ARCHAIA JOURNAL OF SCIENCE AND TECHNOLOGY
VOL. 2, NO. 2, June 2025
https://doi.org/10.48161/ajst.v2n2a89

Blockchain Analytics for Cryptocurrency Transaction Risk Assessment in Forensic Accounting and Audit

Rafia Mukhtar[1*], Rizwan Hameed[2], Muhammad Safdar Bhatti[3]

[1] Information Technology, Faculty of Computing, The Government Sadiq College University, Bahawalpur, Pakistan;
[2] Computer Science, School of Computing, Gold Campus, Superior University, Lahore, Pakistan.
[3] Software Engineering, Computing Faculty, The Islamia University of Bahawalpur, Bahawalpur, Pakistan.

*** Corresponding author:** Onlineaccadmy07@gmail.com**.**

ABSTRACT: This research examines whether blockchain transaction records can support forensic accounting and audit assurance by classifying cryptocurrency transactions according to illicit risk patterns. The analysis uses the Elliptic Bitcoin transaction dataset, which contains transaction labels, transaction links, 49 anonymized time steps, and 166 anonymized numerical features. The empirical period runs from Time Step 1 to Time Step 49 because the dataset does not disclose calendar dates. The literature and contextual discussion are limited to studies available through 2022. The proposed method combines data preparation, class structure analysis, time step trend analysis, network relationship analysis, correlation screening, and supervised classification. Labeled transactions are divided chronologically, with earlier time steps used for training and later time steps used for testing. We evaluate Logistic Regression, Decision Tree, and Random Forest models using accuracy, balanced accuracy, precision, recall, F1 score, and ROC AUC. The findings show that illicit transactions make up only 9.76% of the labeled sample and that illicit risk ratios vary across blockchain time steps. Network links also show that licit, illicit, and unknown transactions are connected within the transaction graph. Random Forest provides the strongest screening result, with ROC AUC of 0.9199 and F1 score of 0.5416. The study concludes that blockchain analytics can help auditors prioritize suspicious transactions, but final fraud judgments still require professional evidence and review for careful, practical audit work.

Keywords: blockchain; forensic accounting; audit assurance; cryptocurrency transactions; machine learning.

I. INTRODUCTION

Blockchain technology has changed the way digital transactions are recorded, transferred, and verified. Because cryptocurrency transactions are stored on a public ledger, auditors can inspect blockchain data for transaction flows, address relationships, and risk patterns. Early Bitcoin studies showed that researchers can analyze public blockchain records through graph and transaction-tracing methods [1-6]. This transparency gives auditors and forensic accountants new forms of digital evidence, but it also creates new challenges because criminal users may rely on pseudonymity, complex transfer paths, and mixing behavior [3, 5, 20].

In accounting and auditing, blockchain is often discussed as a technology that may support real-time record verification, continuous assurance, and smart contract-based controls [10, 12, 14, 17-19, 22, 23]. However, accounting assurance does not depend only on the existence of a blockchain record. Auditors must still assess whether transactions are legitimate, complete, properly classified, and free from material fraud risk [11, 18, 26]. Therefore, blockchain-based audit assurance requires analytical procedures that can identify suspicious transaction behavior and prioritize transactions for professional review.

This study addresses the problem that cryptocurrency transaction data contain both legitimate and illicit activity, but illicit transactions are rare and difficult to detect. This creates a forensic accounting problem

because missing suspicious transactions may increase audit risk, while investigating every transaction is inefficient. Prior studies in blockchain analytics and financial forensics show that transaction networks and machine learning can help detect scams, Ponzi schemes, money laundering, and ransomware activity [9, 15, 21, 24, 29]. Yet these technical methods still need to connect with forensic accounting and audit assurance practice.

This study assesses whether blockchain transaction features and network relationships can classify transaction risk and support audit risk screening. Specifically, the study analyzes class imbalance, time-step risk trends, transaction-link relationships, feature correlations, and model performance using the Elliptic Bitcoin transaction dataset [30]. The literature review, theoretical background, and contextual discussion are limited to 2022; the empirical data is defined as anonymized Time Step 1 to Time Step 49 because the dataset does not disclose exact calendar dates.

The paper is structured as follows. Section II reviews related work and compares 29 studies published from 2013 to 2021. Section III explains the data, proposed method, research design, variables, and modeling procedures. Section IV presents the empirical analysis, charts, tables, diagrams, and model results. Section V concludes with implications, limitations, and future research directions.

II. LITERATURE REVIEW

The reviewed literature falls into three related streams. The first stream focuses on Bitcoin transaction graphs, anonymity, scams, and illicit financial flows. Early studies showed that Bitcoin and other blockchain transactions are not completely hidden, because transaction records are publicly available and can be examined through address clustering, network mapping, and transaction-flow analysis [1-6]. These studies established that blockchain data can be used for empirical tracing, even when users operate under pseudonymous addresses. Later research expanded this area by studying investment fraud, Ponzi schemes, ransomware payments, cryptocurrency crime, and broader Bitcoin market structures [9, 15, 20, 24, 29]. This line of research matters for forensic accounting because it shows that blockchain transactions can provide digital evidence of fund movement, relationships between addresses, and potential concentrations of suspicious activity. Therefore, this stream provides the technical foundation for using blockchain transaction data as evidence in fraud investigation and transaction-risk assessment.

The second stream focuses on the accounting and audit implications of blockchain. These studies argue that blockchain may influence accounting information systems, transaction verification, continuous assurance, triple-entry accounting, and smart-contract audit procedures [10-14, 17-19, 22, 23, 25-28]. In accounting practice, blockchain may improve the visibility and reliability of transaction records by creating a shared ledger that is difficult to alter after confirmation. This has encouraged researchers to discuss blockchain as a possible tool for improving audit trails, reducing reconciliation problems, and supporting more timely assurance procedures. However, the literature also emphasizes that blockchain records do not automatically satisfy all audit assertions. A transaction may be recorded on chain but still be economically suspicious, misclassified, unsupported by real business activity, or linked to illicit behavior [11, 18, 26]. For this reason, auditors still need professional judgment, risk assessment procedures, and analytical tools to evaluate the meaning and reliability of blockchain-based transactions.

The third stream uses data analytics and machine learning for financial forensics. Studies on Ponzi schemes, anti-money laundering, ransomware, and graph learning show that transaction characteristics and network structure can help identify suspicious activity patterns [15, 16, 20, 21, 24]. These studies are relevant because illicit blockchain activity is often difficult to detect through simple observation, especially when suspicious transactions represent only a small proportion of total activity. Data-driven methods can support forensic accountants by ranking transactions by risk, identifying unusual patterns, and reducing the number of transactions requiring manual review. At the same time, these methods should not be treated as final proof of fraud, because classification results depend on data quality, model design, and the interpretation of risk indicators. This study connects this stream to the accounting and auditing literature by treating model output as a transaction-risk screening tool for forensic accounting and audit assurance, rather than conclusive evidence of fraud.

Table 1. Comparison of studies.

No.	Study	Focus and method	Key finding and link with current study
1	Ron & Shamir (2013)	Full Bitcoin transaction graph. Method: Network/graph analysis.	Demonstrated that Bitcoin flows can be quantitatively traced through public ledger data. Supports using blockchain network data as audit evidence.
2	Meiklejohn et al. (2013)	Bitcoin payments and users. Method: Address clustering and payment tracing.	Showed that pseudonymous Bitcoin activity can be linked through transaction behavior. Supports forensic identification logic in transaction monitoring.
3	Moser et al. (2013)	Bitcoin money laundering tools. Method: Empirical investigation.	Identified laundering services and showed how blockchain data may reveal suspicious flows. Connects blockchain analytics with modeling and forensic accounting.
4	Spagnuolo et al. (2014)	Bitcoin intelligence extraction. Method: Blockchain parsing and visualization.	Presented tools for clustering, labeling, and visualizing Bitcoin users and transactions. Supports graph diagrams and transaction-link analysis.
5	Vasek & Moore (2015)	Bitcoin scams. Method: Empirical scam tracking.	Tracked virtual-currency scams and showed that scam profits can be measured on-chain. Shows how blockchain evidence can support fraud investigation.
6	Lischke & Fabian (2016)	Early Bitcoin network. Method: Network and transaction analysis.	Analyzed early Bitcoin structure and transaction growth over the first years. Supports descriptive analysis of blockchain transaction patterns.
7	Peters & Panayi (2016)	Banking ledgers and blockchain. Method: Conceptual analysis.	Explained blockchain as a future transaction-processing and smart contract infrastructure. Provides financial-system context for audit assurance.
8	Atzei et al. (2017)	Ethereum smart contracts. Method: Security survey.	Classified major smart contract attack types and vulnerabilities. Shows that blockchain systems create new audit and control risks.
9	Toyoda et al. (2017)	Bitcoin high-yield investment programs. Method: Pattern analysis.	Used transaction patterns to identify fraudulent investment schemes. Supports transaction-pattern screening for forensic accounting.
10	Dai & Vasarhelyi (2017)	Blockchain-based accounting and assurance. Method: Conceptual framework.	Argued that blockchain can transform accounting records and continuous assurance. Directly motivates audit-assurance use of blockchain data.
11	Coyne & McMickle (2017)	Accounting purpose of blockchains. Method: Conceptual critique.	Discussed limits of blockchain for accounting information and verification. Supports cautious interpretation of blockchain evidence.
12	Kokina et al. (2017)	Industry adoption and accounting. Method: Exploratory/conceptual study.	Discussed emerging adoption and implications for accounting practice. Links technical blockchain adoption to accounting change.
13	O'Leary (2017)	Blockchain architectures in accounting and supply chains. Method: Architecture analysis.	Explored how consortium architectures affect transaction information systems. Supports network and system-design considerations in audit.
14	Yu et al. (2018)	Blockchain in financial accounting. Method: Conceptual application.	Explained blockchain introduction and possible applications in financial accounting. Provides theoretical accounting background.
15	Bartoletti et al. (2018)	Bitcoin Ponzi schemes. Method: Data mining.	Detected Ponzi schemes using transaction and behavioral indicators. Supports supervised risk classification of suspicious transactions.

No.	Study	Focus and method	Key finding and link with current study
16	Demetis (2018)	Technology and anti-money laundering. Method: Case study.	Showed the importance and limits of technology in a modeling practice. Frames blockchain risk models as support tools, not final proof.
17	Bonson & Bednarova (2019)	Blockchain implications for accounting and auditing. Method: Literature/conceptual review.	Identified opportunities and challenges for accounting and auditing. Strengthens the accounting and audit framing of the study.
18	Schmitz & Leoni (2019)	Accounting and auditing at blockchain time. Method: Research agenda.	Outlined a research agenda for accounting and auditing under blockchain technology. Shows the academic gap addressed by empirical risk analysis.
19	Rozario & Thomas (2019)	Audit reengineering with blockchain and smart contracts. Method: Conceptual design.	Proposed using blockchain and smart contracts to redesign audit processes. Supports continuous audit risk screening logic.
20	Foley et al. (2019)	Illegal activity in cryptocurrencies. Method: Econometric blockchain analysis.	Estimated illegal activity financed through cryptocurrency markets. Supports the relevance of illicit-risk detection.
21	Weber et al. (2019)	A modeling in Bitcoin; Elliptic data. Method: Graph learning and modeling.	Introduced experiments on the Elliptic transaction graph for financial forensics. Closest technical foundation for the dataset and classification task.
22	Bonyuet (2020)	Blockchain impact on auditing. Method: Review paper.	Reviewed audit opportunities, risks, and procedure changes from blockchain. Supports audit-assurance interpretation of model results.
23	Pimentel & Boulianne (2020)	Blockchain in accounting research and practice. Method: Literature review.	Synthesized current trends and future opportunities in accounting blockchain research. Positions this study in accounting research.
24	Akcora et al. (2020)	Ransomware on Bitcoin. Method: Topological data analysis.	Used blockchain topology to predict ransomware-related transactions. Supports network features for risk screening.
25	Fullana & Ruiz (2021)	Accounting information systems in the blockchain era. Method: Literature/theoretical review.	Discussed how blockchain reshapes accounting information systems. Links data architecture to accounting systems.
26	Cai (2021)	Triple-entry accounting with blockchain. Method: Critical review.	Reviewed progress and limitations of blockchain-based triple-entry accounting. Supports the audit-evidence and accounting-record discussion.
27	Garanina et al. (2021)	Blockchain in accounting research. Method: Bibliometric/topic analysis.	Mapped research trends and emerging topics in blockchain accounting. Shows how the current topic fits the literature stream.
28	Secinaro et al. (2021)	Blockchain in accounting, auditing and accountability. Method: Bibliometric and coding analysis.	Analyzed the development of blockchain research across accounting-related fields. Supports the need for empirical studies in audit and accountability.
29	Makarov & Schoar (2021)	Bitcoin market structure. Method: Blockchain market analysis.	Used blockchain data to study Bitcoin market participants and flows. Supports the value of blockchain analytics for financial evidence.

The comparison shows a shift from Bitcoin tracing and fraud detection to blockchain accounting, audit assurance, and machine-learning financial forensics. This study connects these areas by using labeled blockchain data to assess transaction risk.

III. MATERIAL AND METHOD

1. DATA COLLECTION

The study uses secondary blockchain transaction data from the Elliptic Bitcoin transaction dataset [30]. The dataset contains transaction classes, transaction links, 49 anonymized time steps, and 166 anonymized numerical transaction features. Class 1 is treated as illicit, class 2 is treated as licit, and unknown transactions are retained for descriptive context but excluded from supervised model training.

The empirical study period runs from Time Step 1 to Time Step 49. The dataset does not disclose exact calendar dates. Therefore, this paper does not claim that the transaction data directly covers calendar years through 2022. Instead, we use 2022 as the reference boundary for the literature review, theoretical framing, and contextual discussion.

Table 2. Dataset summary.

Metric	Value
Total transactions	203,769
Labeled transactions used in modeling	46,564
Unknown transactions kept for context	157,205
Transaction links / edges	234,355
Time-step range	1 to 49
Anonymized transaction features	166
Network features added	in_degree, out_degree, total_degree, degree_balance

The dataset is large enough for transaction risk modeling and includes both individual transaction features and network link information.

2. PROPOSED METHOD

The proposed method follows a practical audit screening sequence. It begins by defining the empirical boundary and preparing transaction labels, then examines class structure, temporal dynamics, and network relationships before building supervised classification models. The final step interprets the model results as audit risk indicators that guide further professional review.

Table 3. Proposed method for blockchain transaction risk assessment.

Step	Stage	Procedure	Output
1	Define the empirical period	Use Time Step 1 to Time Step 49 because the transaction dates are anonymized.	Clear study boundary
2	Prepare transaction labels	Treat class 1 as illicit, class 2 as licit, and keep unknown transactions for descriptive context.	Usable labeled sample
3	Describe class and time patterns	Measure class imbalance and observe how illicit ratios change over time.	Initial risk profile
4	Add network indicators	Calculate in-degree, out-degree, total degree, and degree balance from transaction links.	Graph-based audit context
5	Screen related variables	Rank transaction features by their correlation with the illicit label.	Focused model inputs
6	Train and test models	Use earlier time steps for training and later time steps for testing.	Realistic screening design
7	Evaluate performance	Compare Logistic Regression, Decision Tree, and Random Forest with precision, recall, F1 score, and ROC AUC.	Best screening model
8	Interpret results for audit work	Use model outputs as risk indicators that guide evidence collection.	Audit review priority

The method connects blockchain analytics with audit practice by turning transaction patterns into review priorities.

3. RESEARCH DESIGN

This study follows a quantitative research design. The study uses Python for data preparation, descriptive analysis, network relationship analysis, correlation analysis, and supervised machine learning. The analysis first examines how transactions are distributed by class and time step, then evaluates relationships between transaction features, network degree variables, and the illicit label.

The supervised learning task uses only labeled transactions. We adopt a chronological training and testing design so that earlier time steps train the model and later time steps test it. This design imitates a real audit situation in which a model is trained on historical transactions and then used to screen later transactions.

Table 4. Chronological training and testing design.

Sample	Time steps	Transactions	Licit	Illicit	Illicit percentage
Training period	1-34	29,894	26,432	3,462	11.58
Testing period	35-49	16,670	15,587	1,083	6.50

Short explanation: The chronological design makes the testing stage more realistic because the model is evaluated on later blockchain time steps.

4. DATA ANALYSIS METHODS

The study uses Logistic Regression, Decision Tree, and Random Forest models. The analysis reports accuracy, balanced accuracy, precision, recall, F1 score, and ROC AUC. In forensic accounting, recall and F1 score are especially important because false negatives represent illicit transactions the screening model misses. We add network features, in-degree, out-degree, total degree, and degree balance, to capture the connected nature of blockchain transactions.

IV. DATA ANALYSIS

1. DATASET AND CLASS STRUCTURE

Table 5. Class distribution.

Class	Transactions	Percentage
Unknown	157,205	77.15
Licit	42,019	20.62
Illicit	4,545	2.23

Short explanation: Unknown transactions dominate the dataset, while illicit transactions are a small minority.

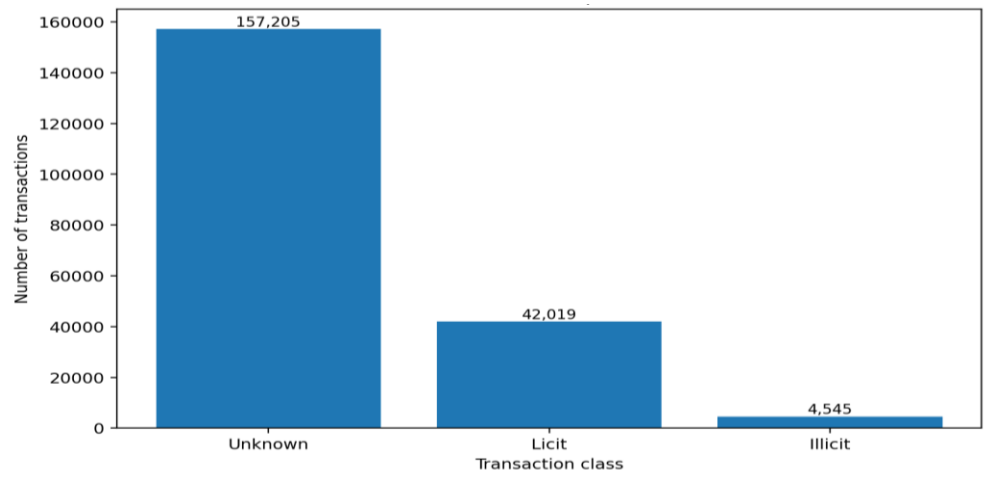


FIGURE 1. Class distribution of Elliptic transactions.

The chart confirms that most observations are unknown, so supervised model training must use only labeled licit and illicit observations.

Table 6. Labeled class distribution.

Labeled class	Transactions	Percentage of labeled data
Licit	42,019	90.24
Illicit	4,545	9.76

The labeled dataset is imbalanced because illicit transactions represent only 9.76 percent of labeled transactions.

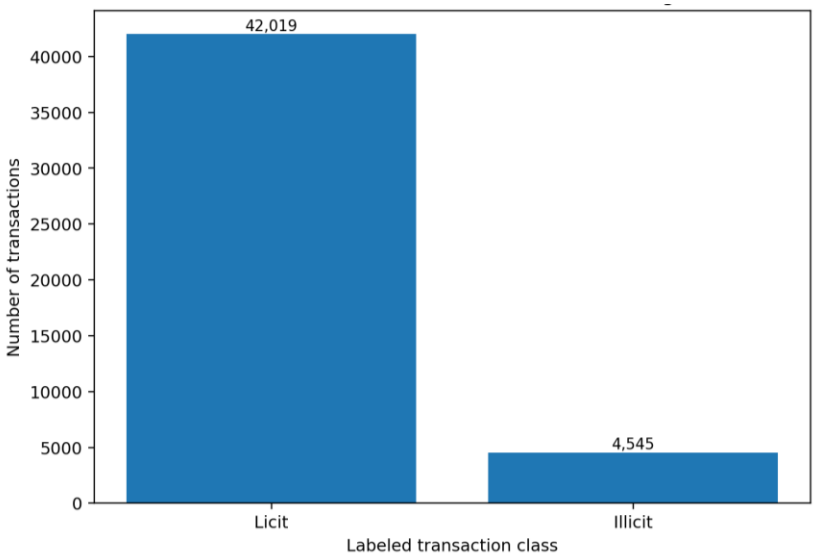


FIGURE 2. Labeled transactions used for modeling.

The imbalance reflects a realistic forensic accounting problem because suspicious transactions are rare compared with normal transactions.

2. TIME STEP RISK TREND

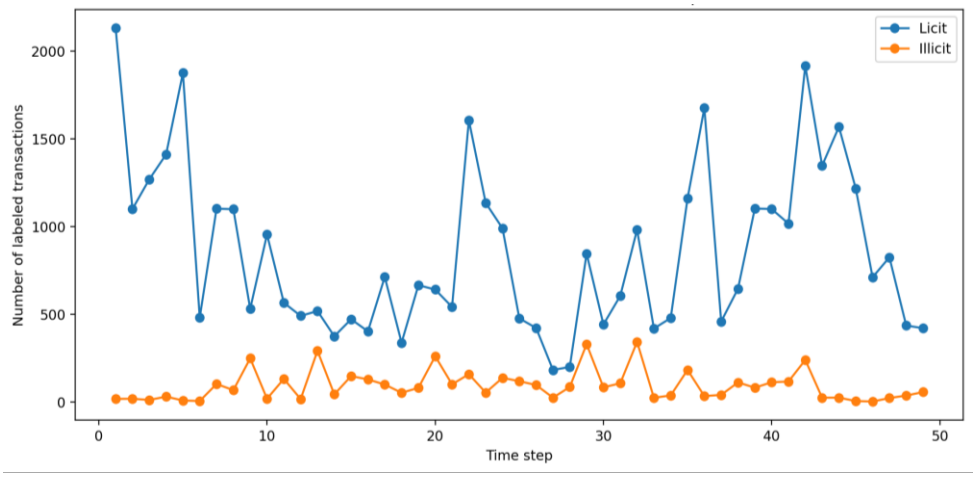


FIGURE 3. Labeled transaction counts across time steps.

The number of licit and illicit labeled transactions changes across blockchain time steps.

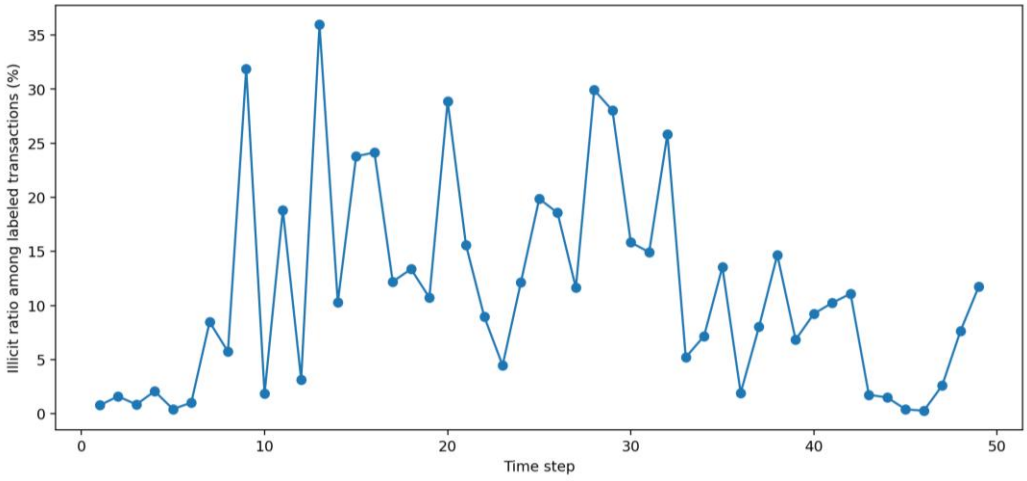


FIGURE 4. Illicit transaction ratio by time step.

The illicit ratio is not constant, supporting continuous monitoring rather than a one-time audit test.

Table 7. Selected illicit ratio by time step.

Time step	Licit	Illicit	Labeled total	Illicit ratio (%)
1	2,130	17	2,147	0.79
2	1,099	18	1,117	1.61
3	1,268	11	1,279	0.86
4	1,410	30	1,440	2.08
5	1,874	8	1,882	0.43
6	480	5	485	1.03
7	1,101	102	1,203	8.48
8	1,098	67	1,165	5.75
9	530	248	778	31.88

Time step	Licit	Illicit	Labeled total	Illicit ratio (%)
10	954	18	972	1.85
11	565	131	696	18.82
12	490	16	506	3.16
13	518	291	809	35.97
14	374	43	417	10.31
15	471	147	618	23.79
16	402	128	530	24.15
17	712	99	811	12.21
18	337	52	389	13.37

The table provides the numeric values behind the risk trend charts for the first 18 time steps; the full trend is shown in Figure 4.

3. NETWORK RELATIONSHIP ANALYSIS

Table 8. Network degree summary by class.

Class	In-degree mean	In-degree median	In-degree max	Out degree mean	Out degree median	Out-degree max	Total degree mean	Total degree median	Total degree max
Illicit	1.27	1.00	177	0.74	1.00	3	2.01	1.00	177
Licit	1.91	1.00	284	1.19	1.00	472	3.10	2.00	473
Unknown	0.94	1.00	212	1.15	1.00	122	2.10	2.00	212

Short explanation: Network degree describes how connected a transaction is; highly connected transactions may require closer audit review.

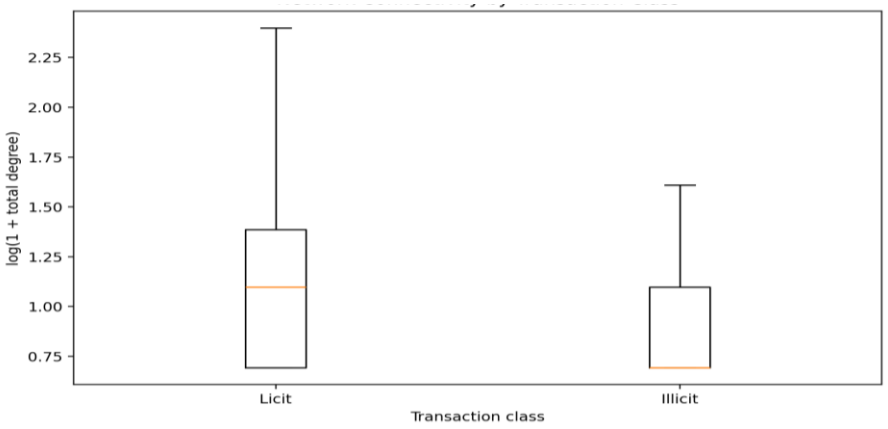


FIGURE 5. Network connectivity by transaction class.

The boxplot compares connectivity for licit and illicit transactions using log total degree.

Table 9. Class-to-class transaction link relationships.

Source class	Unknown	Licit	Illicit
Unknown	131,778	45,386	3,993
Licit	15,116	33,930	781
Illicit	1,458	915	998

The table shows how transaction links connect unknown, licit, and illicit groups in the blockchain graph.

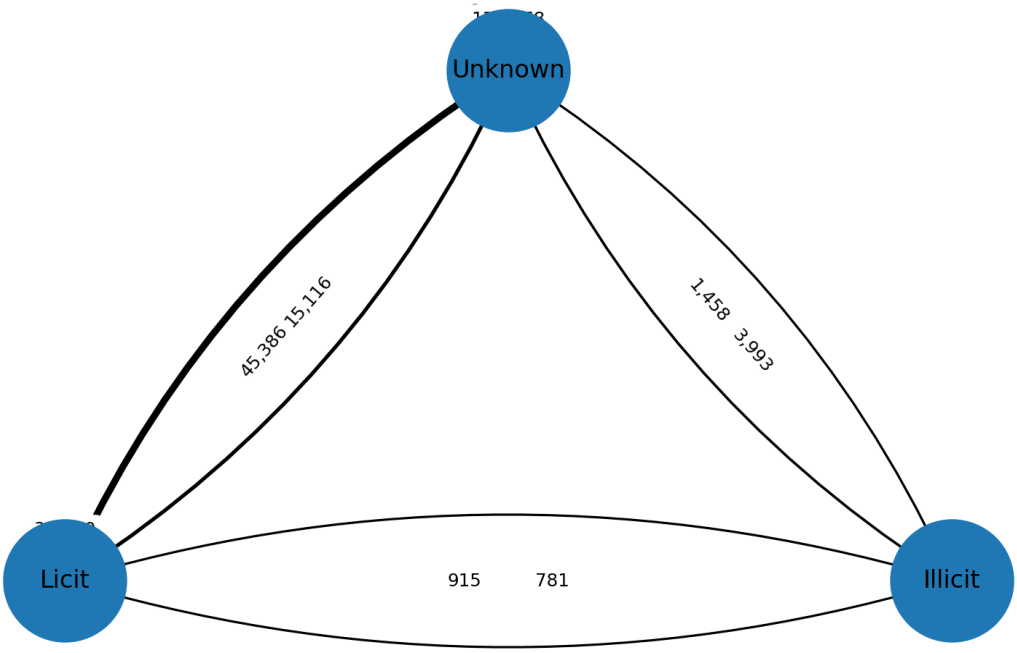


FIGURE 6. Aggregated transaction link network by class.

The diagram summarizes transaction links by class, making blockchain relationships easier to interpret for audit review.

4. VARIABLE RELATIONSHIP ANALYSIS

Table 10. Top variables correlated with illicit transactions.

Variable	Correlation with illicit label	Absolute correlation
feature_053	-0.2615	0.2615
feature_089	-0.2276	0.2276
feature_055	-0.2271	0.2271
feature_090	-0.2213	0.2213
feature_142	0.1919	0.1919
feature_150	-0.1872	0.1872
feature_091	-0.1858	0.1858
feature_052	-0.1718	0.1718
feature_154	0.1530	0.1530
feature_054	-0.1421	0.1421
feature_114	-0.1376	0.1376
feature_148	0.1359	0.1359
feature_156	-0.1352	0.1352
feature_083	-0.1234	0.1234
feature_085	-0.1191	0.1191
feature_077	-0.1180	0.1180
feature_084	-0.1174	0.1174
feature_059	-0.1141	0.1141

Variable	Correlation with illicit label	Absolute correlation
feature_065	-0.1141	0.1141
feature_079	-0.1126	0.1126

These variables have the strongest individual relationship with illicit classification, but correlation does not prove fraud or causation.

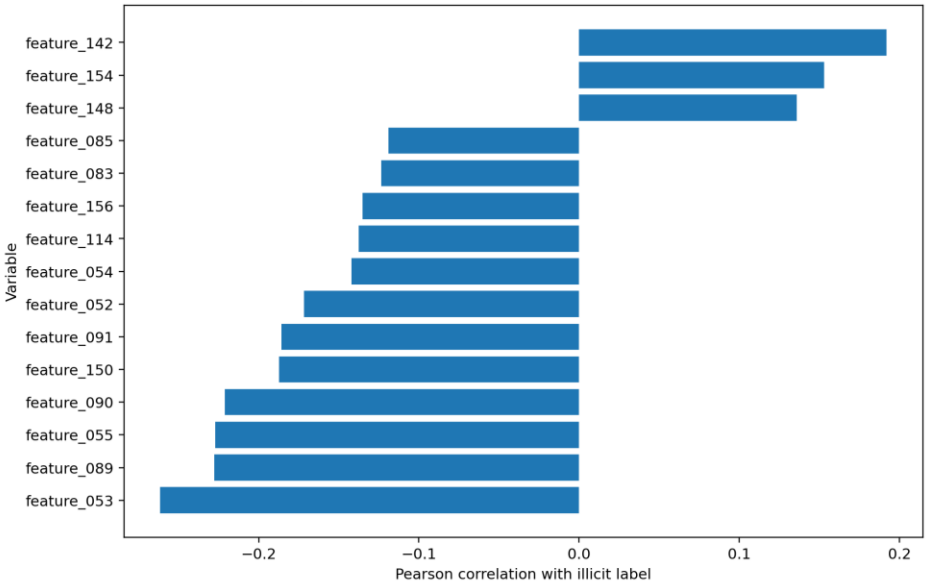


FIGURE 7. Top variable correlations with the illicit label.

Variables farther from zero have stronger statistical association with illicit transaction risk.

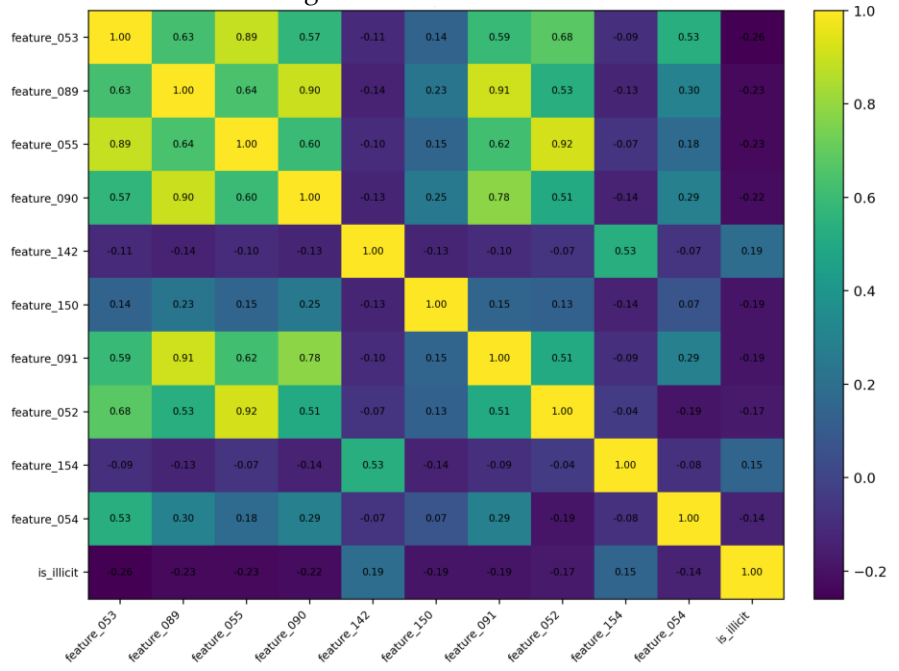


FIGURE 8. Correlation matrix of top risk-related variables.

The heatmap shows whether important variables move together and whether their information overlaps.

5. MACHINE LEARNING RISK CLASSIFICATION

Table 11. Model performance comparison.

Model	Accuracy	Balanced accuracy	Precision	Recall	F1 score	ROC AUC
Logistic Regression	0.6028	0.7163	0.1244	0.8467	0.2169	0.8631
Decision Tree	0.8524	0.8149	0.2741	0.7719	0.4045	0.9034
Random Forest	0.9181	0.8376	0.4254	0.7452	0.5416	0.9199

Random Forest gives the strongest overall balance in this run, especially on F1 score and ROC AUC.

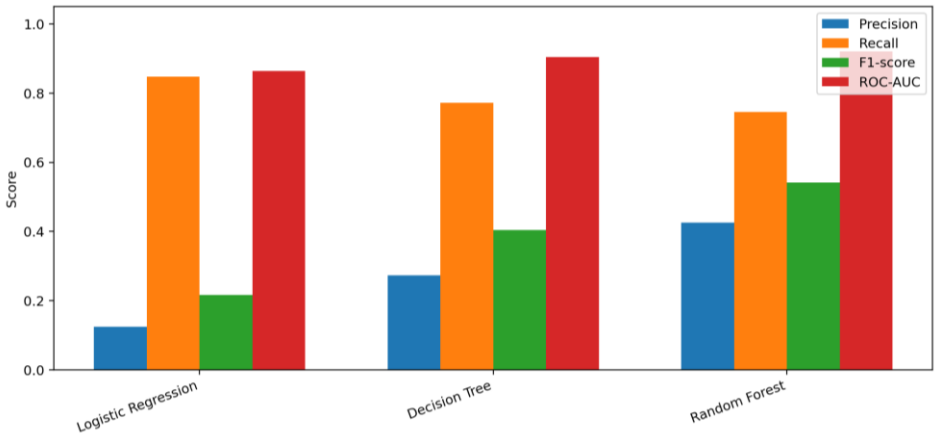


FIGURE 9. Model performance comparison for blockchain transaction risk classification.

The chart compares models using precision, recall, F1 score, and ROC AUC rather than accuracy alone.

Table 12. Confusion matrix for the best model.

Actual class	Predicted licit	Predicted illicit
Actual licit	14,497	1,090
Actual illicit	276	807

The confusion matrix shows correct and incorrect predictions for licit and illicit transactions.

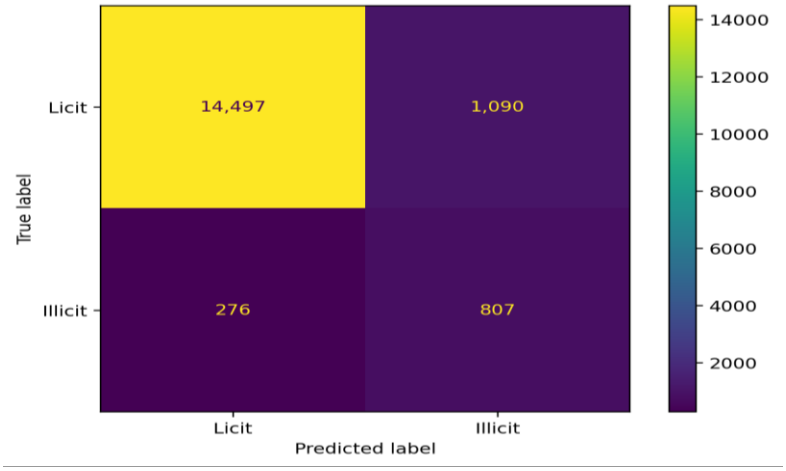


FIGURE 10. Confusion matrix for Random Forest.

For audit assurance, false negatives matter because they represent illicit transactions missed by the model.

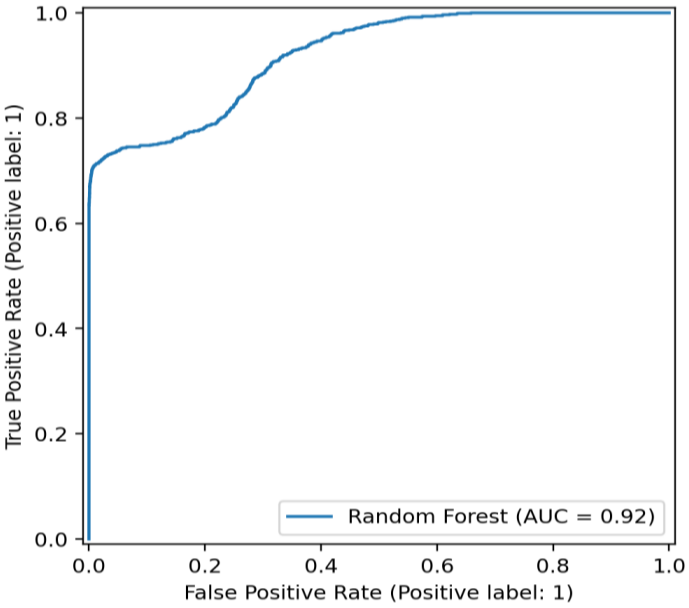


FIGURE 11. ROC curve for Random Forest.

The ROC curve shows how well the model separates licit and illicit transactions across thresholds.

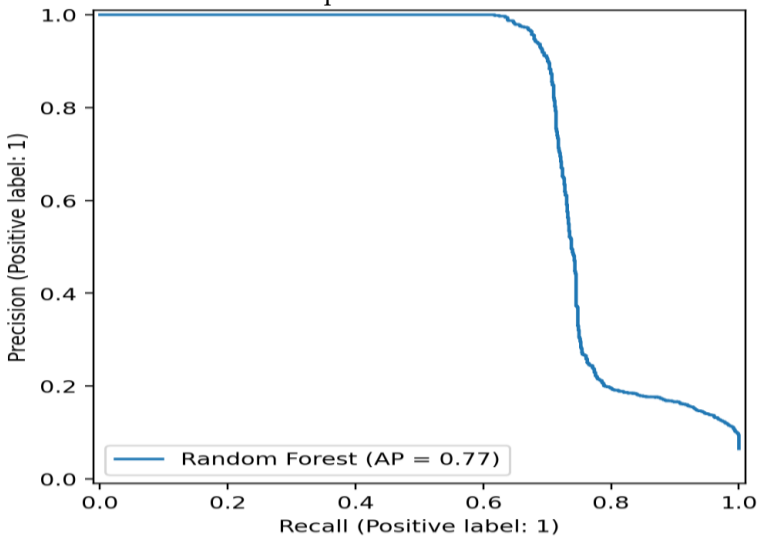


FIGURE 12. Precision-recall curve for Random Forest.

The precision-recall curve is useful because illicit transactions are rare in the data.

Table 13. Top model variables by importance.

Variable	Importance
feature_090	0.1507
feature_089	0.1469
feature_156	0.1405
feature_055	0.0835
feature_142	0.0678
feature_053	0.0519
feature_079	0.0437
feature_052	0.0420
feature_150	0.0418
feature_054	0.0401
feature_154	0.0331
feature_114	0.0314
feature_091	0.0287
feature_065	0.0217
feature_077	0.0180
feature_148	0.0176
feature_083	0.0107
feature_059	0.0093
out_degree	0.0058
feature_085	0.0044

These variables contributed most to Random Forest predictions; the dataset anonymizes the business meaning of individual features.

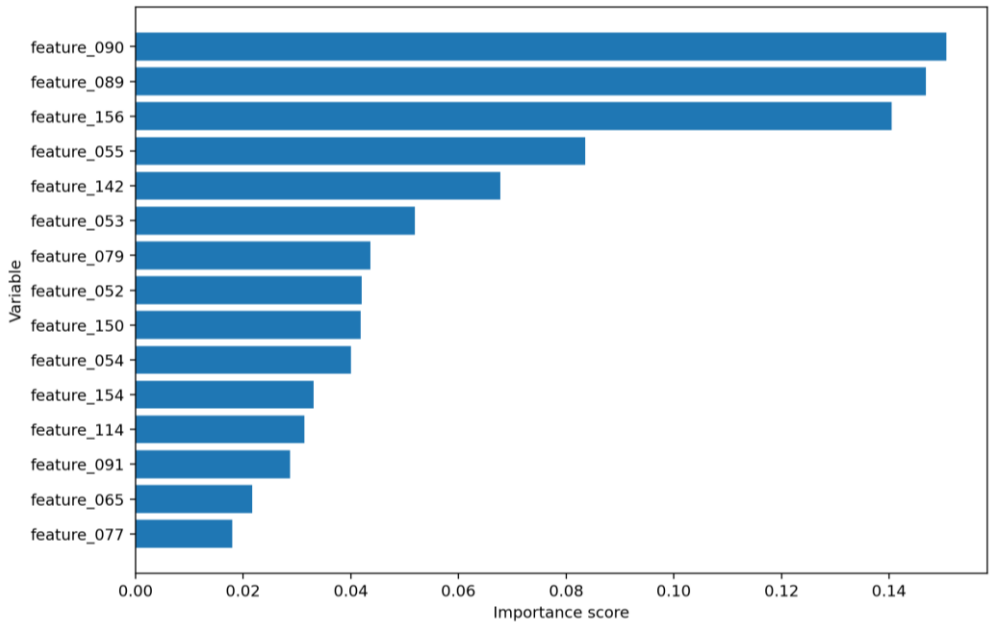


FIGURE 13. Top model variables by importance.

Important variables can guide auditors toward transactions and patterns that deserve closer investigation.

V. CONCLUSION

This study examined whether blockchain transaction records can strengthen forensic accounting and audit assurance by supporting transaction risk screening. Evidence from the Elliptic Bitcoin transaction dataset shows that illicit activity is rare, representing 9.76% of labeled observations, yet its distribution shifts across the 49 anonymized time steps. This pattern confirms that blockchain assurance should not depend on a single review point. Continuous monitoring is more suitable because suspicious activity may rise or fall across different transaction periods.

The network analysis shows that transactions are not isolated. Licit, illicit, and unknown observations connect through the Bitcoin transaction graph, so link relationships can provide useful context for audit review. Correlation analysis identifies several anonymized features that are statistically related to illicit labels, while the classification models show that transaction features and network indicators can separate licit and illicit transactions. Among the tested models, Random Forest performs best, with an ROC AUC of 0.9199 and an F1 score of 0.5416 at later time steps.

The findings support the use of blockchain analytics as an audit risk tool, not as final proof of fraud. Model outputs can help auditors select transactions that deserve evidence, documentation, and professional judgment. Such use can improve sampling decisions, reduce wasted review effort, and keep attention on transactions with higher audit concern. The study is limited by anonymized features and undisclosed calendar dates. Future research should test datasets with explicit dates through 2022 or later, compare additional graph-based models, and link blockchain risk scores to audit procedures, internal controls, and financial reporting assertions.

Author Contributions

The author conducted the conceptualization, methodology, data analysis, investigation, writing, review, editing, and final approval of the manuscript.

Funding

This research received no external funding.

Data Availability

The dataset will be available from the author upon reasonable request.

Conflicts of Interest

The author declares no conflict of interest.

REFERENCES

[1]. Ron, D., & Shamir, A. (2013). Quantitative analysis of the full Bitcoin transaction graph. In A.-R. Sadeghi (Ed.), Financial Cryptography and Data Security (pp. 6-24). Springer.
[2]. Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M., & Savage, S. (2013). A fistful of bitcoins: Characterizing payments among men with no names. Proceedings of the 2013 Internet Measurement Conference, 127-140.
[3]. Moser, M., Bohme, R., & Breuker, D. (2013). An inquiry into money laundering tools in the Bitcoin ecosystem. 2013 APWG eCrime Researchers Summit, 1-14.
[4]. Spagnuolo, M., Maggi, F., & Zanero, S. (2014). BitIodine: Extracting intelligence from the Bitcoin network. In Financial Cryptography and Data Security (pp. 457-468). Springer.
[5]. Vasek, M., & Moore, T. (2015). There is no free lunch, even using Bitcoin: Tracking the popularity and profits of virtual currency scams. In Financial Cryptography and Data Security (pp. 44-61). Springer.
[6]. Lischke, M., & Fabian, B. (2016). Analyzing the Bitcoin network: The first four years. Future Internet, 8(1), Article 7.
[7]. Peters, G. W., & Panayi, E. (2016). Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money. In P. Tasca, T. Aste, L. Pelizzon, & N. Perony (Eds.), Banking Beyond Banks and Money (pp. 239-279). Springer.
[8]. Atzei, N., Bartoletti, M., & Cimoli, T. (2017). A survey of attacks on Ethereum smart contracts. In Principles of Security and Trust (pp. 164-186). Springer.
[9]. Toyoda, K., Ohtsuki, T., & Mathiopoulos, P. T. (2017). Identification of high-yielding investment programs in Bitcoin via transaction pattern analysis. Proceedings of IEEE Global Communications Conference, 1-6.
[10]. Dai, J., & Vasarhelyi, M. A. (2017). Toward blockchain-based accounting and assurance. Journal of Information Systems, 31(3), 5-21.
[11]. Coyne, J. G., & McMickle, P. L. (2017). Can blockchains serve an accounting purpose? Journal of Emerging Technologies in Accounting, 14(2), 101-111.
[12]. Kokina, J., Mancha, R., & Pachamanova, D. (2017). Blockchain: Emergent industry adoption and implications for accounting. Journal of Emerging Technologies in Accounting, 14(2), 91-100.
[13]. O'Leary, D. E. (2017). Configuring blockchain architectures for transaction information in blockchain consortiums: The case of accounting and supply chain systems. Intelligent Systems in Accounting, Finance and Management, 24(4), 138-147.
[14]. Yu, T., Lin, Z., & Tang, Q. (2018). Blockchain: The introduction and its application in financial accounting. Journal of Corporate Accounting & Finance, 29(4), 37-47.
[15]. Bartoletti, M., Pes, B., & Serusi, S. (2018). Data mining for detecting Bitcoin Ponzi schemes. 2018 Crypto Valley Conference on Blockchain Technology, 75-84.
[16]. Demetis, D. S. (2018). Fighting money laundering with technology: A case study of Bank X in the UK. Decision Support Systems, 105, 96-107.
[17]. Bonson, E., & Bednarova, M. (2019). Blockchain and its implications for accounting and auditing. Meditari Accountancy Research, 27(5), 725-740.
[18]. Schmitz, J., & Leoni, G. (2019). Accounting and auditing at the time of blockchain technology: A research agenda. Australian Accounting Review, 29(2), 331-342.

[19]. Rozario, A. M., & Thomas, C. (2019). Reengineering the audit with blockchain and smart contracts. Journal of Emerging Technologies in Accounting, 16(1), 21-35.
[20]. Foley, S., Karlsen, J. R., & Putnins, T. J. (2019). Sex, drugs, and Bitcoin: How much illegal activity is financed through cryptocurrencies? The Review of Financial Studies, 32(5), 1798-1853.
[21]. Weber, M., Domeniconi, G., Chen, J., Weidele, D. K. I., Bellei, C., Robinson, T., & Leiserson, C. E. (2019). Anti-money laundering in Bitcoin: Experimenting with graph convolutional networks for financial forensics. KDD Workshop on Anomaly Detection in Finance.
[22]. Bonyuet, D. (2020). Overview and impact of blockchain on auditing. The International Journal of Digital Accounting Research, 20, 31-43.
[23]. Pimentel, E., & Boulianne, E. (2020). Blockchain in accounting research and practice: Current trends and future opportunities. Accounting Perspectives, 19(4), 325-361.
[24]. Akcora, C. G., Li, Y., Gel, Y. R., & Kantarcioglu, M. (2020). BitcoinHeist: Topological data analysis for ransomware prediction on the Bitcoin blockchain. Proceedings of the Twenty-Ninth International Joint Conference, 4439-4445.
[25]. Fullana, O., & Ruiz, J. (2021). Accounting information systems in the blockchain era. International Journal of Intellectual Property Management, 11(1), 63-80.
[26]. Cai, C. W. (2021). Triple-entry accounting with blockchain: How far have we come? Accounting & Finance, 61(1), 71-93.
[27]. Garanina, T., Ranta, M., & Dumay, J. (2021). Blockchain in accounting research: Current trends and emerging topics. Accounting, Auditing & Accountability Journal, 35(7), 1507-1533.
[28]. Secinaro, S., Dal Mas, F., Brescia, V., & Calandra, D. (2021). Blockchain in the accounting, auditing and accountability fields: A bibliometric and coding analysis. Accounting, Auditing & Accountability Journal, 35(9), 168-203.
[29]. Makarov, I., & Schoar, A. (2021). Blockchain analysis of the Bitcoin market. NBER Working Paper No. 29396.
[30]. Elliptic. (2019). Elliptic Data Set [Data set]. Kaggle.