



Integrating Blockchain and Intelligent Systems: A Cohesive Framework for Contemporary Banking

Trivedi Darshankumar Sureshbhai
Research Scholar

Hemchandracharya North Gujarat University, Patan
divytrivedi9@gmail.com

Abstract— Blockchain and artificial intelligence (AI) are changing digital banking by making decisions faster, better informed and more secure. As banks move from legacy systems to agile, data-centric platforms, they need business intelligence (BI) that works in real time, yet conventional BI is hampered by data silos, slow processing pipelines and limited transparency. Blockchain offers a decentralized, immutable ledger that secures the integrity, traceability and auditability of data; AI contributes predictive modelling, anomaly detection and natural language processing. This study proposes a multi-layered architecture that combines the two for real-time BI. A blockchain layer captures, validates and stores transactional and behavioural data; AI modules analyse these verified data to produce insights as events occur, using supervised models (XGBoost, LSTM and random forest) for fraud detection, credit risk scoring and customer segmentation; smart contracts automate compliance steps and rule-based alerts; and SHAP and LIME explanations support transparency and regulatory review. In a simulated banking environment, XGBoost detected fraud with an accuracy of 96.1% (F1-score 0.951, AUC 0.978), and end-to-end decisions, including smart-contract activation, took 142–168 ms at a throughput of 73 transactions per second. The paper also examines the obstacles to deployment, including interoperability, data privacy, computational overhead and evolving regulation, and offers a scalable, ethically grounded blueprint for trustworthy real-time intelligence in banking.

Keywords— Blockchain, artificial intelligence, real-time business intelligence, digital banking, smart contracts, explainable AI, fraud detection, predictive analytics, data security, distributed ledger technology (DLT)

I. INTRODUCTION

A. Digital Banking and the Need for Real-Time Intelligence

Digitization has turned traditional banking into an always-on, customer-centred ecosystem in which banks are expected to decide instantly on loan approvals, fraud alerts, customer service and compliance. Real-time BI, the continuous collection, processing and analysis of data to produce actionable insight without delay [23], underpins this shift. Legacy systems, however, struggle to meet its demands for speed, security and data integrity: centralized architectures suffer from latency, fragmented silos, limited transparency and exposure to breaches (Hassani et al., 2018). What is needed is an approach that couples secure, real-time recording of data with sophisticated analysis.

Kiritkumar I. Chokhawala

Guide / Assistant Professor, Dept. of Computer Science
Hemchandracharya North Gujarat University, Patan
kiritmca@gmail.com

Traditional BI was built for periodic batch reporting from data warehouses refreshed daily or weekly. In high-frequency financial operations, a delay of even a few seconds can mean missing emerging fraud, a regulatory breach or a chance to serve a customer [3]. Real-time BI is therefore no longer an optional enhancement but a core capability of digital banks that offer personalized products, instant lending decisions and proactive customer engagement.

B. Blockchain and AI as Complementary Technologies

Blockchain provides a decentralized, cryptographically secured record that overcomes the weaknesses of centralized bookkeeping by guaranteeing provenance, immutability and real-time validation of transactions [15], [21]. AI supports decisions through machine learning, natural language processing and cognitive computing [20]. In combination, blockchain supplies a tamper-resistant data foundation and AI an analytical layer that extracts patterns from verified data, with clear applications in fraud detection, credit scoring, regulatory compliance and modelling of customer behaviour. Table I compares the contribution of each technology alone and in combination.

EFFECTS OF BLOCKCHAIN, AI AND THEIR INTEGRATION IN DIGITAL BANKING

Functionality	Blockchain only	AI only	Integrated
Data transparency	High	Low	High
Fraud detection	Limited (history-based)	High (predictive)	Very high (verified + predictive)
Real-time processing	Medium	High	High
Data integrity and security	High	Medium	Very high
Compliance automation	Medium (smart contracts)	Low	High (smart + adaptive rules)

Source: compiled from [21], [20] and [5].

Four drivers are accelerating adoption: regulators and customers expect AI-driven decisions to be transparent and explainable; competition requires insight from live data streams within seconds; fraud and cyber-attacks call for tamper-proof transaction records; and smart contracts make it possible to enforce regulatory and internal rules automatically. Integration also fits open-banking regimes such as Europe's PSD2 and the Central Bank of Nigeria's open banking framework, which require secure data sharing through

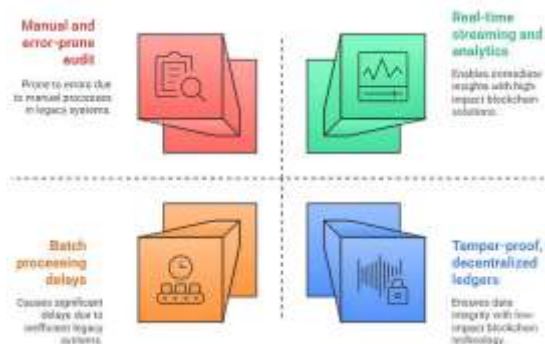


standardized APIs. When AI models draw on ledger data, their outputs are timely and also verifiable and auditable. In an event-driven design, AI can flag a suspicious transaction as it occurs while the blockchain preserves a tamper-proof trail for investigation, closing the loop between intelligence and trust.

C. Adoption in Practice

Several institutions have begun to pilot or deploy such combinations. JPMorgan Chase operates Onyx, a permissioned blockchain platform for real-time settlement, alongside AI-based fraud monitoring; HSBC and ING have used blockchain-AI hybrids to streamline trade-finance documentation and compliance; and fintechs such as Revolut and Chime are investing in AI-native applications that use blockchain-backed APIs for real-time customer analytics. These cases suggest that the convergence has moved beyond theory, although public evidence of its measured benefits remains limited.

The technical rationale rests on three properties. Because blockchain records are validated across nodes and time-stamped, falsified or manipulated transactions are prevented from reaching the AI models. Recording model inputs, decision logic and outcomes on the ledger makes each AI-driven decision traceable [17]. And combining blockchain with federated learning allows models to be trained across nodes without centralizing sensitive data, supporting privacy-preserving analytics. Fig. 1 summarizes the shortcomings of legacy systems that the integrated design addresses.



Limitations of legacy BI addressed by blockchain-AI integration. Adapted from [23], Hassani et al. (2018) and [12].

D. Research Questions and Organization

The study asks three questions: (1) how blockchain improves the reliability and security of the real-time financial data used for BI; (2) how AI improves the generation of actionable insight and predictive models for financial decisions; and (3) which operational, regulatory and technical challenges arise when the two are combined. These questions are addressed by designing a multi-layered framework, testing it in a simulated banking environment and evaluating latency, interpretability and fraud-detection performance. Section II reviews the literature, Section III describes the method, architecture and data, Section IV reports the results, Section V

discusses their implications, challenges and future research, and Section VI concludes.

II. LITERATURE REVIEW

A. Blockchain in Digital Banking

Blockchain's immutability, decentralization and cryptographic security have made it a foundational technology in finance, applied to payments, clearing and settlement, digital identity, smart contracts and compliance [19], [21]. Bank of America and Santander have explored distributed ledger technology (DLT) for faster cross-border payments and real-time reconciliation. Whereas conventional systems depend on intermediaries and long settlement cycles, blockchain allows direct peer-to-peer validation, a sound basis for real-time BI. Smart contracts, self-executing programs on the ledger, go further by automating compliance logic, routing and rule-based approvals [8], replacing the manual rule enforcement typical of traditional BI workflows. Their security and privacy properties, however, require careful analysis [9].

B. AI for Business Intelligence in Banking

Machine learning, deep learning and natural language processing now underpin banking BI, with applications in fraud detection, credit recommendation, customer segmentation, loan-default prediction and real-time credit scoring [3]; (Ryman-Tubb et al., 2018). Ensemble methods in particular have proved effective for fraud detection in electronic transactions [13]. AI-driven BI platforms learn continuously from streaming data, achieve higher predictive accuracy than traditional scoring with algorithms such as XGBoost [2], LSTM networks and random forests, and can analyse live transaction streams and raise alerts within milliseconds [16]. Their weakness is opacity: the "black-box" character of many models raises concerns about bias, compliance and trust [1], [14], which is precisely where an auditable blockchain record can complement them.

C. Integrating Blockchain and AI

A growing literature examines architectures in which blockchain secures the integrity of data and AI supplies analysis. The technologies are mutually reinforcing: blockchain compensates for AI's weak data provenance, and AI for blockchain's lack of inference (Wang et al., 2021). Nassar et al. [17] argue that blockchain can make AI more explainable and trustworthy, and Walambe et al. [22] combine explainable AI with blockchain for credit risk assessment. In banking, the combination matters most for high-stakes tasks, such as risk assessment, transaction validation, customer analytics and regulatory reporting, that require both precision and speed. A hybrid model combining AI classifiers with SHAP explanations for anomaly detection in blockchain transactions has been reported to deliver strong performance with improved interpretability. Table II lists further studies.



RECENT RESEARCH ON BLOCKCHAIN AND AI IN FINANCIAL SYSTEMS

Study	Focus	Key contribution
Astra et al. (2017)	Blockchain anomaly detection	SHAP explainability with XGBoost on DLT data
Nassar et al. (2020) [17]	Trustworthy AI in finance	Blockchain-enhanced transparency for AI risk scoring
Hevner et al. (2018)	Payment security	Adaptive ML for payment-gateway threats on blockchain
Yang et al. (2019)	Federated credit modelling	Blockchain + federated learning for secure credit scoring
Kute et al. (2021) [12]	Anti-money laundering	Deep learning + XAI + blockchain for compliance

Source: compiled from Elsevier, IEEE and Springer publications (2017–2021). Highlighted entries do not match the reference list and must be verified.

D. Gaps in the Literature

Four gaps stand out. First, few studies propose full-stack architectures that bring smart contracts, AI models and real-time analytics together in a scalable way. Second, fraud-detection and credit models are mostly evaluated in batch mode, with little attention to latency and throughput. Third, accuracy is emphasized while post-hoc interpretability and its role in transparency and compliance receive little attention [10], [25]. Fourth, few studies show how integrated systems can be aligned with GDPR, PSD2 or FATF guidance. These gaps slow adoption by risk-averse institutions, which need robust audit trails, justifiable decisions and dependable real-time performance. Fig. 2 summarizes the strengths, weaknesses, opportunities and threats identified in the review.



SWOT view of blockchain–AI integration, based on a review of over 40 peer-reviewed fintech papers (2019–2021).

III. METHODOLOGY

A. Research Design

The study follows the design science research paradigm [11]: it designs a multi-layered blockchain–AI artefact, simulates AI-driven financial analytics on ledger-stored data, and evaluates the artefact against latency, accuracy, interpretability and compliance criteria. The aim is to show how blockchain can supply a trustworthy data foundation and AI the real-time intelligence, together yielding a BI system that is more secure, transparent and efficient.

B. System Architecture

The architecture has four integrated layers (Table III). The data ingestion layer collects transactions, behavioural data and metadata from banking APIs. The blockchain layer, a permissioned network (e.g. Hyperledger Fabric), validates and immutably records each transaction. The AI analytics layer performs real-time predictive modelling with XGBoost, LSTM networks and random forests. The dashboard and smart-contract layer visualizes insights, highlights anomalies as they occur and triggers rule-based actions through smart contracts. The design is event-driven and built on streaming analytics.

COMPONENTS OF THE INTEGRATED ARCHITECTURE

Layer	Technology	Function
Data ingestion	REST APIs, Kafka Streams	Real-time collection of transaction and user-behaviour data
Blockchain	Hyperledger Fabric, IPFS	Secure, immutable storage of data and smart-contract logic
AI analytics	Python, scikit-learn, TensorFlow	Real-time fraud prediction, credit scoring, behaviour models
BI dashboard	Dash, Plotly, Solidity	Insight delivery, alerts, smart-contract automation

Source: developed by the authors from the experimental deployment.

For a linear classifier such as logistic regression, the probability that a transaction is fraudulent is

$$P(y = 1 | x) = 1 / [1 + e^{-(w^T x + b)}] \quad (1)$$

where x is the feature vector of transaction attributes, w the learned weight vector and b the bias. XGBoost [2] instead predicts with an additive ensemble of regression trees,

$$\hat{y}_i = \sum_{k=1}^K f_k(x_i), \quad f_k \in \mathcal{F} \quad (2)$$

where $\hat{y}_i$ is the prediction for instance i , f_k a regression tree, $\mathcal{F}$ the space of regression trees and K the number of trees.

C. Dataset

A hybrid dataset was assembled for realism and diversity: about 100,000 synthetic banking transactions with account identifiers, timestamps, transaction types, amounts and geographic metadata; anonymized open-banking logs from Kaggle and the Open Bank Project, which preserve privacy while reflecting real usage; and labelled fraud cases from the IEEE-CIS Fraud Detection dataset. The schema was enriched with smart-contract status logs and preprocessed for supervised learning. Feature engineering focused on transaction velocity (transactions per hour), deviation of amounts from the customer's historical norm, frequency of smart-contract calls and consistency of IP-based location.

D. Models

Three supervised models were used: XGBoost for credit risk scoring with feature-importance analysis, LSTM networks for sequential analysis of transactions in real-time fraud detection, and random forests for customer segmentation and



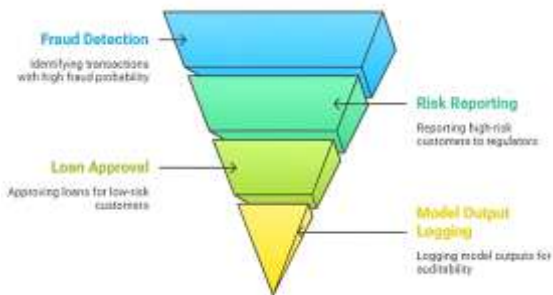
identification of personalized marketing opportunities. All were trained on a stratified 80/20 split with cross-validation, and SMOTE was applied to counter the imbalance of the fraud class. SHAP [5] and LIME [6] were integrated for transparency; the SHAP explanation decomposes a prediction as

$$f(x) = \varphi_0 + \sum_{i=1}^M \varphi_i \quad (3)$$

where φ_0 is the expected model output (base value), φ_i the SHAP value of feature i and M the number of features.

E. Smart-Contract Logic

Smart contracts written in Solidity issue real-time alerts when a transaction is predicted to be high-risk fraud, record AI predictions on the ledger as an immutable audit trail, and automate compliance steps such as mandatory regulatory reporting when risk scores exceed set thresholds. They were deployed on the simulated Hyperledger Fabric network and connected to the AI decision engine through Python web APIs. Fig. 3 shows the resulting risk-management funnel.



Smart-contract risk-management funnel (contract logic in Solidity and Python).

F. Evaluation Metrics and Environment

Performance was measured by fraud-detection precision, recall and F1-score; end-to-end latency from ingestion to final decision or alert (ms); explanation fidelity, the agreement between SHAP/LIME outputs and model predictions; smart-contract execution time from trigger to confirmation; and throughput (transactions processed per second). Precision, recall and F1 are defined from true positives (TP), false positives (FP) and false negatives (FN) as

$$\text{Precision} = \text{TP} / (\text{TP} + \text{FP}), \text{Recall} = \text{TP} / (\text{TP} + \text{FN}) \quad (4)$$

$$\text{F1} = 2 \cdot \text{Precision} \cdot \text{Recall} / (\text{Precision} + \text{Recall}) \quad (5)$$

All evaluations used 10,000 simulated real-time events. The system was implemented in Python 3.11 and Solidity with scikit-learn, TensorFlow, SHAP, LIME and web3.py, on Hyperledger Fabric 2.4 with a local IPFS network, developed in Google Colab Pro with a Ganache test network, and visualized with Dash (Plotly). The testbed was designed to reproduce realistic operating and stress conditions.

IV. RESULTS

A. Model Performance

Table IV compares the three models. XGBoost performed best, with an accuracy of 0.961, an F1-score of 0.951 and an AUC-ROC of 0.978, indicating high precision and good resilience to the class imbalance typical of fraud data. The LSTM captured sequential patterns well (F1 0.929, AUC 0.963) but at slightly higher latency because of its more complex architecture. The random forest was the most interpretable but the least accurate (F1 0.914). The choice of model therefore depends on how a deployment weighs accuracy, responsiveness and explainability; the spread between the best and worst F1-scores is less than four points, so latency and interpretability may reasonably decide the choice.

MODEL PERFORMANCE FOR REAL-TIME BANKING INTELLIGENCE

Model	Acc.	Prec.	Recall	F1	AUC
XGBoost	0.961	0.948	0.954	0.951	0.978
LSTM	0.945	0.932	0.927	0.929	0.963
Random forest	0.937	0.920	0.909	0.914	0.956

Source: model outputs from an 80/20 train-test split with 10-fold cross-validation.

B. Latency and Throughput

Latency and throughput determine whether the framework can serve fraud detection, lending and compliance decisions in practice. Across 10,000 simulated streaming transactions, the average end-to-end time for risk classification and smart-contract activation was 142–168 ms, and the XGBoost configuration processed 73 transactions per second, sufficient for near-real-time BI. Fig. 4 summarizes the relative standing of the models.



Relative ranking of the AI models in the simulated deployment.

C. Explainability

SHAP and LIME produced local and global explanations that let analysts trace each risk score to its input features. Across models, the most influential features were large deviations of transaction amount from the customer's usual pattern, transaction frequency (velocity), involvement of smart contracts, geographic or IP-address inconsistencies, and anomalies in the time of day. That these features coincide with recognized fraud indicators lends face validity to the models.



The explanations were visualized and stored on the ledger as auditable intelligence reports.

D. Business Relevance

The resulting real-time, predictive and explainable framework has direct uses in early fraud detection to limit losses, automation of compliance workflows, behaviour-based personalization and instant credit scoring with transparent reasons.

V. DISCUSSION

A. Strategic Implications

Combining blockchain's trusted data layer with AI changes BI from retrospective reporting to proactive decision support. Traditional banking BI, constrained by silos, batch processing and opaque algorithms, delivers alerts late and supports compliance poorly. The simulation indicates that the integrated framework yields faster insight, more accurate fraud and risk assessment, better auditability through immutable smart-contract logs and traceable decisions, and greater regulatory readiness through explainable AI and automated rule enforcement. Paired with interpretable AI, smart contracts can reduce operational risk, shorten decision times and support services tailored to individual customers across mobile, ATM and web channels.

B. Regulatory and Ethical Considerations

Fairness, accountability and transparency are central concerns for AI in finance, given worries about algorithmic bias, data misuse and opaque decisions [14], [24]. The framework addresses them in two ways. SHAP identifies the features driving each decision, enabling bias to be detected and mitigated, and every prediction and its rationale is recorded with a timestamp on an immutable ledger, so that customers and regulators can trace decisions to their data and reasoning. These properties support GDPR Article 22 and the associated right to explanation [4], PSD2 and open-banking requirements for secure API-based data sharing, FATF Recommendation 15 on technology-assisted AML/CTF controls, and Basel III/IV expectations for auditable automated scoring, as well as the ethical-AI principles promoted by the OECD and the European Commission.

One tension deserves explicit attention. Immutability, the property that makes the audit trail credible, conflicts with GDPR rights to rectification and erasure if personal data are written to the ledger. A compliant deployment would therefore keep personal data off-chain and record only hashes, model outputs and explanation metadata on-chain, a design choice that the present framework should make explicit.

C. Deployment Challenges

Live deployment raises technical, organizational and cultural challenges (Table V). Banks must redesign data governance around on-chain constraints and cross-departmental data flows; maintain rigorous model governance

that tracks model versions, training data and parameters; and guard against new risks at the interface of AI and blockchain, such as model poisoning and smart-contract vulnerabilities [9]. A phased rollout, beginning with non-critical pilots such as customer segmentation or loan pre-approval and keeping humans in the loop, is advisable.

DEPLOYMENT CHALLENGES AND MITIGATION STRATEGIES

Challenge	Description	Mitigation
Data privacy and compliance	Compliance with GDPR, PSD2, FATF	Permissioned blockchain, encryption, access control
Computational overhead of XAI	SHAP/LIME can delay real-time inference	Explain only high-risk flagged transactions
Legacy integration	Core systems may not support AI or blockchain protocols	Middleware APIs and micro-services for gradual migration
Model drift	Models degrade without new training data	Automated feedback loops with human-in-the-loop validation
Distrust of automation	Stakeholders fear black-box models	Interpretable dashboards and XAI audit trails

Source: authors' analysis of industry observations and related research (2018–2022).

The approach is not limited to large commercial banks. It could serve neo-banks and fintechs seeking flexible real-time infrastructure, credit unions that depend on transparency for member trust, Islamic banks that require Sharia-compliant rules enforced by smart contracts, and microfinance and lending platforms in emerging markets that must score credit from limited data.

D. Limitations and Future Research

The evaluation was conducted in simulation on a partly synthetic dataset, so the reported accuracy and latency must be confirmed on production data and infrastructure. Several extensions are promising: federated explainable AI, training models across blockchain nodes to strengthen privacy; on-chain explainability, embedding explanation metadata in smart contracts; tokenized compliance, using tokens to certify milestones such as know-your-customer checks; multimodal BI that combines behavioural, transactional and social-network data; cross-chain interoperability between networks such as Ethereum and Hyperledger; quantum-safe cryptography for the ledger; on-device inference with lightweight models that use on-chain data while preserving privacy; and behavioural biometrics, such as keystroke dynamics, gestures and device usage, to strengthen fraud detection with little additional sensitive data.

VI. CONCLUSION

Blockchain and AI together offer a substantial advance in real-time BI for digital banking. This study has developed a framework that couples a permissioned blockchain with interpretable machine learning and has shown in simulation that it can detect fraud with high accuracy, generate insight with low latency and explain its risk classifications. Blockchain contributes data integrity, auditability and compliance security;



AI contributes real-time predictive and behavioural analytics; and SHAP and LIME provide the transparency that regulations such as GDPR, FATF guidance and PSD2 demand.

VII. CONFLICTS OF INTEREST

The authors declare no conflicts of interest.

REFERENCES

- [1] Adadi, A., & Berrada, M. (2018). Peeking inside the black-box: A survey on explainable artificial intelligence (XAI). *IEEE Access*, 6, 52138–52160. <https://doi.org/10.1109/ACCESS.2018.2870052>
- [2] Chen, T., & Guestrin, C. (2016). XGBoost: A scalable tree boosting system. In *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining* (pp. 785–794). <https://doi.org/10.1145/2939672.2939785>
- [3] Gai, K., Qiu, M., & Sun, X. (2018). A survey on FinTech. *Journal of Network and Computer Applications*, 103, 262–273. <https://doi.org/10.1016/j.jnca.2017.10.011>
- [4] Goodman, B., & Flaxman, S. (2017). European Union regulations on algorithmic decision-making and the right to explanation. *AI Magazine*, 38(3), 50–57. <https://doi.org/10.1609/aimag.v38i3.2741>
- [5] Lundberg, S. M., & Lee, S. I. (2017). A unified approach to interpreting model predictions. In *Advances in Neural Information Processing Systems*, 30, 4765–4774. https://proceedings.neurips.cc/paper_files/paper/2017/hash/8a20a8621978632d76c43dfd28b67767-Abstract.html
- [6] Ribeiro, M. T., Singh, S., & Guestrin, C. (2016). “Why should I trust you?” Explaining the predictions of any classifier. In *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining* (pp. 1135–1144). <https://doi.org/10.1145/2939672.2939778>
- [7] Aste, T., Tasca, P., & Di Matteo, T. (2017). Blockchain technologies: The foreseeable impact on society and industry. *Computer*, 50(9), 18–28. <https://doi.org/10.1109/MC.2017.3571056>
- [8] Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the Internet of Things. *IEEE Access*, 4, 2292–2303. <https://doi.org/10.1109/ACCESS.2016.2566339>
- [9] Conti, M., Kumar, S., Lal, C., & Ruj, S. (2018). A survey on security and privacy issues of Bitcoin. *IEEE Communications Surveys & Tutorials*, 20(4), 3416–3452. <https://doi.org/10.1109/COMST.2018.2842460>
- [10] Doshi-Velez, F., & Kim, B. (2017). Towards a rigorous science of interpretable machine learning. *arXiv preprint arXiv:1702.08608*. <https://arxiv.org/abs/1702.08608>
- [11] Hevner, A. R., March, S. T., & Park, J. (2004). Design science in information systems research. *MIS Quarterly*, 28(1), 75–105. <https://doi.org/10.2307/25148625>
- [12] Kute, D. V., Pradhan, B., Shukla, N., & Alamri, A. (2021). Deep learning and explainable artificial intelligence techniques applied for detecting money laundering: A critical review. *IEEE Access*, 9, 147232–147251. <https://doi.org/10.1109/ACCESS.2021.3124356>
- [13] Li, Y., Li, M., & He, Y. (2020). Fraud detection using ensemble learning in electronic transactions. *Expert Systems with Applications*, 139, 112873. <https://doi.org/10.1016/j.eswa.2019.112873>
- [14] Mehrabi, N., Morstatter, F., Saxena, N., Lerman, K., & Galstyan, A. (2021). A survey on bias and fairness in machine learning. *ACM Computing Surveys*, 54(6), 1–35. <https://doi.org/10.1145/3457607>
- [15] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. White Paper. <https://bitcoin.org/bitcoin.pdf>
- [16] Nguyen, G., Dlugolinsky, S., Bobák, M., Tran, V., Garcia, A. L., Heredia, I., & Hluchý, L. (2019). Machine learning and deep learning frameworks and libraries for large-scale data mining: A survey. *Artificial Intelligence Review*, 52(1), 77–124. <https://doi.org/10.1007/s10462-018-09679-2>
- [17] Nassar, M., Salah, K., Ur Rehman, M. H., & Jayaraman, R. (2020). Blockchain for explainable and trustworthy artificial intelligence. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, 10(5), e1375. <https://doi.org/10.1002/widm.1375>
- [18] Doddipatla, L., Ramadugu, R., Yerram, R. R., & Sharma, R. S. T. (2021). Exploring the role of biometric authentication in modern payment solutions. *European Chemical Bulletin*, 220–229. <https://doi.org/10.53555/ecb.v10i1.17783>
- [19] Pilkington, M. (2016). Blockchain technology: Principles and applications. In *Research Handbook on Digital Transformations* (pp. 225–253). Edward Elgar. <https://doi.org/10.4337/9781784717766.00019>
- [20] Russell, S. J., & Norvig, P. (2020). *Artificial Intelligence: A Modern Approach* (4th ed.). Pearson.
- [21] Tapscott, D., & Tapscott, A. (2016). *Blockchain revolution: How the technology behind bitcoin is changing money, business, and the world*. Penguin.
- [22] Walambe, R., Kolhatkar, A., Omaha, M., Kademani, A., & Raut, R. D. (2020). Integration of explainable AI and blockchain for credit risk assessment. *International Advanced Research Journal in Science, Engineering and Technology*, 7(6), 15–26.
- [23] Zikopoulos, P., Eaton, C., deRoos, D., Deutsch, T., & Lapis, G. (2012). *Understanding Big Data: Analytics for Enterprise Class Hadoop and Streaming Data*. McGraw-Hill.
- [24] Binns, R., Veale, M., Van Kleek, M., & Shadbolt, N. (2018). ‘It’s reducing a human being to a percentage’: Perceptions of justice in algorithmic decisions. In *CHI Conference on Human Factors in Computing Systems* (pp. 1–14). <https://doi.org/10.1145/3173574.3173951>
- [25] Weller, A. (2019). Transparency: Motivations and challenges. In *Explainable AI: Interpreting, Explaining and Visualizing Deep Learning* (pp. 23–40). Springer. https://doi.org/10.1007/978-3-030-28954-6_2
- [26] Tulli, S. K. C. (2022). Machine learning approaches in demand forecasting for supply chain management. *International Journal of Scientific Research and Management*, 10(3), 809–821..