Fraud Detection: A Review on Blockchain

Anuska Rakshit[1], Shriya Kumar[2], Ramanathan L [3]

[3]Professor at Vellore Institute of Technology, Vellore
[1-2]Vellore Institute of Technology, Vellore

Abstract - *A blockchain is a distributed database of records, commonly known as a public book, of all completed transactions or digital events that may be shared between participants. Most program participants double check each activity in the community manual. Once the data is entered, it will never be erased. Keeping track of what is being done permanently, implicitly, and irrevocably, can help prevent many types of information fraud. Fraudulent transactions cannot surpass accumulated guarantees and guarantees as each transaction must be made by a group of miners. With moderate data storage and administrative systems, hacking, hacking, and breach are all possible, but the widespread blockchain compliance mechanism prevents this. Any asset, goods, or service may be directed. Identity theft, fraud, and network or system failure. On the Internet, malicious behavior includes identity theft, fraud, and network or system intrusion. Blockchain-based trading has to deal with challenges such as online fraud, identity theft, and fraud. We will examine how blockchain technology works in detecting fraud in this study. While there are many more types of information fraud, we will focus on a few of the most common ones in this study, such as rating fraud, insurance fraud, employment history fraud, fraudulent acquisition fraud, and various other fraudulent scams. our industries.*

Key Words: Fraud, Blockchain supported, Detection, Consensus, Intrusions

1.INTRODUCTION

In recent years, blockchain technology has attracted a lot of attention. A number of measures have been proposed and implemented to detect fraudulent transactions and activities that deviate from normal patterns of activity. Outlier analysis approaches include guided classifications like decision trees, support vector machines, evolutionary algorithms, Bayesian belief networks, and neural networks. Despite the fact that previous research has substantially improved the accuracy of information fraud detection, only a few models are capable of accurately detecting all fraudulent situations. Even if the deception is exposed and the sources of input are properly identified, we may still be unable to access the truth and make informed decisions. Maintaining security, correctness, reliability, and transparency among the market's participating parties is crucial in a world where everything is done digitally. This research looks at a variety of fraud detection systems that are presently in use around the world and have proven to be effective in combatting swindling. We've looked at ten various areas where blockchain technology has made an impact, and we've come up with practical solutions to the problems that people encounter on a daily basis.

2. PROPOSED ANALYSES

2.1 Blockchain for Fraud Detection: Work-History Prevention System

A vast number of documents must be submitted as part of the current job application process. Verifying an applicant's work history is a vital stage in the recruiting process because it verifies that the individual is qualified for the job. This paper uses blockchain to improve work history verification. Blockchain is used to preserve encrypted versions of work history as a way of data authentication. This technology will also allow potential employees to bundle many records and present them to employers, who will be able to authenticate each record against the blockchain version while respecting the privacy of both parties. Although it should be impossible to edit a work history record after it has been produced, mistakes may happen, such as when data is entered incorrectly.

2.2 Fraud Detections for Online Businesses

On the internet, interactions with anonymous people can be risky. As a result, in the cyber world, it is preferable to use reputation systems to assess a potential seller's trustworthiness ahead of time, allowing customers to assess the quality of unknown suppliers. Reputation management systems collect, integrate, and publish information about an entity's previous actions. Despite their efficacy, they are prone to rating fraud, which occurs when raters profit from giving skewed evaluations. It proposes a preventive technique against subjective information fraud to assist prevent rating fraud. While blockchain systems can avoid some sorts of rating fraud, such as badmouthing and whitewashing, they may not be able to eliminate ballot stuffing. Using blockchain-based technologies, sybil, continuous, and disguise assaults can all be prevented. As a result, blockchain systems can prevent bogus decisions by anonymous individuals utilising genuine identities. As a result, no illegal ratings will be distributed, and a legitimate buyer-vendor relationship can be established.

2.3 The Influence of Blockchain Detection on Fraud and Fake Prevention

Blockchain is one of the most well-known new technical trends, with applications in both financial and non-financial activities. People are cautious of media reporting and news commercials because we live in a distrustful atmosphere. This article focuses on reducing revenue losses as a result of fraud attacks and fraudulent activity, as well as securing finance and supply chain business processes. By adopting a shared digital ledger in which the visibility and transparency of transactions can be raised among the members of a business network, blockchain technology aids to the reduction of fraud crime. Blockchain technology benefits food trust, diamond commerce, the vehicle supply chain, and online voting. As a result, Blockchain technology can help businesses reduce fraud while also enhancing employee morale.

2.4 Are Blockchains Immune to all Malicious Attacks?

The data management capabilities and functionality of a repository determine the integrity of any data. In contrast to this centralized system, a blockchain uses a peer-to-peer network to register and store transactions. Every network node stores a copy of the blockchain. Cyberspace is a perfect setting for deceit and fraud because of its low entry barriers, user anonymity, and spatial and temporal separation between users. Potential dangers such as a 51 percent attack, identity theft, system hacking, and more can be mitigated using blockchain techniques. Because transactions on a blockchain are anonymous and irrevocable, it is a highly effective tool for preventing fraud.

2.5 A Blockchain-Based Framework for Fraud Detection

This model includes the following four major entities/layers: 1) The Federal Government in General 2) The Administration of the State 3) Municipal Government 4) Additional Departments and Sub-Departments

The proposed architecture is Ethereum blockchain compatible. Central authorities will deploy smart contracts (schemes), and other entities will only be able to update existing smart contracts. As a result, only data updates will be used to carry out transactions.

2.6 Counterfeit Detection of Documents using Blockchain

This paradigm incorporates the following four major entities/layers: 1) The National Government 2) Administration of the State 3) Municipalities 4) Sub-Departments that aren't listed above.

The framework that has been proposed is Ethereum-compatible. Central authority will deploy smart contracts (schemes), and other entities will only be able to amend smart contracts that have already been published. As a result, only data updates will be used for transactions.

2.7 A Multifaceted Approach to Bitcoin Fraud Detection: Global and Local Outliers

Outliers are divided into two categories: global outliers and local outliers. In this study, global outliers are examples that are farther apart from the centroids in terms of Euclidean distance, as determined by the use of trimmed k-means. The top 1% of occurrences based on kd and trimmed k-means will be labelled as anomalies, while the rest will be categorized as normal. In this way, the two algorithms act as proxies for normality and abnormality, allowing supervised learning techniques to be used for assessment.

2.8 Video Fraud Detection using Blockchain

A workable prototype of a rudimentary Blockchain system for detecting video fraud has been constructed as part of the proposed study. Our graphical User Interface was built with Java and MySQL (GUI). Finally, in our study, nodes are captured on a network. Some of the users are represented by the nodes in this network. A video will be transferred from one node to the next, and the video's hash will be kept on all nodes. Because each movie has its own hash, as previously stated, a node will distribute one film to other users, each of whom will keep a hash of it. If a node tries to tamper with the video later, the hash will be modified, and the other nodes will get a different hash when that node uploads the same video, signaling that fraud has occurred and the video has been tampered with. As a result, the solution is found in this manner.

2.9 Avoiding Insurance Fraud: A blockchain-based Solution for the Vehicle Sector

The insurance industry is a massive economic sector with several complex business activities and vast amounts of operational data. Unfortunately, insurance companies confront more issues than just carrying out their responsibilities and storing information about insured automobiles. Fraud is another significant problem that costs them a lot of money, and some fraud scenarios are difficult to avoid without the assistance of insurance carriers. The proposed solution is for all insurance companies to have access to the data, however there are a few difficulties. A client-server design incorporating blockchain technology can address these issues. It aids in the connection of every node in the network to another node, resulting in a decentralized, non-nuclear system. Second, the issue of security is solved when blockchain is used.

2.10 Avoiding Insurance Fraud: A Blockchain-based Solution for the Vehicle Sector

The first challenge can be solved by creating a blockchain-based application in which each node is connected to every other node via the network. The second challenge, data security, is also solved by taking into consideration the blockchain's intrinsic qualities of data durability and immutability, as well as the consensus procedures utilized to store new data. The data used in the fraud prevention insurance support system that we propose is available to all insurance firms. Every organization that participates in this solution receives a copy of the data and code stored in the blockchain. There is no longer a single point of failure that compromises the entire network; instead, numerous computers in the same network interact with one another.

3. KEY CHALLENGES OF PROPOSED ANALYSIS

3.1 Blockchain for Fraud Detection: A Work-History Prevention System

The proposed method has a number of challenges, including the need to rely on data producers to keep a public valid sender address up to date. To put data and smart contacts on the public blockchain, employers must pay a transaction fee. Employees must maintain their private keys in a secure location. If an employee's private key is lost, he or she will be unable to access the system. She can't make sense of the information about her career history. These are some of the constraints that this argument must impose.

3.2 Fraud Detections for Online Businesses

Customers may make erroneous purchases as a result of rating fraud, decreasing their motivation for future interactions. It's tough to discern the difference between honest and phony raters because their evaluations are so identical. Although blockchain protocols can avoid some objective frauds, subjective frauds continue to be a source of concern for market portals. Even though the research proposes an important strategy for reducing subjective rating fraud, more work needs to be done to improve accuracy.

3.3 The Influence of Blockchain Detection on Fraud and Fake Prevention

During this time, the number of fraud attempts and the expense of preventing those fraud issues has skyrocketed. As a result, as fraud becomes more sophisticated, merchants and security firms will need to invest more in fraud detection systems. In a variety of exclusive trade areas, the adoption of blockchain technology to prevent fraud and impersonation has made transactions more secure and less vulnerable to impersonation. Despite these advancements, there is still opportunity for cost-effectiveness and dependability enhancement.

3.4 Are Blockchains Immune to all Malicious Attacks?

Fraud has always been a source of concern for the financial industry, since it has the potential to result in serious consequences and financial losses for those who fall victim to it. Malefactors may devise novel methods for stealing money and committing fraud. Despite the fact that blockchain developers are constantly improving the technology, new threat detection strategies and procedures are required. As a result, blockchain is not immune to all types of fraud, hacking, attacks, and other malicious activity.

3.5 A Blockchain-Based Framework for Fraud Detection

The goal of this study is to show and suggest a blockchain-based framework for preventing corruption and embezzlement during the transfer of monies from government schemes. Because corruption leads to inequitable money distribution and poverty, governments all over the world have begun to design and implement strategies, frameworks, and policies to improve transparency and openness in cash transfers.

3.6 Counterfeit Detection of Documents using Blockchain

Organizations issue certificates in the form of a paper document, which can be easily altered using modern technologies. Both the entity that issues the document and the organization that receives it are at danger. As a result, the document must be independently checked. We take advantage of the immutability of the blockchain to improve the security and transparency of the proposed system, which generates digital certificates with more precise information without the need for a third party.

3.7 A Multifaceted Approach to Bitcoin Fraud Detection: Global and Local Outliers

The Bitcoin network's lack of class classifications makes it difficult to comprehend unexpected financial behavior. To investigate fraud in the financial sector's most recent expansion, a holistic strategy is offered. Recent anomaly detection research has taken a comprehensive approach to the problem. A three-pronged approach to anomaly detection challenges faced by domain researchers is considered in a study. This includes truths like the fact that 1. datasets are unbalanced by nature, 2. static procedures are often used, and 3. the real world operates in dynamic conditions.

3.8 Video Fraud Detection using Blockchain

According to recent data, 93 percent of marketers use video advertising, with 65 percent placing their digital ads on YouTube. This issue is feasible, given the large number of online films available via the World Wide Web, Internet news feeds, electronic mail, business databases, and digital libraries. To our knowledge, no video fraud detection technique that uses Blockchain to determine whether a video has been modified has been reported in the literature. In addition, this industry is quickly growing.

As previously said, the biggest concern of video fraud can put individuals in danger since fraudulent information can brainwash them and radically alter their judgement. As a result, the project's purpose is to concentrate on detecting such video frauds.

3.9 Avoiding Insurance Fraud: A blockchain-based Solution for the Vehicle Sector

The purpose of this study is to describe a blockchain-based method for combating insurance fraud. This is a significant issue that is costing insurance companies a significant amount of money. The suggested blockchain-based fraud protection system helps to eliminate various issues brought on by falsified papers and fraud. One of the mentioned constraints is that a company may not want its data to be made public and hence will not use the system. In order to cope with the insurance plans that may be offered in such a system, the client may require anonymity from the company with whom he is dealing.

3.10 Avoiding Insurance Fraud: A Blockchain-based Solution for the Vehicle Sector

Servers hold all of the data and wait for client requests to process it and return the results. Despite the fact that this architecture is well-known and widely utilized, with a significant number of successful applications produced and running, it has a few flaws: The server is a vital component of the system since it is a single point of failure; if it fails, the entire system fails. Even if security measures are in place, data stored on the server has the potential to be altered or deleted. This is a severe problem that is costing insurers a lot of money. The proposed method aims to prevent a type of fraud known as double-dipping, which entails buying multiple insurance policies for the same car from different companies with the intention of simulating them after a traffic accident and thus receiving money from multiple insurance policies for the same event.

4. APPLICATIONS OF PROPOSED TECHNIQUES

In recent years, blockchain applications have attracted a lot of attention. They are more valuable than money and can be used to replace fiat money and traditional banking. The ability to trade wealth on a blockchain, on the other hand, is at the heart of the system and must be reliable. Blockchains have built-in features that assure the system's stability and durability. Malicious actors can still use well-known tactics to steal money, such as virus software or falsified emails. We also undertake a sensitivity analysis to show how the models offered rely on specific attributes and how the lack of some of them impacts overall system performance. Blockchain can be used to fight and prevent fraud in a business network. One of the fundamental characteristics that determines blockchain's worth is its ability to share data rapidly and securely without relying on a single institution to assume responsibility for data security.

One of the most significant advantages of blockchain technology is increased security. The increased security provided by blockchain is due to the way the technology works: With end-to-end encryption, blockchain generates an unalterable record of transactions, preventing fraud and unauthorized activity. Furthermore, blockchain data is kept across a network of computers, making it nearly impossible to attack (unlike conventional computer systems that store data together in servers). Furthermore, by anonymizing data and requiring permissions to limit access, blockchain can solve privacy concerns better than traditional computer systems.

Because blockchain transactions cannot be removed or modified, they are immutable. Before a "block" of transactions can be added to the blockchain, network participants must agree that the transaction is valid via a consensus process.

5. LITERATURE REVIEW

The comparative analysis of the various strategies will be presented in a tabular format in this section (Table 1). The comparison can be conducted based on the papers examined, the methods used, and the results obtained, the strategy employed, and the outcomes received with a validated future scope for the methods.

Table-1: Detailed Survey

Ref. No	Methods	Advantages	Disadvantage	Future scope
1-Fraud detections for online businesses: a perspective from blockchain technology	This research looks at how to rate fraud by distinguishing between subjective and objective fraud. It goes on to talk about how effective blockchain technology is for objective fraud and how limited it is for subjective fraud. Finally, it examines the reliability of blockchain-based reputation systems. It is based on the Reputation System concept. They essentially collect, aggregate, and disseminate information about entities' previous actions. Customers have found them to be effective in pre-evaluating the object's quality and controlling interaction-specific risks.	The user account can be created with a genuine identity in blockchain-based reputation systems, but the real identity is not revealed. One of the few benefits of reputation management systems: a) Use reputation systems to assess a potential seller's dependability in advance, allowing people to appraise the quality of unknown suppliers. b) They've been proven to be particularly successful at safeguarding clients against transactional threats. c) It boosts retailers' sales by increasing client confidence and assisting them in making purchasing selections. Also, if a seller offers tokens to fake ratings, the quantity of legitimate transactions will be reduced. These systems aid in the purchasing of high-quality goods, which is crucial for client satisfaction.	Rating systems are subject to rating fraud, which can lead to customers making erroneous purchases and lowering their motivation for future interactions. Because their evaluations are so identical, it's impossible to tell the difference between a fraudulent ratter and a genuine one. There are six different models of fraudulent ratter behaviour. Constant attack, camouflage attack, and whitewashing attack are three of them. By using skewed ratings, these attacks have an impact on the customer's choices. "Ballot stuffing" refers to fraudulent ratters injecting unduly high ratings into a target entity, whereas "bad-mouthing" refers to inappropriately poor ratings. Fraudulent raters can either complete the transaction, submit the rating, and then be reimbursed by the seller, or they can complete the transaction, submit the rating, and then be reimbursed by the seller. When a vendor is targeted by Sybil assaults, he or she is more inclined to advertise his or her own product by encouraging ratters to make legitimate transactions.	Blockchain systems are extremely good at avoiding objective information fraud, such as loan application fraud, in which the fake information is based on facts. However, subjective information fraud, such as rating fraud, when the fake information is difficult to verify, is a different storey. It's a type of record-keeping system that keeps records that are both permanent and incorruptible. However, because blockchain systems preserve users' privacy, we can only enable accounts created with true identities to submit reviews. The development of new methods for identifying both objective and subjective information frauds, as well as a deeper understanding of blockchain technology, will be the focus of future study.

2-Avoiding Insurance Fraud: A Blockchain-based Solution for the Vehicle Sector	They hope to explain how blockchain and smart contracts might be combined to improve organisational operations in this study. They show how these technologies could be utilised to create a system that prevents certain sorts of fraud in the automobile insurance industry.	The proposed system's goal is to make data from used car policies available to all insurance firms. This can be accomplished via a blockchain-based client-server architecture in which each node can view but not modify data. This aids in the consumer-buyer relationship's security, dependability, and transparency. By using blockchain, the system becomes decentralised, eliminating the need for a single system to serve as the central node. The primary solution entails the formation and termination of insurance policies, the creation of claims, and the keeping of a vehicle's life history. Blockchain also aids in the prevention of a sort of fraud known as "double-dipping," which comprises acquiring many insurance policies for the same car with different companies in order to simulate a traffic accident and collect money from multiple plans. In addition to combating insurance fraud, the technology allows insurance companies to access a vehicle's insurance history without having to rely on third parties.	The goal of this essay is to discuss a blockchain-based solution that demonstrates how this new technology could be used to avoid insurance fraud. This is a severe problem that is costing insurers a lot of money. The proposed blockchain-based fraud prevention system aids in the elimination of different challenges caused by forged documents and fraud. Some of the proposed constraints include the fact that a corporation might not want its data to be visible to the public and hence would not participate in the system. The client may require privacy from the company with which he is dealing to deal with the insurance policies that may be given in such a system.	Other features could be added in the future to improve efficiency and alleviate the limits of the existing approach. Because this project is still in the hypothetical stage, where it has been tested with fictitious insurance companies, clients, and automobiles, it must be implemented and thoroughly tested.
3-Blockchain for Fraud Prevention: A Work-History Fraud	This article looks at how blockchain technology can provide real-time job history verification at a low cost. The proposed	The proposed system's goal is to ensure that once a person's employment history has been confirmed, it	The verification procedure is frequently outsourced to external parties, which can be time consuming. The following are some	The project's future scope would entail delving more into the idea of a time-consuming process that every

Prevention System	method additionally assures that (work-history) data sharing is secure and private. As a means of authenticating data, blockchain is used to store encrypted versions of work history. This technology will also allow prospective employees to bundle many records and submit them to prospective employers, who will be able to authenticate each record against the blockchain version while maintaining both parties' privacy. The Smart Contract's sole purpose is to store the three elements that the System requires: encrypted data, a hash of unencrypted data, and the Smart Contract's creator.	can be stored in the system, eliminating the need for subsequent employers to separately seek such information. Individual employee work history verification is one of the benefits. b) Reduction in the amount of time it takes to verify job history. b) Individual employee data ownership, privacy, and integrity. This technology will also allow prospective employees to bundle many records and submit them to prospective employers, who will be able to authenticate each record against the blockchain version while maintaining both parties' privacy.	drawbacks: a) time-consuming and expensive process for employers. This blockchain method aids in the protection of data privacy. b) Relies on Data Producer to keep a public sender address up to date. There will be no way for the system to verify if the Data Producer deletes or removes access. c)To deploy data (work history) and smart contacts in the public blockchain, employers (data Producers) must pay a transaction fee. d)Employees must keep their private keys in a secure location. If an employee's private key is lost or stolen. She is unable to decipher the work-history information.	company must go through when employing new staff. It might serve as a foundation for additional blockchain systems, allowing them to aid fraud detection and keep user data private and undamaged across convergent parties. It quickly implemented smart contact to protect people's privacy. For further information, we can experiment with alternative blockchain implementations to see how the goal we set for ourselves, namely retrieving work history, has changed.
4-The Influence of Blockchain Technology on Fraud and Fake Protection.	The goal of this paper is to examine existing ideas and solutions that leverage Blockchain to reduce fraud and theft in some businesses and our society. The relationship between a supplier and a consumer, as well as a buyer and a seller, has become increasingly trusting.	By protecting against financial losses due to fraud, cheating, and counterfeiting, blockchain technology can assist to address several social and financial problems in a variety of domains, including finance, healthcare, supply chain, automobiles, democracy, and so on. By drastically lowering fraud and untruth, Blockchain technology is opening the road for the development of community trust. Because openness, visibility, and the integrity of organisations are crucial characteristics in an era, blockchain technology will be one of the most important attributes in cybersecurity in the	Blockchain applications can be too costly and time-consuming to be useful in certain areas of society. The network size adopted by blockchain is considerably too large and necessitates far too many servers, which are out of reach for most businesses.	The paper's future scope is to delve deeper into the details of blockchain as a fraud detection environment in various industries. For a rising economy like ours, looking into numerous combat aspects such as reliability, trustworthiness, and visibility. Blockchain is a valuable future asset for the country, and it must be included into future technical projects.

		near future.		
5-Are blockchains immune to all malicious attacks?	This study looked at a variety of strategies that have been suggested and used to detect fraudulent transactions and behaviours that depart from normal patterns of behaviour. Guided classifications such as decision trees, support vector machines, evolutionary algorithms, Bayesian belief networks, and neural networks are common outlier analysis methods.	Due to the distributed consensus and cryptographic transactions enforced by blockchain technology, it is difficult to damage the integrity of its records without being noticed by the whole network. Registration, verifying, and managing transactions are some of the unique features of blockchain. Double-spending and record hacking are two sorts of online criminal acts that blockchain technology prevents.	Fraud is a sort of malicious behaviour that involves deceiving people in order to get an advantage or benefit. Fraud has long been a source of concern for the financial industry since it can result in major consequences and losses for its victims. 51 percent attack, account takeover, digital identity theft, money laundering, and hacking are all potential hazards for blockchain.	Blockchain technology's bookkeeping and attack prevention capabilities are highlighted by distributed consensus, trustlessness, anonymity, cryptography, and other aspects. The following suggestions address methods to improve its resilience, fraud prevention, and anti-hacking capabilities. a) Detection equipment. b) Blockchains for identity and reputation. c)Legislation and regulation, as well as widespread acceptance
6-A Blockchain-Based Framework for Fraud Detection	The goal of this study is to use blockchain technology to minimise corruption and fraud. To develop our system, we used a generic scenario in which a government runs several schemes for the benefit of the general public, and the money are dispensed through a layered government architecture that passes through various institutions. Corruption in various programmes at various levels can be caused by lack of transparency, poor administration of government documents, and delays in the verification process.	Blockchain technology is described in this paper as a way to decrease the layers of corruption in government procedures. This study focuses on employing a novel form of encryption method to overcome security and privacy concerns in blockchain. The proposed model ensures that everyone linked to a soon-to-be-implemented blockchain network may see all government procedures. This enables ordinary citizens to investigate the operation of any government scheme, track its progress, and track financial transfers.	The following are some of the drawbacks of this model: • Stagnation of funds caused by middle-level authorities. • Money is misappropriated in the middle levels, with everyone blaming each other. • Schemes are executed slowly. • Identifying the true needy/beneficiary is a challenge. • Inappropriate financial allocation. • The beneficiary's illiteracy and stupidity	Because it is secure and meets the required triad of cryptography, namely confidentiality, integrity, and authenticity, blockchain has now become the future of finance. As a result, ordinary people may audit this system to track the financial flow of any plan, making it completely open and equitable.
7-Counterfeit Detection of Documents using Blockchain	Document verification is a domain that entails a number of problems and time-consuming processes in order to authenticate documents.	The blockchain's immutability provides greater security and transparency in the proposed system's transactions, which	In terms of public security, the scrutiny of printed documents is crucial. In theory, there are two methods to approach the problem of document	This paper can be used to offer a blockchain-based solution to the problem of counterfeit documents. The blockchain technology offers the

	The purpose of this article is to use blockchain to improve document verification. For storing and distributing data in a distributed file system, we present a system that employs the InterPlanetary File System [IPFS] protocol as well as a peer-to-peer network. We can offer a more secure and efficient digital certificate validation by utilising blockchain technology.	produce digital certificates with more accurate information without the intervention of a third party. The blockchain allows for the storing of immutable data. The blockchain technology is being utilised to reduce document frauds. The papers on the blockchain must meet certain basic requirements, including authentication, authorization, secrecy, ownership, and privacy. This method is designed to eliminate the problem of phoney certificates or document fraud.	counterfeit detection: model-based or generically. The model-based approach necessitates prior knowledge of the characteristics of the document to be checked and then searches for them precisely. Frequently, papers are prepared with the prospect of such checks in mind, incorporating security elements that are easy to check for later, either with the naked eye or with the aid of special instruments. Generic counterfeit detection systems have a higher rate of mistake than model-based systems due to limited knowledge, but they have the advantage of being applicable to a broader class of documents. In most cases, the generic method does not work.	user's documents with authentication, authorisation, privacy, confidentiality, and ownership, which are all necessary features of digital documents. As a result, this system will benefit both the students and the company.
8-A Multifaceted Approach to Bitcoin Fraud Detection: Global and Local Outliers	The lack of class designations in the Bitcoin network tends to obfuscate the interpretation of unusual financial behaviour. Using trimmed k-means and kd-trees, this article describes Bitcoin fraud from both a global and local perspective. Random forests, maximum likelihood-based, and boosted binary regression models are used to study the two spheres further.	Using global and local reference frames, this study will use a dual approach to identifying fraud and non-fraud behaviour. The results of the supervised learning algorithms utilised in this study highlighted the most essential features that were beneficial in detecting perceived anomalous actions on the network.	It should be noted that certain nodes were exclusively involved in sending or receiving Bitcoins. As a result, there were missing values in the final dataset, which necessitated the use of imputation. Based on the concept of equivalent to giving or receiving 0 BTC, all missing quantities were imputed with zeroes.	Random forest was determined to be the highest performing classifier with 8 features across the three models, regardless of class imbalances. The results of the supervised learning algorithms utilised in this study highlighted the most essential features that were beneficial in detecting perceived anomalous actions on the network.
9- Video Fraud Detection using Blockchain	The subject of Video Fraudulence has been addressed in this study, which means that attackers can tamper with the original video and generate their own phoney video. Given the vast volume of online	To make it a real-time fraud detection tool for films, the scheme is totally developed on the Ethereum or Hyperledger Blockchain frameworks. The discussion of how	A dangerous environment is created by a lack of regulation. Because of its intricacy, end users have a hard time appreciating the benefits. To offer security and achieve consensus over a dispersed network,	The entire real-time Blockchain network will be used in our future effort to detect video fraudulence on a wide scale.

	films available via the World Wide Web, Internet news feeds, electronic mail, corporate databases, and digital libraries, this challenge is quite practical. The focus is on Blockchain's usability and how to utilise it to get the desired result. Decentralization, data transparency, and security and privacy are three properties of Blockchain that are being used to give a viable solution.	cryptography and blockchain technology can be used to detect video fraud has been summarised in this article.	blockchain relies on encryption. This essentially means that complicated algorithms must be executed in order to "prove" that a user has authorization to write to the chain, which requires a lot of processing power. This, of course, comes at a price.	
10- Avoiding Insurance Fraud: A Blockchain-based Solution for the Vehicle Sector	We will explain how blockchain and smart contracts can be utilised together to improve organisational operations in this article. We show how these technologies could be utilised to design a system that prevents certain sorts of fraud in the vehicle insurance industry.	The purpose of this article is to discuss a blockchain-based solution that highlights the possible application of this new technology in the area of insurance fraud prevention. The proposed approach aims to prevent one type of fraud known as double dipping, which involves purchasing many insurance policies for the same car with different companies in order to later imitate a traffic accident and get money from multiple insurance plans for the same occurrence.	The server plays a critical function in the system, serving as a primary point of failure in the sense that if it fails, the entire system fails. Even if security precautions are in place, the data stored on the server has the potential to be modified or erased.	The purpose of this article is to discuss a blockchain-based solution that highlights the possible application of this new technology in the area of insurance fraud prevention. Our proposed approach is now in the prototyping stage. It has been proven to operate with data from fictitious insurance firms, clients, and automobiles. We plan to expand the solution's functionality in the future and, possibly, evolve it into a finished product.

CONCLUSION

All of the papers mentioned above have introduced blockchain technology and its defining characteristics. They also review state-of-the-art technologies for detecting online fraud and intrusions, identify certain fraud and malicious activities that blockchain technology can effectively prevent, and make recommendations for strategically fighting various attacks to which blockchain technology may be vulnerable. Existing machine learning and data-mining algorithms could find new uses in identifying fraud and intrusions in blockchain-based transactions. Guided machine learning methods like deep-learning neural networks, support vector machines, and Bayesian belief networks may help detect outlier behaviors by profiling, monitoring, and detecting behavioral trends based on people's transaction histories. Despite the advancement in technology, still, the problems regarding Video Fraudulence are faced and there is no concrete solution for this problem. To improve the technology and related anti-attack methods, more research is required.

REFERENCES

[1] Joshi, P., Kumar, S., Kumar, D., & Singh, A. K. (2019, September). A blockchain based framework for fraud detection. In 2019 Conference on Next Generation Computing Applications (NextComp) (pp. 1-5). IEEE.

[2] Cai, Y., & Zhu, D. (2016). Fraud detections for online businesses: a perspective from blockchain technology. Financial Innovation, 2(1), 1-10.

[3] Dhiran, A., Kumar, D., & Arora, A. (2020, July). Video Fraud Detection using Blockchain. In 2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA) (pp. 102-107). IEEE.

[4] Nerurkar P, Bhirud S, Patel D, Ludinard R, Busnel Y, Kumari S. Supervised learning model for identifying illegal activities in Bitcoin. Appl Intell. 2020;209(1):1-20.

[5] Ostapowicz, M., & Żbikowski, K. (2020, January). Detecting fraudulent accounts on blockchain: a supervised approach. In International Conference on Web Information Systems Engineering (pp. 18-31). Springer, Cham.

[6] Raikwar, M., Mazumdar, S., Ruj, S., Gupta, S. S., Chattopadhyay, A., & Lam, K. Y. (2018, February). A blockchain framework for insurance processes. In 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS) (pp. 1-4). IEEE.

[7] Dhieb, N., Ghazzai, H., Besbes, H., & Massoud, Y. (2020). A secure ai-driven architecture for automated insurance systems: Fraud detection and risk measurement. IEEE Access, 8, 58546-58558.

[8] Shanmuga Priya P and Swetha N, "Online Certificate Validation using Blockchain", Special Issue Published in Int. Jnl. Of Advanced Networking and Applications (IJANA).

[9] Monamo, P. M., Marivate, V., & Twala, B. (2016, December). A multifaceted approach to bitcoin fraud detection: Global and local outliers. In 2016 15th IEEE International Conference on Machine Learning and Applications (ICMLA) (pp. 188-194). IEEE.

[10] Xu, J. J. (2016). Are blockchains immune to all malicious attacks? Financial Innovation, 2(1), 1-9.

[11] M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[12] R. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press.

[13] K. Elissa, "Title of paper if known," unpublished.