Review the Recent Fraud Detection Systems for Accounting Area using Blockchain Technology

Rania Alsulami, Raghad Albalawi, Manal Albalawi, Hetaf Alsugair,Khaled A.Alblowi, and Adel R. Alharbi*

Faculty of Business Administration, University of Tabuk, Tabuk 71491, Saudi Arabia
*College of Computing & Information Technology, University of Tabuk, Tabuk 71491, Saudi Arabia

Abstract
With the increasing interest in blockchain technology and its employment in diverse sectors and industries, including: finance, business, voting, industrial and many other medical and educational applications. Recently, the blockchain technology has played significant role in preventing fraud transactions in accounting systems, as the blockchain offers high security measurements, reduces the need for centralized processing, and blocks access to the organization information and system. Therefore, this paper studies, analyses, and investigates the adoption of blockchain technology with accounting systems, through analyzing the results of several research works which have employed the blockchain technology to secure their accounting systems. In addition, we investigate the performance of applying the deep learning and machine learning approaches for the purpose of fraud detection and classification. As a result of this study, the adoption of blockchain technology will enhance the safety and security of accounting systems, through identifying and classifying the possible frauds that may attack the accounting and business organizations.

Keywords:
blockchain technology, autonomous fraud detection, accounting systems, machine learning, deep learning.

1. Introduction

Recently, the society has increasingly relied on accounting and finance systems in order to meet the increasing need for information. Finance is considered as one of the most significant issues for any company in managing its business to always run smoothly, where accounting systems can positively assist to perform this. In general, companies employ accounting systems in order to manage and organize financial information, including keeping track of all transactions that are processed by a company. Therefore, accounting systems play vital role in most of the companies and organizations [1].

Accounting systems enable complete tracking of financial transactions, real-time reporting, and analysis. Moreover, accounting systems assist businesses to track and manage their financial transactions and allow easier work of accountants. An efficient accountant system application should be user-friendly, easy to access, and accurate.

In general, accounting information system is an element of an organization that collects, classifies, processes, and communicates financial information. However, accounting systems are prone to several threats, including: error in software and malfunction of equipment, violation of internal control, and manipulation of financial information. The work presented in [2] involves the discussion of 19 computerized accounting threats, where this study explored that potential threats include virus and online attackers who may violate the privacy of the accounting systems.

Usually, the accounting firms routinely gather sensitive information, where the data may include personally identifiable information, for instance: credit card numbers, national ID, and bank account information. Therefore, this valuable information may attract hackers and malicious insiders to access this sensitive information.

There are several data security procedures that may be processed to secure the accounting firms, through employing several strategies [3], including: *First*, physical security through adopting basics access restrictions to the physical space. *Second*, protecting the accounting system assets using firewalls and make sure that it's with the latest patches, in addition to employing antivirus and antimalware software which can help in preventing malware attacks. *Third*, controlling the sensitive data transfers through employing Data Loss Prevention (DLP) approaches in order to monitor and control the transfer of sensitive information (accounting information). *Fourth*, the securing of external devices, through either restricting the use of external and removable disks or adding an extra layer of security. And *fifth*, training the

Manuscript received May 5, 2023
Manuscript revised May 20, 2023
https://doi.org/10.22937/IJCSNS.2023.23.5.13

employees in the organization, through educating the employees with the recent attacks and the significant procedures that need to be accomplished.

However, in this paper, we focus on the area of securing and protecting the accounting information that exist in the accounting systems through the adopting of the blockchain technology. This paper investigates the adoption of blockchain technology for the purpose of fraud detection in the accounting area, and discusses how the employment of blockchain technology will significantly enhance the fraud detection efficiency. Therefore, the main contribution of this paper lies on the following aspects:

Discuss and analyze the term blockchain technology and its significant in the area of accounting systems.

Present the possible employment of blockchain technology for the purpose of fraud detection in the area of accounting.

Summarize the recent employment of machine learning and deep learning in fraud detection for accounting systems.

Discuss and analyze a set of evaluation metrics to assess the efficiency of any fraud detection system in accounting applications.

The remainder of this paper is organized as follows: Section 2 presents the methodology which has been adopted to accomplish this study, whereas Section 3 discusses the term Blockchain technology, whereas Section 4 presents the employment of blockchain technology in accounting systems. The recent developed fraud detection accounting systems that are based on the blockchain technology are discussed in Section 5. A comparison study is presented in Section 6, where a set of validation metrics is presented. Section 7 discusses the obtained results and presents the main findings of this study. And finally, Section 8 concludes the work presented in this paper and presents a set of future works.

2. Methodology

The main research question in this paper is: what is the impact of employing blockchain technology in accounting systems to prevent the fraud detection. Therefore, in order to address this research question, the following research methodology which is presented in Figure 1, has been adopted. *First*, we study and analyze the main practices of blockchain technology and the recent applications that have employed the blockchain technology.

Second, the recent research works that have targeted the area of fraud detection for accounting systems using the blockchain technology, has been investigated. The investigation process involves surveying the recent research works in the field from several research engines for research works, including: Google Scholar, Scopus, Web of Science, and Scopus. However, we focused on the research works that includes practical studies and results. The total obtained research papers were around 52, where a number of 19 research articles were excluded as they do not include practical studies. Therefore, a total number of 33 research studies was included in this research work.

Third, the chosen research studies have been analyzed and discussed in order to show the impact of the blockchain technology on fraud detection in accounting systems.

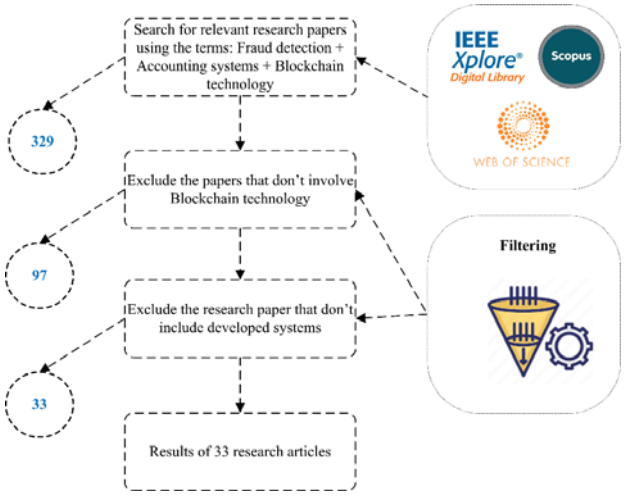

Figure 1: The structure of the research methodology

3. Blockchain Technology

Recently, the term blockchain has been involved in diverse types of applications, including: governmental, healthcare, finance, manufacturing, and so on. Blockchain is considered as a method for recording information that makes it difficult for the system to hacked, changed, or manipulated. The blockchain technology is considered as a structure that

stores transactional records, that is also known as "block", of the public in several databases, that is known as the "chain" in a network connected through peer-to-peer nodes. Generally, this storage is referred to as a "digital ledger" [4]. Figure 2 presents the concept of the blockchain technology.

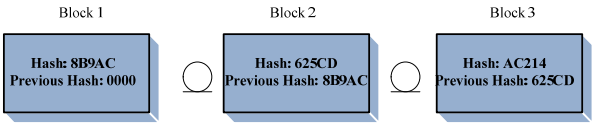

Figure 2: The main concept of the blockchain technology

The blockchain technology is a distributed, decentralized, and public digital ledger which is used to record transactions across several computers, then the records cannot be changed retroactively without the modification of all subsequent blocks and the compromise of the network [5]. In general, the blockchain is an emerging technology that involves several advantages in an increasingly digital world, including:

1. Highly secure: blockchain technology employs a digital signature feature in order to assure fraud-free transactions that make it impossible to corrupt or alter the data of an individual by other users without having the specific digital signature.
2. Automation capability: blockchain technology is a programmable and can produce systematic actions, events, and payments in an automatic way, when a certain condition of the trigger is met.
3. Decentralized system: the blockchain technology allows the transactions to be accomplished with the mutual consensus of the users resulting in safe, faster, and smoother transactions.

In addition, the blockchain technology allows users to verify, maintain, and synchronize the contents of a data file replicated by several users. Blockchain technology has offered significant advantages to industries through enabling better services. However, the blockchain technology is a new technology and there is still inaccurate details and uncertainty regarding the potential value of blockchain [6].
On the other hand, according to [7] the blockchain technology is in the experimental phase and has several issues that need to be addressed, including: information confidentiality, limited data processing capacity, and regulatory challenges. In addition, Yu et al (2018) argued that the blockchain will be used as a platform for firms to voluntarily share information. Moreover, in the long run, the blockchain technology could effectively minimize errors in disclosure and earnings management, mitigate information asymmetry, and increase the quality of accounting information [7].

The blockchain technology has been employed widely in financial accounting due to its possible impacts. One of the most famous uses of Blockchain technology is the Bitcoin, where the Bitcoin is a cryptocurrency that is used to exchange digital assets online. The Bitcoin concept employs cryptographic proof instead of adopting a third-party trust for two parties to communicate and execute transaction over the Internet. Figure 3 shows an example on money transaction using the Blockchain technology. As presented below, the first stage includes requesting a transaction, where then a block representing the transaction is created. Then the block is sent to every node in the network, where the nodes validate the transaction and receive a reward for the proof of work. At the end the block is added to the existing Blockchain and then the transaction is complete.

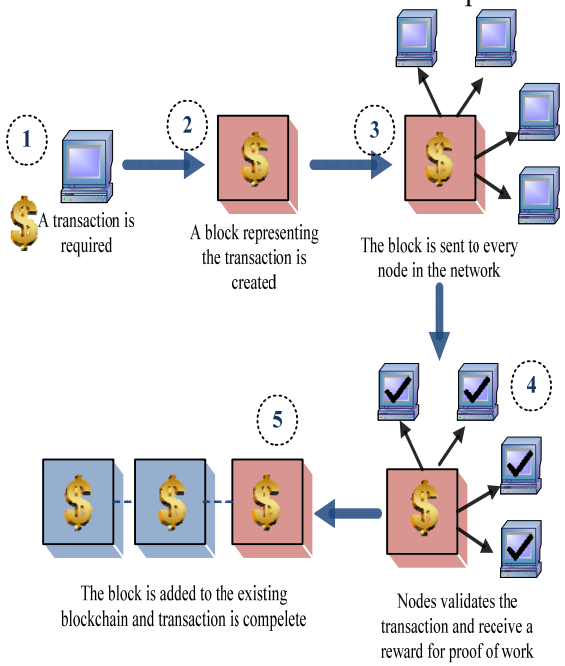

Figure 3: The process of blockchain technology in money transaction

4. Blockchain Technology in Accounting Systems

The Blockchain technology is also known as Distributed Ledger Technology (DLT) which is a system where the transaction records stored in blocks are maintained across several linked computers. The blockchain in accounting technology is concerned with transferring the ownership of assets and maintaining a ledger of precise financial details. The employment of Blockchain technology with the finance and accounting systems has offered several advantages. Figure 4 shows an example of two companies trying to establish a transaction between them, using the traditional accounting practices.

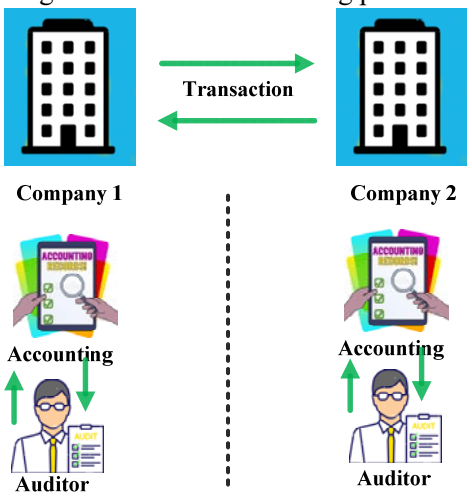

Figure 4: Current accounting practices

Blockchain technology offers new ways to record, process, and store financial transactions and information, and has the ability to fundamentally alter the landscape of the accounting profession and reform the business ecosystem.

In accounting systems, there are two possible types of blockchain: the permissionless and permissioned blockchain technologies [8]. The former can be described as one that enables records to be shared by all the network users, updated by miners, observed by everyone, and owned and controlled by no one, whereas the later, such as Bitcoin, any host may use its computers to join the network. The permissionless blockchain has the benefit of decentralization and has been backed by the success of various widespread applications. However, the permissionless blockchain has a speed limit in processing large volumes of transactions [9].

The permissioned blockchain technology refers to a type of blockchain with boundaries in its membership and control procedures. Different members have different access control authorization, therefore the permissioned blockchain is intended to be partially decentralized. In addition, permissioned blockchain is likely to maintain privacy and fit business governance requirements than a permissionless blockchain [10]. Figure 5 presents an example of an accounting practice using the blockchain technology.

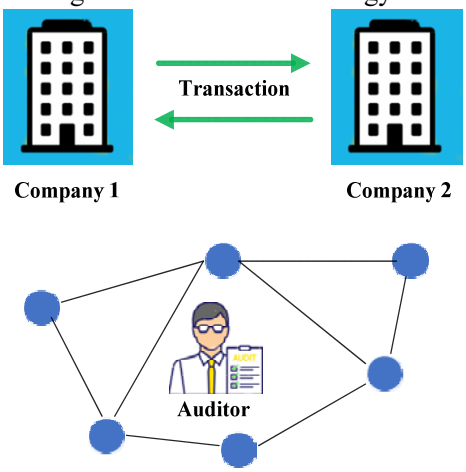

Figure 5: Potential blockchain accounting practices

Recently, the dramatic changes in accounting area have occurred due to the recent development of software that is capable of producing different information and keeping records of transactions. Blockchain technologies have allowed the accounting systems to help professionals and keep tracking of transactions that are represented by “blocks” in a secure manner. The blockchain technology offers transaction recording functionalities and verify transactions without the requirement of intermediary. Moreover, blockchain technology benefits the accounting systems through eliminating errors that may occur due to intermediary [11].

The blockchain technology has been employed in accounting because of the vast internet infrastructure that is available in most of the organization. In addition, accounting is considered as a significant area and requires an intensive protection and encryption mechanisms in order to make accounting systems safe [12].

The blockchain technology employs a cybersecurity mechanism in order to allow for safe and reliable transactions over the Internet. In general,

the blockchain guarantees the ledger database to be secure, tamper proof, and offer permanent transaction records of the business between any two parties. As soon as the transaction is approved by the participants, then the transaction is added to the blockchain, and it cannot be altered, edited, or deleted. Therefore, blockchain technologies have been employed with accounting systems due to several reasons: blockchain technology offers affordable cost, and minimizes the possibility of loss information.

5. Fraud Detection-based Blockchain Technology for Accounting Systems

Transactions in accounting systems can be protected through employing several approaches, where one of the most widely used methods is the data encryption, where it is considered as a method for securing transaction records from unauthorized access. Data encryption involves restructures the transactions into incomprehensible pattern. Therefore, the successful and safe deployment of distributed ledger systems and the point-to-point network is impossible without the existence of an efficient security mechanism.

Recently, blockchain technology has been employed in diverse applications, especially in financial and currency exchange applications, due to its high security and trustworthiness. In general, employing the blockchain technology to secure data transactions can be occurred in two different methods: cryptography and hashing. The former is adopted to encrypt transactions in Peer-to-Peer (P2P) network, whereas the latter is employed to secure block information and link blocks in a blockchain.

The employment of machine learning approaches has received considerable attention recently driven by the requirements to obtain high anomaly detection classification accuracy with the least time possible. In general, the adoption of machine learning in blockchain technology for the purpose of identifying anomalies and attacks in accounting systems. This section discusses the recent developed fraud detection methods for accounting systems that have deployed the blockchain technology and the Artificial Intelligence (AI). Therefore, AI-based fraud detection methods for accounting systems using the blockchain technology, can be divided into four phases, as presented in Figure 6.

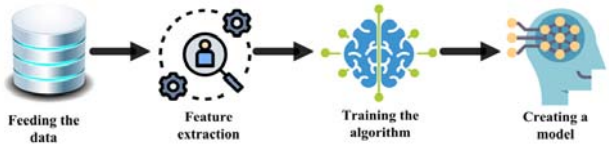

Figure 6: Main stages of fraud detection system using machine learning

The first phase involves collecting the transaction records and feed them to the machine learning system. In the second phase, the most significant features are extracted in order to involve the most relevant data in the training process. The third phase involves train the machine learning model using the processed transaction records. And finally, the model creation is constructed in phase four.

The work presented in [13] reviews the recent developed anomaly detection systems for blockchain technology, and covers the general aspects of anomaly detection in details from basics to the integration perspective at diverse layers of the blockchain technology.

A security mechanism is presented in [14] based on analysing the blockchain technology traffic statistics to detect malicious attacks through the function of data collection and anomaly detection. This mechanism works by sensing underlying blockchain traffic and generates multi-dimensional data streams in a periodic manner. Then, the anomaly detection engine detects anomalies from the established data instances based on the employment of semi-supervised machine learning approach.

The work presented in [15] involves developing a deep learning model to detect the threat hunting in Ethereum blockchain. The Ethereum blockchain is a decentralized, open-source blockchain that has been employed in widespread accounting organizations, it aims for building applications and organizations, transacting and communicating without the requirements of a central authority control [16]. The developed system in [15] incorporated both the machine learning algorithms including unsupervised and supervised algorithms for the purpose of attack classification. The achieved classification accuracy was equal to 97.72% for Ethereum attack detection, whereas a 99.4% for attack classification.

The work presented in [17] involves the identification of suspicious transactions from Binance, which is an open-source cryptocurrency, through the means of

identifying and detecting the cryptocurrency wallets. An unsupervised learning expectation maximization algorithm has been employed in order to cluster the dataset. Anomaly detection has been performed using the Random Forest (RF) classifier.

In [18], Ashfaq et al. (2022) addressed the problem of fraud and anomalies in the Bitcoin network. A secure fraud detection model has been developed that is based on the adoption of machine learning and blockchain technology. Two different machine learning algorithms have been employed for the purpose of transaction classification, named as XGboost and RF, where a 99% classification accuracy has been performed.

Ibrahim et al. (2021) investigated the lllicit accounts on the Ethereum blockchain and developed a fraud detection model through employing three different machine learning algorithms: decision tree (J48), K-Nearest Neighbors (KNN), and RF, and tested using a real dataset that consist of 42 features where only a set of 6 features has been extracted. This work revealed that RF classification model offers the best classification accuracy [19].

In [20], Kumar et al (2020) proposed a system to detect malicious nodes using supervised machine learning based anomaly detection method in the transactional behavior of the finance accounts. Two different machine learning model have been adopted and considered for two account types: Externally Owned Account (EOA) and smart contract accounts. The obtained results proved the detection accuracy of 96.54% with a percentage of 0.92% false-positive ratio, whereas the results obtained for the EOA and smart contract accounts are 96.82% with 0.78% false positive ratio, respectively.

A mobile edge computing-based mobile application framework is presented in [21] in order to protect the data security and privacy of the transactions using the mobile devices in the industrial Internet of Things (IoT). A deep reinforcement learning additional practical swarm optimization algorithm is proposed to solve the unnecessary search of a deep deterministic policy gradient approach.

A new methodology has been proposed in [22] which involves the employment of intelligent software agents to monitor the activity of stakeholders in the blockchain network, in order to detect anomaly (collusion for instance), through the adoption of machine learning and game theory algorithms.

Podgorelec et al. (2019) proposed a machine learning approach that involves automated signing of blockchain transactions, while including a personalized identification of anomalous transaction. For validation purposes, several experiments were conducted based on the data obtained from Ethereum public main network. The results showed promising outcomes and paved the road for a probable future integration of a method in dedicated digital signing software for blockchain transactions [23].

The work presented in [24] involves an analysis of a real case study of recent accounting scandal of Luckin Coffee. This work studied how the blockchain technology may help to detect and prevent accounting fraud through employing the fraud triangle model. In addition, authors discussed the three characteristics of blockchain technology will assist to break the fraud triangle. As the decentralized phase will basically increase the fraud cost, the append-only linear shape of the transactional data will improve the tracking to tokenized assets, and with smart-contracts that operate in automatic controls, the blockchain removes the human factor and thus improve the control environment. Based on the case study, this paper discussed how the blockchain-based accounting systems can break the fraud triangle, and hence facilitate the accuracy and reliability of fraud detection and prevention.

In [25], Cai and Zhu (2016) explored the rating fraud through differentiating the subjective fraud from the objective fraud. Moreover, this work discussed the potential strengths and limitations of blockchain-based reputation systems under two attacks: the ballot-stuffing and bad-mounting attacks. Authors revealed that the blockchain-based systems are more robust to bad-mounting rather than ballot-stuffing frauds.

In [26], Tan and Low (2019) examined the prediction that blockchain technology will transform the accounting profession, where the prediction assumes that transactions are recorded in a blockchain will be easily aggregated into financial statements, and hence can be automatically confirmed as true and precise. The final results showed that the blockchain will likely change the existing accounting information systems at the database engine level where the data are processed. In addition, digitizing the current paper-based validation process may reduce honest errors and hence the immutability of a blockchain can discourage frauds.

The work presented in [27] involves applying supervised learning techniques to detect fraudulent accounts on the Ethereum blockchain. Authors analyzed the performance of Random Forest, Support Vector Machine, and XGBoost classifiers in order to identify such accounts basing on a dataset of more than 300,000 accounts. As a result, this work achieved efficient recall and precision values allowing the designed system to be applicable as an anti-fraud rule for digital wallets or currency exchanges.
As presented above, several fraud detection and classification approaches have been developed using both the blockchain technology and machine learning methods for accounting systems. The existing systems employed various machine learning models and different fraud detection accuracy has been achieved.

6. A Comparison Study of Fraud Detection methods for accounting systems

As presented earlier in the previous section, there are several fraud detections accounting systems have been employed widely through the adoption of blockchain technology. However, it is important to investigate the performance of the developed fraud detection approaches for accounting systems. Therefore, the recent developed systems are discussed and analyzed based on the evaluation of several significant metrics, including:

1. Investigated attack: this refers to the attack type that is addressed in the research work. As known, several attacks may affect the accounting systems, therefore, it is important to identify the attack type.
2. Security approach: this refers to the method that is employed to protect the accounting system from the potential attack.
3. Employed dataset/network: usually, fraud detection systems require the employment of a dataset in order to allow the AI model to adapt with the potential thread. Therefore, the dataset size is a crucial metric to assess the efficiency of the developed solution.
4. Obtained results: this refers to the results obtained from the developed security approach.

Table 1 presents a comparison among the recent developed fraud detection methods for accounting systems, where different attacks were investigated by the existing research works, however, there is a demand on protecting accounting systems from cryptocurrency wallet attacks.

On the other hand, several machine learning models have been employed in the detection and classification phase, through the adoption of a certain dataset of transaction records in order to train the employed machine learning model. Figure 7 shows the employment frequency for each machine learning model in the fraud detection process. As noticed from Figure 6, RF machine learning model has been employed in 4 different research studies for the purpose of attack detection and classification, whereas XGBoost model occupies the second place, where it was employed in 3 different research studies. Finally, the SVM, DT, KNN, and autoencoder machine learning models were used in a single research work.
Machine learning methods plat significant rule in fraud detection for accounting systems. However, as noticed in the comparison table, each machine learning model offers diverse classification accuracy. Therefore, it is important to adopt an efficient machine learning model for the purpose of fraud detection.

As presented below, there are several types of attacks that can be classified using the machine learning approaches, including: cyber-attacks on bitcoin, Ethereum threats, cryptocurrency wallets, anomaly attacks, signature frauds, ballot-stuffing, digital wallets, and currency exchange attacks. Hence, the adoption of machine learning has the ability to detect and classify diverse types of attacks.

Table 1: A comparison among the recent developed blockchain-based accounting systems

Research work	Investigated attacks	Security approach/model	Employed Dataset/network	Obtained results
[14]	Cyber-attacks on Bitcoin	Autoencoder	Mainnet	Classification accuracy: 100%
[15]	Ethereum threats	Deep learning method	Ethereum	Detection accuracy: 97.72% Classification accuracy: 99.4%
[17]	Cryptocurrency wallets	Random Forest	Binance	This work revealed that labelling the wallets with discernible transactions may help financial institutions, private sectors, and government agencies
[18]	Fraudulent transaction	Xgboost and Random Forest	Bitcoin network	Classification accuracy: 99%
[19]	Fraud detection	Decision Tree Random Forest K-nearest neighbour	Ethereum Kaggle.com	RF achieves the best classification accuracy: 95.2
[20]	Ethereum DOA attack	XGBoost	Ethereum	Classification accuracy: 96.82
[22]	Anomaly attacks	Game theory algorithm	NA	Classification accuracy: 93
[23]	Signature frauds	Unsupervised anomaly detection	Local dataset/Ethereum	An efficient machine learning method is proposed that will enable an automatic digitally signing of blockchain transactions
[24]	Fraud triangle	NA	NA	Blockchain technology is able to break the fraud triangle
[25]	Ballot-stuffing and bad mouthing	NA	NA	Blockchain based system are more robust to bad-mounting than ballot-stuffing fraud
[27]	Digital wallet and currency exchange attacks	Random Forest, Support Vector Machine, and XGBoost	Etherscan	Efficient precision and recall values allowing the designed system to identify anti-fraud for digital wallets and currency exchanges.

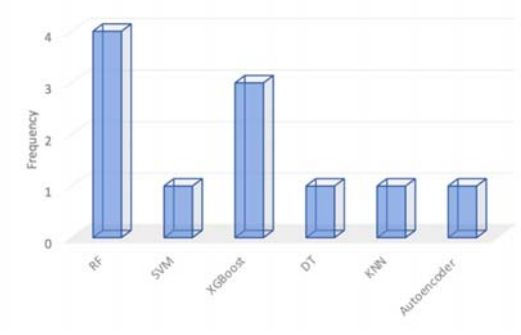

Figure 7: The frequency for the employment of each machine learning model in the investigated studies

Finally, the obtained results are discussed for each fraud detection model. The existing developed fraud detection systems achieve various classification and detection accuracy. The average fraud classification accuracy was around 98%, whereas the average fraud detection accuracy was around 97%.

Figure 8 depicts the classification accuracy for each fraud detection model.

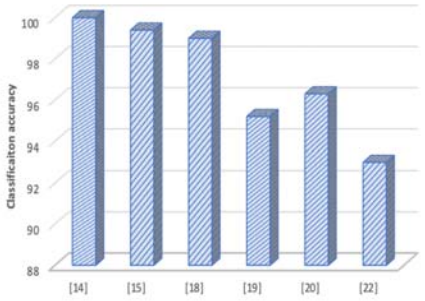

Figure 8: The fraud classification accuracy for several approaches

7. Discussion

Blockchain technology showed a highly impact on the accounting systems in a positive way, as the blockchain offers several advantages to the accounting systems. The blockchain technology processes the transactions in a decentralized manner, where the entire process does not require any authority from negotiators.

In general, the blockchain technology is a large database shared and distributed among different entities, decentralized, cryptographically protected, and managed into blocks of mathematically related transactions. The main principle of blockchain is decentralized accounting, where the entities in the network may approve, validate, and record the transactions, instead of allocating the whole responsibility on a single-entity.

Typically, the computer accounting systems are hot target for attackers due to the value of information of the companies that they handle, including: email addresses, financial records, credit card information, and bank accounts. In accounting systems, it is a key to maximize the security management and minimize the risk [28, 29].

Several recent research works analyzed the performance of blockchain technology into accounting systems. For instance, the work presented in [30] investigated and analyzed how the blockchain technology can enhance the transparency and trust in accounting practice, and how its professionals can improve decision-making by using the blockchain's ability to offer immutable, verified, shared, append-only, and agreed-upon data. In addition, the investigation showed how the blockchain technology affected positively the accounting, particularly with relevance to AI-enabled auditing and recognizing themes.

In addition, the employment of blockchain technology with accounting systems offer several advantages, as the adoption of blockchain technology offers new possibilities to record and backup sensitive and confidential data of accounting systems. As a result, the adoption of blockchain technology with accounting systems offer many benefits, include: transparency and trust, smart contracts, and continuous audit [31].

Therefore, the adoption of blockchain technology is a safe method to secure accounting transactions. This refers to that the blockchain technology is a secure and permanent transaction records between two parties. As soon as the transaction is approved by participants, then the transaction is added to the blockchain, and hence it cannot be altered, removed, or edited [32].

On the other hand, the adoption of blockchain technology with accounting systems may raise several challenges, where these challenges include: flexibility, scalability, and cybersecurity. In addition, an intensive discussion between auditors, regulators and other parties are needed to take place, before adopting the blockchain technology with the accounting systems [33].

The adoption of the machine learning methods for the purpose of fraud detection in accounting systems offers efficient security solutions. For instance, the work presented in [14] achieves the best classification accuracy with a percentage of 100. On the other hand, the fraud detection solutions presented in [15, 18] offer almost 90% classification accuracy, whereas the works presented in [19, 20, 22] offer reasonable classification accuracy (93% - 96%). Therefore, machine learning methods have significantly enhanced the efficiency of fraud detection tasks in accounting systems, and hence the employment of machine learning methods is an advantage for security purposes.

Moreover, various challenges posed by the blockchain technology to forensic accountants in the detection and prevention of frauds may arise. As a result, the blockchain technology will affect the core functions of accountants, however the overall effects on the roles of forensic accountants and auditors are still vague [34].

In conclusion, the adoption of blockchain technology with accounting systems will involve a significant transformation of the traditional accounting systems, with the requirement of modifications of the work of accountants and auditors [35]. Also, the adoption will aim to address various risks associated with the data security and privacy [36]. On the other hand, the employment of blockchain technology in accounting systems guarantee to reduce the cost of the business organization, add additional security layer, and eliminate the possibility to loss information.

In addition, the blockchain technology is the underlying of accounting systems, and the blockchain technology has offered several benefits to the business and accounting systems, since all transactions in the

blockchain are distributed on the network and encrypted, making it impossible to falsify, delete or modify them [37].

8. Conclusion

Over the past decade, the blockchain technology has attracted a large attention from industry and academic fields, because it can be combined with many of everyday applications of modern information and communication technologies. In general, accountants aim to ensure that the financial transactions for their company are precise and without errors. As a result, the blockchain technology showed a great potential for enhancing the trust between market participants. In addition, blockchain technology has offered several benefits to the accounting area, by allowing the financial transactions to more transparent, permanent, secure, and immutable. Therefore, our findings can be summarized as follows:

1. Blockchain technology can assist in protecting the accounting systems
2. Several challenges may appear when employing the blockchain technology in accounting systems.
3. Adoption of blockchain technology will reduce the management cost for the organization.
4. The employment of machine learning and deep learning approaches will significantly enhance the fraud detection and classification accuracy.

References

[1] Nugraheni, B.L.Y., Cummings, L.S. and Kilgore, A., 2022. The localised accounting environment in the implementation of fair value accounting in Indonesia. *Qualitative Research in Accounting & Management*.

[2] Tarmidi, M., Rashid, A.A. and Abdullah, W.M.T.W., 2017. An analysis of computerized accounting system security threats in Malaysian public listed companies. *Terengganu International Finance and Economics Journal (TIFEJ)*, *2*(1), pp.28-35.

[3] Feng, Q., He, D., Zeadally, S., Khan, M.K. and Kumar, N., 2019. A survey on privacy protection in blockchain system. *Journal of Network and Computer Applications*, *126*, pp.45-58.

[4] Biktimirov, M.R., Domashev, A.V., Cherkashin, P.A. and Shcherbakov, A.Y., 2017. Blockchain technology: universal structure and requirements. *Automatic Documentation and Mathematical Linguistics*, *51*, pp.235-238.

[5] Dutta, P., Choi, T.M., Somani, S. and Butala, R., 2020. Blockchain technology in supply chain operations: Applications, challenges and research opportunities. *Transportation research part e: Logistics and transportation review*, *142*, p.102067.

[6] Ali, O., Jaradat, A., Kulakli, A. and Abuhalimeh, A., 2021. A challenges and functionalities. *Ieee Access*, *9*, pp.12730-12749.

[7] Yu, T., Lin, Z. and Tang, Q., 2018. Blockchain: The introduction and its application in financial accounting. *Journal of Corporate Accounting & Finance*, *29*(4), pp.37-47.

[8] Zheng, Z., Xie, S., Dai, H.N., Chen, X. and Wang, H., 2018. Blockchain challenges and opportunities: A survey. *International journal of web and grid services*, *14*(4), pp.352-375.

[9] Liu, M., Wu, K. and Xu, J.J., 2019. How will blockchain technology impact auditing and accounting: Permissionless versus permissioned blockchain. *Current Issues in auditing*, *13*(2), pp.A19-A29.

[10] Dai, J. and Vasarhelyi, M.A., 2017. Toward blockchain-based accounting and assurance. *Journal of information systems*, *31*(3), pp.5-21.

[11] Kwilinski, A., 2019. Implementation of blockchain technology in accounting sphere. *Academy of Accounting and Financial Studies Journal*, *23*, pp.1-6.

[12] Zhang, K. and Jacobsen, H.A., 2018. Towards Dependable, Scalable, and Pervasive Distributed Ledgers with Blockchains (Technical Report).

[13] Hassan, M.U., Rehmani, M.H. and Chen, J., 2022. Anomaly detection in blockchain networks: A comprehensive survey. *IEEE Communications Surveys & Tutorials*.

[14] Kim, J., Nakashima, M., Fan, W., Wuthier, S., Zhou, X., Kim, I. and Chang, S.Y., 2021, May. Anomaly detection based on traffic monitoring for secure blockchain networking. In *2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)* (pp. 1-9). IEEE.

[15] Rabieinejad, E., Yazdinejad, A. and Parizi, R.M., 2021, October. A deep learning model for threat hunting in ethereum blockchain. In *2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)* (pp. 1185-1190). IEEE.

[16] Vujičić, D., Jagodić, D. and Ranđić, S., 2018, March. Blockchain technology, bitcoin, and Ethereum: A brief overview. In *2018 17th international symposium infoteh-jahorina (infoteh)* (pp. 1-6). IEEE.

[17] Baek, H., Oh, J., Kim, C.Y. and Lee, K., 2019, July. A model for detecting cryptocurrency transactions with discernible purpose. In *2019 Eleventh International Conference on*

Ubiquitous and Future Networks (ICUFN) (pp. 713-717). IEEE.

[18] Ashfaq, T., Khalid, R., Yahaya, A.S., Aslam, S., Azar, A.T., Alsafari, S. and Hameed, I.A., 2022. A Machine Learning and Blockchain Based Efficient Fraud Detection Mechanism. *Sensors*, *22*(19), p.7162.

[19] Ibrahim, R.F., Elian, A.M. and Ababneh, M., 2021, July. Illicit account detection in the ethereum blockchain using machine learning. In *2021 International Conference on Information Technology (ICIT)* (pp. 488-493). IEEE.

[20] Kumar, N., Singh, A., Handa, A. and Shukla, S.K., 2020. Detecting malicious accounts on the Ethereum blockchain with supervised learning. In *Cyber Security Cryptography and Machine Learning: Fourth International Symposium, CSCML 2020, Be'er Sheva, Israel, July 2–3, 2020, Proceedings 4* (pp. 94-109). Springer International Publishing.

[21] Ning, Z., Sun, S., Wang, X., Guo, L., Wang, G., Gao, X. and Kwok, R.Y., 2021. Intelligent resource allocation in mobile blockchain for privacy and security transactions: a deep reinforcement learning based approach. *Science China Information Sciences*, *64*(6), p.162303.

[22] Dey, S., 2018, September. Securing majority-attack in blockchain using machine learning and algorithmic game theory: A proof of work. In *2018 10th computer science and electronic engineering (CEEC)* (pp. 7-10). IEEE.

[23] Podgorelec, B., Turkanović, M. and Karakatič, S., 2019. A machine learning-based method for automated blockchain transaction signing including personalized anomaly detection. *Sensors*, *20*(1), p.147.

[24] Chen, T., 2022, April. Blockchain and Accounting Fraud Prevention: A Case Study on Luckin Coffee. In *2022 7th International Conference on Social Sciences and Economic Development (ICSSED 2022)* (pp. 44-49). Atlantis Press.

[25] Cai, Y. and Zhu, D., 2016. Fraud detections for online businesses: a perspective from blockchain technology. *Financial Innovation*, *2*, pp.1-10.

[26] Tan, B.S. and Low, K.Y., 2019. Blockchain as the database engine in the accounting system. *Australian Accounting Review*, *29*(2), pp.312-318.

[27] Ostapowicz, M. and Żbikowski, K., 2019. Detecting fraudulent accounts on blockchain: a supervised approach. In *Web Information Systems Engineering–WISE 2019: 20th International Conference, Hong Kong, China, January 19–22, 2020, Proceedings 20* (pp. 18-31). Springer International Publishing.

[28] Huerta, E. and Jensen, S., 2017. An accounting information systems perspective on data analytics and Big Data. *Journal of information systems*, *31*(3), pp.101-114.

[29] Dunk, A.S., 2004. Product life cycle cost analysis: the impact of customer profiling, competitive advantage, and quality of IS information. *Management accounting research*, *15*(4), pp.401-414.

[30] 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.

[31] ALKAN, B.Ş., 2021. Real-time Blockchain accounting system as a new paradigm. *Muhasebe ve Finansman Dergisi*, pp.41-58.

[32] Demirkan, S., Demirkan, I. and McKee, A., 2020. Blockchain technology in the future of business cyber security and accounting. *Journal of Management Analytics*, *7*(2), pp.189-208.

[33] Bonsón, E. and Bednárová, M., 2019. Blockchain and its implications for accounting and auditing. *Meditari Accountancy Research*, *27*(5), pp.725-740.

[34] Oladejo, M.T. and Jack, L., 2020. Fraud prevention and detection in a blockchain technology environment: challenges posed to forensic accountants. *International Journal of Economics and Accounting*, *9*(4), pp.315-335.

[35] Pascual Pedreño, E., Gelashvili, V. and Pascual Nebreda, L., 2021. Blockchain and its application to accounting. *Intangible Capital*, *17*(1), pp.1-16.

[36] Fuller, S.H. and Markelevich, A., 2020. Should accountants care about blockchain?. *Journal of Corporate Accounting & Finance*, *31*(2), pp.34-46.

[37] Abad-Segura, E., Infante-Moro, A., González-Zamar, M.D. and López-Meneses, E., 2021. Blockchain technology for secure accounting management: research trends analysis. *Mathematics*, *9*(14), p.1631.

Rania M. Alsulami received her Bachelor Degree in Major Accounting from the University of Tabuk, 2019. In the mid of 2019, Rania joined the Faculty of Business Administration at the University of Tabuk, and worked as a teacher assistant for almost one year. At the meanwhile, Rania acts as a Financial Accountant in the private sector in Tabuk city since June 20th 2021 until now. Rania holds a CME-1 certificates. Her research interests including Blockchain technology in accounting and Finance.

Raghad M. Albalawi received the Bachelor Degree in Major Accounting from Tabuk University In 2020, She working in Astra Company in tabuk as general Accountant since 2020, She is a member in Saudi organization for chartered and professional accountant. Her research interests including Blockchain technology in accounting and auditing and Finance.

Hetaf A. Alsugair received the Bachelor Degree in Law from Tabuk University In 2020, She is now a master's researcher in forensic accounting, her research interests are the employment of artificial intelligence tools in law.

Manal F. Albalawi Trainee lawyer, BA in Law 2019, master's researcher, forensic accountant, writer, interested in artificial intelligence and law in different countries.

ADEL R. ALHARBI received the B.S. degree in computer science from Qassim University, Saudi Arabia, in 2008, and the M.S. degrees in security engineering and computer engineering and the Ph.D. degree in computer engineering from Southern Methodist University, Dallas, TX, USA, in 2013, 2015, and 2017, respectively. He has been a Faculty Staff Member with the Col-lege of Computing and Information Technology, University of Tabuk, Saudi Arabia, since 2009.

Khaled A. Alblowi received the PhD degree in Accounting from University of Hull, UK, in 2018. He joined the Faculty of Business Administration, University of Tabuk, Tabuk, Saudi Arabia, as a lecturer, in 2012. After receiving his PhD, he took the post of assistant professor at the same university. He has also taken a chair as the head of accounting department, as well as the faculty's vice dean for graduate studies and scientific research until now. His research interests include, but not limited to, investment and lending decision making modeling, strategic costing systems, new management accounting techniques, knowledge-based assets, environmental accounting, forensic accounting.