sidin, A. I., &Razak, A. (2021). How to detect healthcare fraud?"A systematic review". Gaceta sanitaria, 35, S441-S449.

[6] Mishra, A., Kokare, A., &Bhoite, S. (2025). Blockchain in Insurance: Enhancing Claims Processing, Fraud Prevention, and Risk Management.

[7] Meyer, L. (2024). Physiotherapists' Experiences of Forensic Audits by South African Medical Funding Schemes (Master's thesis, University of Pretoria (South Africa)).

[8] Nofer, M., Gomber, P., Hinz, O., &Schiereck, D. (2017). Blockchain. Business & information systems engineering, 59, 183-187.

[9] Haque, A. B., Islam, A. N., Hyrynsalmi, S., Naqvi, B., &Smolander, K. (2021). GDPR compliant blockchains–a systematic literature review. Ieee Access, 9, 50593-50606.

[10] Banerjee, S. S., &Chandani, A. (2022). Challenges of blockchain application in the financial sector: a qualitative study. Journal of Economic and Administrative Sciences.

[11]Roriz, R., & Pereira, J. L. (2019). Avoiding insurance fraud: A blockchain-based solution for the vehicle sector. Procedia Computer Science, 164, 211-218.

[12] Queiroz, M. M., Telles, R., & Bonilla, S. H. (2020). Blockchain and supply chain management integration: a systematic review of the literature. Supply chain management: An international journal, 25(2), 241-254.

[13] McGhin, T., Choo, K. K. R., Liu, C. Z., & He, D. (2019). Blockchain in healthcare applications: Research challenges and opportunities. Journal of network and computer applications, 135, 62-75.

[14] Bhaskar, P., Tiwari, C. K., & Joshi, A. (2021). Blockchain in education management: present and future applications. Interactive Technology and Smart Education, 18(1), 1-17.

[15] SobreiraLeite, G., Bessa Albuquerque, A., &RogerioPinheiro, P. (2020). Process automation and blockchain in intelligence and investigation units: an approach. Applied Sciences, 10(11), 3677.

[16] Johnson, G. L. (2017). Planning the future: blockchain Technology and the Insurance Industry. House Defense Quarterly, 73, 73-78.

[17] Liu, J., Wang, Y., & Yu, J. (2023). A study on the path of governance in health insurance fraud considering moral hazard. Frontiers in Public Health, 11, 1199912.

[18] Ahadiat, N., &Gomaa, M. (2018). Healthcare Fraud and Abuse: An Investigation of the Nature and Most Common Schemes. Journal of Forensic and Investigative Accounting, 10(3), 428-435.

[19] Ahadiat, N., &Gomaa, M. (2018). Healthcare Fraud and Abuse: An Investigation of the Nature and Most Common Schemes. Journal of Forensic and Investigative Accounting, 10(3), 428-435.

[20] Payment Accuracy Dataset downloads, Annual Improper Payments Datasets - Payment Accuracy 2020 Dataset. 2020 https://www.paymentaccuracy.gov/payment-accuracy-the-numbers/. Downloaded on July 26, 2021. [Google Scholar] [Ref list].

[21] Kumaraswamy, N., Markey, M. K., Barner, J. C., &Rascati, K. (2022). Feature engineering to detect fraud using healthcare claims data. Expert Systems with Applications, 210, 118433.
[22] Kamboj, D., & Yang, T. A. (2018). An exploratory analysis of blockchain: applications, security, and related issues. In Proceedings of the International Conference on Scientific Computing (CSC) (pp. 67-73). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).
[23] Ogiela, M. R., &Majcher, M. (2018, May). Security of distributed ledger solutions based on blockchain technologies. In 2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA) (pp. 1089-1095). IEEE.
[24] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.
[25] Helliar, C. V., Crawford, L., Rocca, L., Teodori, C., &Veneziani, M. (2020). Permissionless and permissioned blockchain diffusion. International Journal of Information Management, 54, 102136.
[26] De Angelis, S., Aniello, L., Baldoni, R., Lombardi, F., Margheri, A., &Sassone, V. (2018). PBFT vs proof-of-authority: Applying the CAP theorem to permissioned blockchain. In CEUR workshop proceedings (Vol. 2058). CEUR-WS.
[27] Leap, T. L. (2011). Phantom billing, fake prescriptions, and the high cost of medicine: Health care fraud and what to do about it (p. 256). Cornell University Press.