International Journal of
Applied Data Science in Engineering and Health
https://ijadseh.com

A Systematic Review on the Application of Artificial Intelligence in Decentralized Finance

Saeid Ataei[1*] , Seyyed Taghi Ataei[2], Parisa Omidmand[3], Ghazaleh Alikaram[4]

[1] *Stevens Institute of Technology, Hoboken, NJ, USA*

[2] *Independent Researcher*

[3] *Texas Tech University, Lubbock, TX, USA*

[4] *Idaho State University, Pocatello, ID, USA*

Received date: October 21, 2025; Accepted date: November 5, 2025

Abstract

This study presents a comprehensive systematic review of Artificial Intelligence (AI) applications in Decentralized Finance (DeFi), emphasizing AI's pivotal role in mitigating the vulnerabilities and operational complexities inherent in permissionless financial systems. By systematically analyzing 39 peer-reviewed studies from major scholarly databases, the review identifies five dominant application domains: fraud detection, smart contract security, market prediction, credit risk assessment, and decentralized governance. It examines the diverse range of AI methods spanning machine learning, deep learning, graph neural networks, and reinforcement learning—and evaluates their comparative performance and limitations. The findings reveal that AI not only enhances DeFi's transparency, trust, and efficiency but also underpins emerging capabilities such as autonomous governance and adaptive market mechanisms. Persistent challenges including data scarcity, cross-chain generalization, interpretability, and scalability—underscore the need for robust, explainable, and ethical AI solutions. The review concludes that AI constitutes a foundational enabler for secure, transparent, and resilient decentralized financial ecosystems, and outlines critical future research directions for integrating trustworthy intelligence into the evolving DeFi landscape.

Keywords*:* Artificial Intelligence; Decentralized Finance; Cryptocurrency; Deep learning; Reinforcement learning

Introduction

Decentralized Finance (DeFi) is transforming the global financial system by leveraging blockchain technology to eliminate intermediaries and enable permissionless, transparent financial services [1], [2], yet its rapid growth exposes it to challenges such as security vulnerabilities, scalability constraints, and systemic risks [3]. Artificial Intelligence (AI), already a transformative force in traditional finance, assumes an even more critical role in DeFi due to the absence of centralized safeguards, offering solutions in fraud detection, risk management, and predictive analytics through models such as tree-based classifiers and graph neural networks [4]. While AI has shown potential to enhance DeFi's reliability and efficiency, challenges such as its "black box" nature, the need for explainable AI methods (e.g., SHAP, LIME) [5], scalability limitations, and regulatory uncertainties persist [6]. Furthermore, existing research is fragmented, often focusing on isolated applications rather than systemic integration, which underscores the need for a comprehensive synthesis of AI's role in this domain. Recent systematic analyses underscore deep learning's growing effectiveness in cryptocurrency and DeFi domains, particularly through hybrid, ensemble, and reinforcement models for predictive and autonomous decision-making [49]. [47, 48] have emphasized the importance of systematic model benchmarking and optimization in AI applications. Motivated by DeFi's exponential

* Corresponding author. e-mail: sataei@stevens.edu.

growth and the substantial financial losses caused by hacks and various fraudulent schemes [7], this systematic review seeks to map the intersection of AI and DeFi through the following research questions: (1) What are the primary application areas of AI in DeFi? (2) What specific AI techniques are being employed? (3) What are the strengths and limitations of current AI applications? and (4) What emerging trends and future directions can be identified for AI in DeFi research? By addressing these questions, the study aims to support future integrations that preserve transparency, trustlessness, and systemic stability.

Methodology

This systematic review employed a rigorous methodology to identify, screen, and synthesize

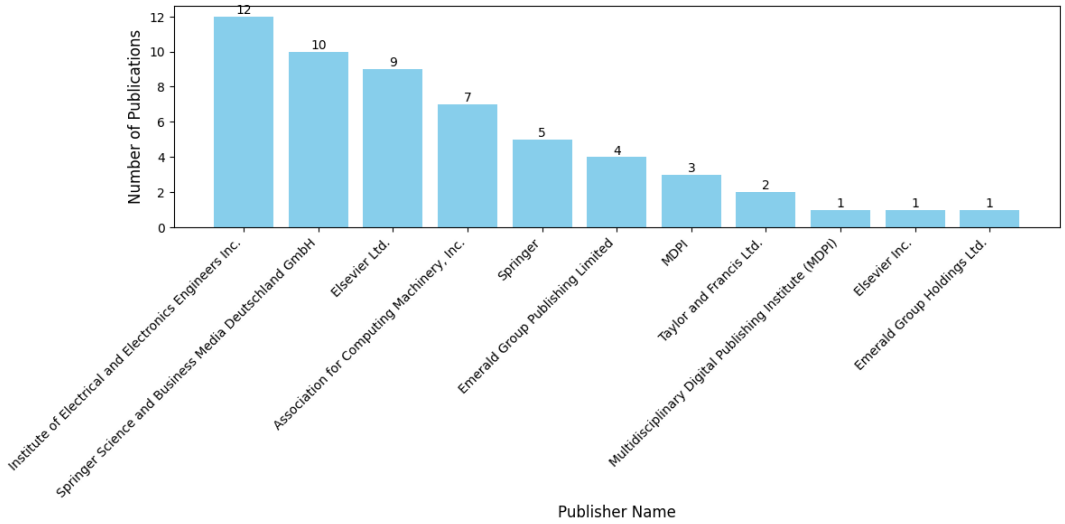

Fig.1. Distribution of publications across different publishers for selected papers.

literature at the intersection of AI and DeFi, drawing from two leading scholarly databases, Scopus and Web of Science. Targeted title and abstract searches focusing on AI techniques (including machine learning, deep learning, and reinforcement learning) within DeFi contexts yielded 267 records from Scopus and 77 from Web of Science, producing a combined initial set of 344 studies. To ensure precision and relevance, inclusion criteria restricted papers to peer-reviewed primary research explicitly applying AI to DeFi, while excluding reviews, books, and studies limited to blockchain or traditional finance without DeFi integration. The study selection process followed a systematic review, reducing the pool to 39 papers through stages of identification, screening, eligibility, and inclusion, thereby enhancing transparency, replicability, and methodological rigor. Data extraction focused on AI application areas, techniques, datasets, findings, limitations, and proposed research directions, while thematic synthesis enabled the identification of common trends, methodologies, and persistent challenges providing a comprehensive overview of the field's current

maturity and highlighting gaps to guide future investigations. Fig.1 illustrates the number of publications contributed by various publishers.

Fig. 2 outlines the systematic process of identifying and screening studies related to AI in decentralized finance. It details the number of records identified, duplicates removed, records screened, full-text articles assessed, reports excluded, and the final studies included in the review.

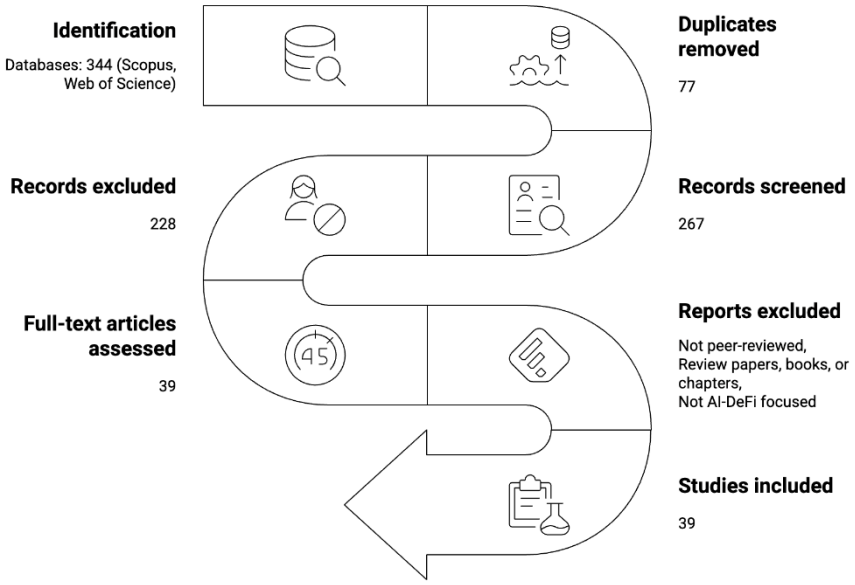

Fig. 2. Systematic Flow Diagram for Study Selection

Results

This systematic review synthesizes findings from 39 peer reviewed studies, each highlighting the diverse applications of AI in DeFi. The literature demonstrates that AI is not a peripheral tool but a foundational enabler across multiple domains of DeFi, providing capabilities for fraud detection, smart contract auditing, credit risk assessment, market optimization, price forecasting, governance, and broader economic innovation. Fig. 3 illustrates the various applications of artificial intelligence within the DeFi sector, including price prediction, fraud and scam detection, DeFi governance, smart contract security, market dynamics, credit risk assessment, and the synergy between AI and blockchain technologies.

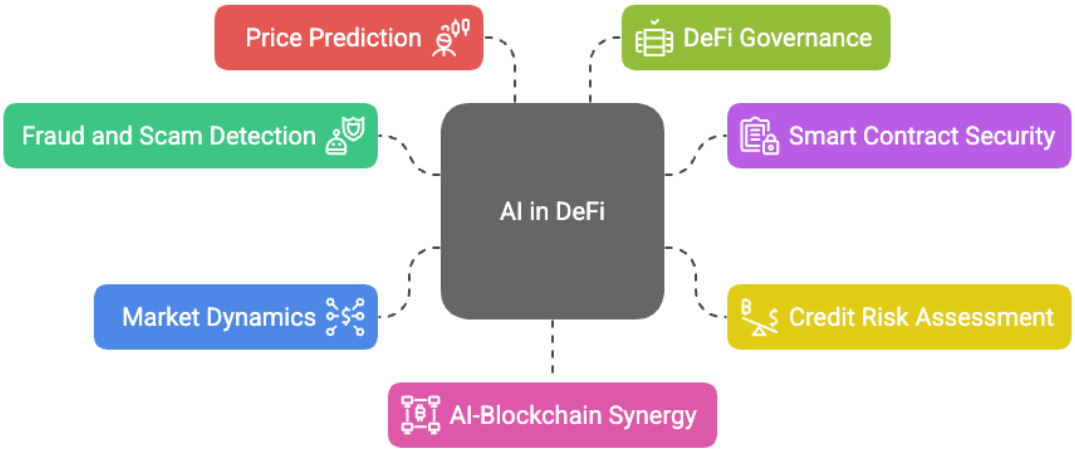

Fig. 3. AI Applications in Decentralized Finance

Fraud and Scam Detection

DeFi is reshaping the global financial landscape by eliminating intermediaries through blockchain-based smart contracts, enabling peer-to-peer transactions, transparency, and innovative services such as lending, trading, and insurance. However, its unregulated and complex nature exposes it to risks like scams, technical vulnerabilities, and extreme market

volatility. To address these challenges, AI and machine learning are increasingly being applied to fraud detection, with models such as the Anomaly VAE-Transformer [8] for anomaly detection, DeFiScanner [9] for flash loan and price manipulation attacks using a multi-model deep learning framework, XGBoost and FT-Transformer [10] for scam prediction, and graph-based models like MVCG-SPS [11] for Ponzi scheme detection.

The paper [12] addresses the issue of rug pull scams on decentralized exchanges, while TTPS [13], an LSTM-based framework, leverages temporal and static features of Ethereum smart contracts for fraud detection. In addition, [14] apply machine learning and clustering techniques to uncover hidden illicit networks on Ethereum, further broadening the scope of AI-driven security analysis in DeFi. Multi-model approaches, including trust scoring systems [15], further enhance security by integrating insights from code audits, transaction anomalies, price fluctuations, and sentiment analysis, offering a proactive defense against DeFi's evolving threats.

Smart Contract Security and Vulnerability Detection

AI is increasingly being applied to enhance smart contract security by proactively detecting vulnerabilities that traditional analyzers often miss. Advanced models such as multimodal deep learning frameworks [16] achieve up to 90% accuracy across multiple vulnerability types by integrating code, opcode, and dynamic features, while frameworks like HARDEN [17] and DeFiTail [18] deliver over 98% accuracy in detecting reentrancy, access control, and flash loan exploits. Similarly, StateGuard [19] uses AST-based Graph Convolutional Networks to identify state derailment defects with 94.83% accuracy and uncover new vulnerabilities in real-world contracts, and variable-length opcode detection models [20] preserve opcode integrity to detect diverse flaws with 93.5% accuracy. These AI-driven methods complement traditional tools by offering automated, adaptive, and highly precise defenses that keep pace with the evolving complexity of decentralized finance systems.

Credit Risk Assessment and Liquidation Prediction

AI is increasingly being applied in DeFi to enhance credit risk evaluation and price forecasting, replacing traditional credit systems with more transparent and data-driven approaches. [21] demonstrates that ensemble machine learning models trained on Aave protocol data can achieve 95% accuracy in assessing borrower creditworthiness, offering a decentralized alternative to traditional credit scoring while reducing manipulation risks. Similarly, [22] show that models such as XGBoost and CatBoost, leveraging DeFi-specific features, can effectively predict wallet liquidations across multichain ecosystems, reaching Area Under the Curve (AUC) values up to 0.847. Beyond credit risk, DREGL model [23] introduces deep regression learning for DeFi stock performance forecasting, reducing prediction errors by up to 20% compared to conventional methods. These advances highlight how AI-driven models enable more secure credit evaluation and sophisticated financial strategies in DeFi.

Market Dynamics and Trading Optimization

AI is increasingly being integrated into Automated Market Makers (AMMs) and arbitrage strategies, shifting DeFi from static protocols toward adaptive, learning-driven systems. Predictive frameworks like hybrid LSTM-Q-learning model [24] enhance liquidity utilization and reduce slippage, while ZeroSwap [25] uses reinforcement learning to track external prices and optimally set bids and asks without relying on oracles. Similarly, QLAMMP [26] leverages Q-learning to dynamically adjust fee rates and leverage coefficients, outperforming static protocols with fixed parameters. On the arbitrage side, deep learning and reinforcement learning models are proving highly effective in uncovering complex patterns, with the Deep Learning Statistical Arbitrage model [27], for example, extracting time-series signals to optimize trading policies and maximize risk-adjusted returns, even under transaction costs. These approaches

illustrate how AI is transforming AMMs and arbitrage into intelligent, adaptive mechanisms capable of responding in real-time to DeFi's volatile market dynamics.

Price Prediction and Forecasting

AI models are increasingly applied to predict cryptocurrency and DeFi asset prices, offering powerful tools for navigating volatile markets. Ensemble learning methods, such as ISOMAP-GBR and UMAP-RF, have been used to analyze NFT and DeFi price dynamics, with explainable AI techniques showing that technical indicators and major cryptocurrencies like ETH and BTC are the strongest predictors, while media chatter provides moderate short-term insights [28]. Hybrid deep learning approaches [29], [30], including Bi-LSTM and LSTM networks, have achieved high accuracy in forecasting price variations, with models integrating sentiment analysis and attention mechanisms effectively capturing volatility and temporal trends. Beyond price prediction, risk forecasting models like GARCH and DeepAR [31] have been applied to DeFi protocols such as Uniswap-V2, demonstrating complementary strengths in predicting Value-at-Risk and Expected Shortfall. These studies underscore the critical role of AI in enhancing predictive accuracy and risk management across the DeFi ecosystem.

DeFi Governance and Policy

AI is beginning to shape decentralized governance by introducing automation into decision-making processes, with the goal of reducing human bias and strengthening security. Xu et al.'s Auto.gov framework employs a Deep Q-Network reinforcement learning approach to optimize lending protocol parameters, demonstrating greater resilience to manipulations—retaining over 60% more funds than baseline models during simulated oracle attacks [32]. Also, [33] applied deep learning to analyze public sentiment on social media regarding Central Bank Digital Currencies (CBDCs), highlighting AI's potential to inform governance and policy by integrating public perception into decision-making. AI also contributes to governance and policy by analyzing investor psychology and public sentiment, helping institutions and regulators make more informed decisions [34]. These studies illustrate how AI can make decentralized governance more adaptive, data driven, and resistant to systemic risks.

Broader AI-Blockchain Synergy and Trust

There is a symbiotic relationship between AI and blockchain, emphasizing how their complementary strengths can transform finance and governance [35]. Blockchain serves as a "trust machine" [36] offering transparency, immutability, and decentralization that provide AI with a secure and verifiable data foundation. In turn, AI enhances blockchain by enabling intelligence, automation, and adaptive decision making, as seen in frameworks like WallStreetFeds [37], which introduce client-specific tokens to create new economic models for federated learning and DeFi participation. This synergy enhances security, inclusivity, and innovation, paving the way for autonomous, trustworthy, and more adaptive financial systems that extend beyond traditional banking.

Overall, AI plays an indispensable role in securing, optimizing, and enhancing DeFi ecosystems. Applications span fraud detection, smart contract auditing, credit risk evaluation, market optimization, price prediction, governance, and broader trust mechanisms. The studies reviewed demonstrate AI's adaptability to DeFi's complex and decentralized environment, although challenges remain, including interpretability, computational scalability, and cross-chain generalization. Future research must address these gaps to further integrate AI as a resilient and autonomous pillar of the DeFi ecosystem. Table 1 includes the primary application, key techniques utilized, main findings or contributions of each study, and their limitations, highlighting the challenges and effectiveness of AI methods in this evolving landscape.

Table 1. Key AI Applications in DeFi From Selected Papers

Ref.	Primary AI Application	Key AI Techniques Used	Main Findings/Contribution	Limitations
[9]	DeFi Attack Detection	Deep Learning, Fusion Models	DeFiScanner: 0.91 TPR for flash loan/price manipulation; first deep learning DeFi attack system	Ethereum-centric; dataset timeframe limits evolving patterns
[10]	Rug Pull Detection	ML, FT-Transformer, XGBoost	0.9936 accuracy pre-occurrence detection; 97.7% of analyzed tokens were rug pulls	May not generalize to other chains; high computational cost
[15]	DeFi Security Trust Scoring	Multi-Model AI (GPT-3.5, XGBoost, Prophet, Fin-BERT)	86.17% accuracy for flash loan attacks; beat Mythril	Ethereum focus; historical/sentiment limits
[16]	Smart Contract Vulnerability Detection	Multimodal fusion, Deep Learning (bi-LSTM, GCN)	85–90% accuracy; outperformed traditional tools	Limited to 4 vulnerabilities; Ethereum/Solidity specific
[17]	Reentrancy Detection	Graph Convolution Networks (GCN)	HARDEN: 98.06% accuracy; better than symbolic tools	Only EVM bytecode; costly for big CFGs
[18]	Exploit Detection (Cross-Contract)	DL (BERT, GCN)	98.39% access control accuracy; low FPR	Slow for large DApps; lacks multi-chain
[22]	Credit Risk & Liquidation Prediction	ML (XGBoost, RF, CNN, etc.)	0.92 AUC for liquidation; key: collateral volatility	Ethereum bias; static contract analysis
[24]	AMM Optimization	Deep RL (LSTM-Q-learning)	93% liquidity use; 50% less slippage	Synthetic data; scale limits
[25]	Optimal Market Making	RL (POMDP, Q-learning)	0.2% avg loss without oracles; robust strategies	Fixed trade size; scaling Q-table
[28]	NFT & DeFi Price Prediction	Ensemble ML (GBR, RF), ISOMAP, UMAP, XAI (SHAP, LIME)	Superior prediction during COVID-19; technical indicators critical	Limited to 8 tokens; COVID-19 period only
[32]	Learning-Based Governance	Reinforcement Learning (DQN)	Auto.gov retained 60% more profit; beat manual rules	Simplified; adversarial risks; centralized
[33]	Public Sentiment Analysis (CBDC Adoption)	Deep Learning, BERT, Text Mining, Econometrics	Increased CBDC adoption sentiment post-2020; influenced by government effectiveness and DeFi adoption	Limited to Facebook data; cross-sectional limits temporal analysis
[35]	AI-Blockchain in Finance	Algorithmic (LSTM, VaR)	95.2% accuracy; 92.8% efficiency	Scalability, compliance, retraining
[36]	Blockchain as Trust Machine	Historical Analysis, Taxonomy, Application Survey	Boosts trust in DeFi, NFTs, IoT; reduces AIGC risks	Scalability, interoperability, regulation
[38]	Scam Token Detection	ML, Guilt-by-association heuristics	Identified 10,000 scam tokens (50%) on Uniswap V2; $16M profit by scammers	Focused on Uniswap V2; evolving fraud may be missed
[39]	Cryptocurrency Sentiment Analysis	ML, Lexicon Sentiment Analysis	33.2% positive sentiment; 'scam' most negative word in 15,000 tweets	Limited to English Twitter; no demographic info
[40]	AI in Finance / DeFi	Systematic Literature Review	AI improves investment, fraud detection, credit scoring; DeFi boosts inclusion	Security, scalability, regulation challenges
[41]	Scam DeFi Token Detection	Transformer, BERT Sentiment	96% precision; flagged irregular transactions and negative sentiment	Ethereum/Reddit bias; post-hoc explanations
[42]	Smart Contract Auditing	ML (RF, KNN, Naive Bayes)	93–94% accuracy; improved auditing efficiency	Ethereum focus; tool-based limitations
[43]	Securities Violations Detection	ML (Random Forest)	80% F1 using opcode frequencies; CALLDATA-SIZE critical	Small dataset; lacks transaction data

[44]	Pre-Deployment Scam Detection	Static Analysis, N-gram, SVM	91.7% accuracy; early runtime cues effective	Code reuse hurts accuracy; interpretability lacking
[45]	Multichain Fraud Detection	ML (DNN, XGBoost, SVM, GPT-3 Curie)	F1 = 0.742; key DeFi traits	Severe class imbalance; short scope
[46]	Crypto Arbitrage Dynamics	Economic Theory, Game Theory	DEXes offer more arbitrage; persistent gaps identified	Data gaps; market change; regulation

Discussion

The systematic review of AI applications in DeFi highlights AI's increasingly central role in providing security, trust, and operational efficiency within a permissionless environment. AI is predominantly employed for fraud detection, smart contract vulnerability mitigation, and risk management, addressing the absence of traditional intermediaries and their safeguards. The literature demonstrates a shift toward advanced AI techniques, including deep learning architectures such as LSTMs and Transformers, Graph Neural Networks, and reinforcement learning, reflecting the complexity and dynamic nature of DeFi challenges. Researchers are increasingly integrating multimodal data (from transactional histories and smart contract code to social media sentiment and macroeconomic indicators) to improve predictive accuracy. Moreover, a proactive approach to detection, exemplified by early-stage scam and fraud identification, underscores AI's strategic role in preventing losses before they manifest, effectively becoming a functional "trust layer" that compensates for the decentralized nature of DeFi.

Despite impressive predictive performance, practical deployment of AI in DeFi faces significant challenges. Data limitations, such as short asset histories, class imbalance, and code-reuse issues, constrain model generalizability, while computational complexity, reliance on historical patterns, and high on-chain transaction costs hinder real-time applicability. Cross-chain generalizability is limited, with many models tailored to specific blockchains or older protocols, and the evolving threat landscape requires continuous retraining of adaptive models. Additional concerns include interpretability, regulatory uncertainty, and vulnerability to adversarial manipulation, which affect trust, adoption, and compliance. Compared to traditional rule-based or static methods, AI offers adaptive learning, relational understanding through transaction graph analysis, automation at scale, multi-modal data fusion, and the creation of novel DeFi primitives such as decentralized credit scoring and learning-based governance. Collectively, these capabilities position AI not merely as an enhancement of existing practices but as a foundational enabler of DeFi's decentralized future. Table 2 outlines various AI techniques, including their specific algorithms and primary application areas within decentralized finance, along with representative academic papers that discuss these methodologies.

Limitations

The systematic review identifies several recurring limitations in the application of AI in DeFi, highlighting systemic challenges that constrain practical deployment. Dataset constraints, including limited size, severe class imbalance, reliance on historical data, and the "code-reuse problem," reduce the accuracy and generalizability of AI models. Many approaches are validated on specific platforms or older protocols, limiting cross-chain applicability, while the computational cost of advanced models hinders real-time scalability. The rapidly evolving nature of DeFi, with constantly changing protocols, market conditions, and attacker tactics, requires continuous model adaptation, increasing operational complexity. Additional challenges include the lack of interpretability in complex models, regulatory uncertainty, and the narrow scope of vulnerabilities addressed in current research, often relying on simulated environments that may not fully capture real-world complexities. Collectively, these limitations indicate that despite

promising academic results, AI in DeFi remains largely nascent regarding robust, production-ready solutions.

Table 2. AI Techniques and Their Applications in DeFi

AI Technique Category	Specific Algorithms/Models	Primary Application Areas in DeFi
Deep Learning	LSTMs, BiLSTMs, GRUs, CNNs, VAE-Transformers, Deep Neural Networks	Anomaly Detection, Smart Contract Vulnerability Detection, Price Prediction, General Attack Detection, Financial Management
Machine Learning	Random Forest, XGBoost, SVM, LightGBM, AdaBoost, KNN, RGF	Scam Token Detection, Credit Scoring, Fraud Detection, Risk Forecasting, Securities Violations
Graph Neural Networks	GCNs, Multi-view GNNs	Fraud Detection (complex patterns), Smart Contract Vulnerability Detection
Reinforcement Learning	Q-learning, Deep Q-Networks (DQN), POMDP	Learning-Based Governance, Optimal Market Making, AMM Fee Optimization
Natural Language Processing / Sentiment Analysis	BERT, FinBERT, Text Mining	Public Opinion Analysis, Price Prediction, Scam-related Discourse
Explainable AI	SHAP, LIME, Integrated Gradients	Price Prediction, Scam Detection
Large Language Models	GPT-3 Curie, GPT-3.5, GPT-4	Smart Contract Audits, Fraud Detection

Fig. 4 highlights key obstacles to effective AI implementation, including scalability issues, data scarcity, model opacity, privacy and security concerns, and various risks such as security vulnerabilities, adversarial attacks, ethical dilemmas, regulatory challenges, and interpretability barriers impacting public understanding.

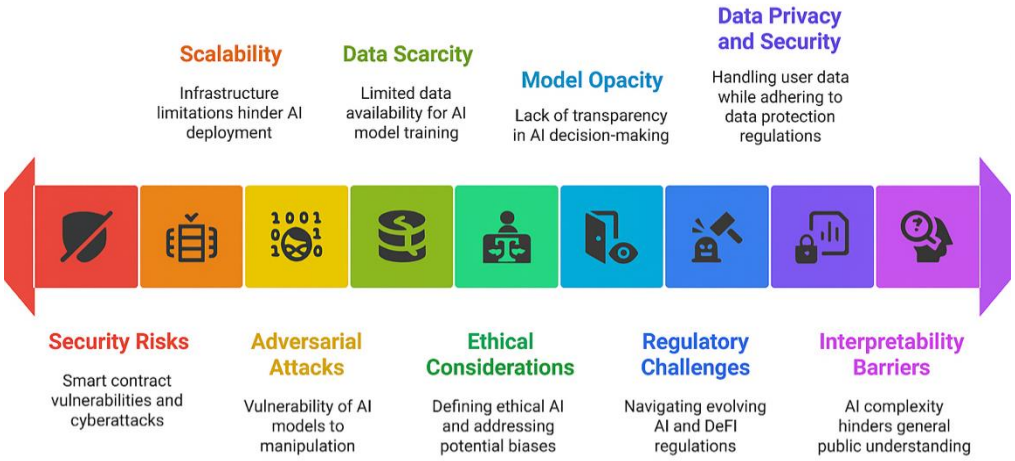

Fig. 4. challenges in integrating AI into DeFi

Future Directions

Future research directions focus on addressing these systemic limitations and advancing AI toward more integrated, adaptive, and practical solutions for DeFi. Key areas include developing cross-chain and multi-protocol frameworks, enabling real-time monitoring and adaptive threat detection, and enhancing data sources through multi-modal integration, sophisticated feature engineering, and comprehensive blockchain analytics. Exploring advanced and hybrid AI architectures, including ensemble models and combinations of supervised and unsupervised approaches, can improve robustness and predictive performance. Increasing model interpretability through XAI, establishing clear regulatory frameworks, and investigating human-AI collaboration are also critical to fostering trust and adoption. Finally, the creation of standardized datasets and benchmarks will improve comparability and reliability across studies. These future directions emphasize that AI solutions must evolve beyond isolated academic exercises toward holistic, scalable, and ethically considered tools capable of supporting the complex and dynamic DeFi ecosystem.

Conclusion

This systematic review underscores the transformative role of Artificial Intelligence (AI) in redefining the architecture and resilience of Decentralized Finance (DeFi). Across 39 peer-reviewed studies, evidence consistently demonstrates that AI serves not merely as a technological enhancement but as a foundational enabler of security, efficiency, and autonomy in permissionless financial ecosystems. Through advanced approaches ranging from deep learning and graph neural networks to reinforcement learning and natural language processing—AI effectively addresses critical DeFi challenges, including fraud detection, smart contract vulnerability analysis, credit risk assessment, market forecasting, and governance optimization. Beyond technical efficacy, AI introduces a new paradigm of adaptive intelligence that functions as a "trust layer" compensating for DeFi's lack of centralized oversight. By enabling predictive, self-learning, and data-driven decision processes, AI significantly enhances DeFi's operational robustness and investor confidence. Yet, the review reveals persistent limitations—most notably, data scarcity, class imbalance, computational inefficiency, and restricted cross-chain generalizability—that constrain real-world deployment. Additionally, the black-box nature of advanced AI models raises concerns regarding explainability, transparency, and regulatory compliance, challenging both trust and accountability in decentralized systems. Future research must therefore prioritize cross-chain interoperability, real-time adaptive learning, and explainable AI (XAI) frameworks that promote interpretability and fairness. The development of standardized benchmark datasets, open-source toolkits, and ethical AI protocols will be essential to ensure reproducibility and governance alignment. Finally, this review positions AI as a cornerstone of next-generation decentralized finance—one capable of transforming DeFi from an experimental innovation into a secure, transparent, and institutionally credible financial paradigm.

Conflict of interest

The authors declared no conflict of interest.

References

[1] F. A. Bakare, J. Omojola, and A. C. Iwuh, "Blockchain and decentralized finance (DEFI): Disrupting traditional banking and financial systems," World Journal of Advanced Research and Reviews, vol. 23, no. 3, pp. 3075–3089, 2024.

[2] P. K. Ozili, "Decentralized finance research and developments around the world," Journal of Banking and Financial Technology, vol. 6, no. 2,
pp. 117–133, 2022.

[3] N. Carter and L. Jeng, "DeFi protocol risks: The paradox of DeFi," Regtech, suptech and beyond: innovation and technology in financial services, riskbooks, forthcoming Q3, 2021.

[4] B. Luo, Z. Zhang, Q. Wang, A. Ke, S. Lu, and B. He, "AI-powered fraud detection in decentralized finance: A project life cycle perspective," ACM Computing Surveys, vol. 57, no. 4, pp. 1–38, 2024.

[5] S. J. Chavakula, C. A. J. Albert, E. Ebenezer, M. H. Bhagat, and C. V. Mahamuni, "Explainable AI (XAI) Using SHAP and LIME for Financial Fraud Detection and Credit Scoring," in 2025 International Conference on Advanced Computing Technologies (ICoACT), IEEE, pp. 1–8, 2025.

[6] E. Zmaznev, "Measuring decentralised finance regulatory uncertainty," Master's thesis, 2021.

[7] B. Luo, Z. Zhang, Q. Wang, A. Ke, S. Lu, and B. He, "AI-powered fraud detection in decentralized finance: A project life cycle perspective," ACM Computing Surveys, vol. 57, no. 4, pp. 1–38, 2024.

[8] A. Song, E. Seo, and H. Kim, "Anomaly VAE-transformer: A deep learning approach for anomaly detection in decentralized finance," IEEE Access, vol. 11, pp. 98115–98131, 2023.

[9] B. Wang, X. Yuan, L. Duan, H. Ma, C. Su, and W. Wang, "DeFiScanner: Spotting DeFi attacks exploiting logic vulnerabilities on blockchain," IEEE Transactions on Computational Social Systems, vol. 11, no. 2, pp. 1577–1588, 2022.

[10] B. Mazorra, V. Adan, and V. Daza, "Do not rug on me: Leveraging ma- chine learning techniques for automated scam detection," Mathematics, vol. 10, no. 6, p. 949, 2022.

[11] X. Jiang and W.-T. Tsai, "MVCG-SPS: A Multi-View Contrastive Graph Neural Network for Smart Ponzi Scheme Detection," Applied Sciences, vol. 15, no. 6, p. 3281, 2025.

[12] Y. Qiao, G. Li, J. Zhou, and W. Wu, "Detecting Rug Pull Scams on Blockchain via Feature Fused Graph Classification," in CCF China Blockchain Conference, pp. 67–83, Singapore: Springer Nature Singa- pore, 2023.

[13] L. Wang, H. Cheng, Z. Zheng, A. Yang, and M. Xu, "Temporal transaction information-aware Ponzi scheme

detection for Ethereum smart contracts," Engineering Applications of Artificial Intelligence, vol. 126, p. 107022, 2023.
[14] J. Li, F. Baldimtsi, J. P. Brandao, M. Kugler, R. Hulays, E. Showers,
Z. Ali, and J. Chang, "Measuring illicit activity in DeFi: The case of Ethereum," in International Conference on Financial Cryptography and Data Security, pp. 197–203, Berlin, Heidelberg: Springer Berlin Heidelberg, 2021.
[15] V. Mothukuri, R. M. Parizi, J. L. Massa, and A. Yazdinejad, "An AI multi-model approach to DeFi project trust scoring and security," in 2024 IEEE International Conference on Blockchain (Blockchain), pp. 19–28, IEEE, 2024.
[16] J. Li, G. Lu, Y. Gao, and F. Gao, "A smart contract vulnerability detection method based on multimodal feature fusion and deep learning," Mathematics, vol. 11, no. 23, p. 4823, 2023.
[17] H. Lakadawala, K. Dzigbede, and Y. Chen, "Detecting reentrancy vulnerability in smart contracts using graph convolution networks," in 2024 IEEE 21st Consumer Communications & Networking Conference (CCNC), pp. 188–193, IEEE, 2024.
[18] W. Li, X. Li, Y. Zhang, and Z. Li, "Defitail: DeFi protocol inspection through cross-contract execution analysis," in Companion Proceedings of the ACM Web Conference 2024, pp. 786–789, 2024.
[19] Z. Li, W. Li, X. Li, and Y. Zhang, "Stateguard: Detecting state derail- ment defects in decentralized exchange smart contracts," in Companion Proceedings of the ACM Web Conference 2024, pp. 810–813, 2024.
[20] X. Liu, G. Wang, M. Chen, P. Li, and J. Zhu, "A vulnerability detec- tion method for smart contracts using opcode sequences with variable length," in International Conference on Intelligent Computing, pp. 369– 380, Singapore: Springer Nature Singapore, 2024.
[21] M. O. Kotb, "Credit scoring using machine learning algorithms and blockchain technology," in 2023 Intelligent Methods, Systems, and Applications (IMSA), pp. 381–386, IEEE, 2023.
[22] G. Palaiokrassas, S. Scherrers, E. Makri, and L. Tassiulas, "Machine learning in DeFi: Credit risk assessment and liquidation prediction," in 2024 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), pp. 650–654, IEEE, 2024.
[23] L. Ramachandran, S. Shanthana, A. Gokulakrishnan, S. Kumar, K. S. Vishal, and G. Sahaana, "Decentralized financial stocks prediction using deep regression learning," in 2024 2nd International Conference on Disruptive Technologies (ICDT), pp. 1298–1302, IEEE, 2024.
[24] T. Lim, "Predictive crypto-asset automated market making architecture for decentralized finance using deep reinforcement learning," arXiv preprint arXiv:2211.01346, 2022.
[25] V. Nadkarni, J. Hu, R. Rana, C. Jin, S. Kulkarni, and P. Viswanath, "Ze- roSwap: Data-driven optimal market making in decentralized finance," in International Conference on Financial Cryptography and Data Security,
pp. 209–227, Cham: Springer Nature Switzerland, 2024.
[26] D. Churiwala and B. Krishnamachari, "Qlammp: A Q-learning agent for optimizing fees on automated market making protocols," in 2023 Fifth International Conference on Blockchain Computing and Applications (BCCA), pp. 274–281, IEEE, 2023.
[27] R. Jagdale and M. Deshmukh, "Natural language processing in finance: Techniques, applications, and future directions," in Machine Learning and Modeling Techniques in Financial Data Science, pp. 411–434, IGI Global Scientific Publishing, 2025.
[28] I. Ghosh, E. Alfaro-Corte´s, M. Ga´mez, and N. Garc´ıa-Rubio, "Prediction and interpretation of daily NFT and DeFi prices dynamics: Inspection through ensemble machine learning & XAI," International Review of Financial Analysis, vol. 87, 2023, article 102558.
[29] B. B. Gupta, A. Gaurav, J. Pin˜eiro-Chousa, M. A´ . Lo´pez-Cabarcos, and I. Gonza´lez Lo´pez, "Predicting the variation of decentralised finance cryptocurrency prices using deep learning and a BiLSTM-LSTM based approach," Enterprise Information Systems, 2025, article 2483456.
[30] S. Sruthi and D. Saravanan, "Forecasting cryptocurrency prices in the DeFi ecosystem using predictive models," in 2025 International Conference on Computing for Sustainability and Intelligent Future (COMP-SIF), pp. 1–6, IEEE, 2025.
[31] L. Mussoi Almeida, F. M. Mu¨ller, and M. S. Perlin, "Risk forecasting comparisons in decentralized finance: An approach in constant product market makers," Computational Economics, vol. 65, no. 1, pp. 395–428, 2025.
[32] J. Xu, Y. Feng, D. Perez, and B. Livshits, "Auto. gov: Learning-based governance for decentralized finance (DeFi)," IEEE Transactions on Services Computing, 2025.
[33] V. M. Ngo, P. V. Nguyen, H. H. Nguyen, H. X. T. Tram, and L. C. Hoang, "Governance and monetary policy impacts on public acceptance of CBDC adoption," Research in International Business and Finance, vol. 64, 2023, article 101865.
[34] S. V. Jin, ""Technopian but lonely investors?": Comparison between investors and non-investors of blockchain technologies, cryptocurrencies, and non-fungible tokens (NFTs) in artificial intelligence-driven FinTech and decentralized finance (DeFi)," Telematics and Informatics Reports, vol. 14, 2024, article 100128.
[35] S. Agal, K. M. Raulji, Y. Farooqui, N. Bhavsar, and R. Agrawal, "Innovative financial services driven by AI and blockchain synergy for decentralized trust and personalized solutions," in 2024 Eighth International Conference on Parallel, Distributed and Grid Computing (PDGC), pp. 363–370, IEEE, 2024.
[36] S. Fan, N. Ilk, A. Kumar, R. Xu, and J. L. Zhao, "Blockchain as a trust machine: From disillusionment to enlightenment in the era of generative AI," Decision Support Systems, vol. 182, 2024, article 114251.
[37] A. Geimer, B. Fiz, and R. State, "WallStreetFeds: Client-specific tokens as investment vehicles in federated learning," in Proceedings of the 5th ACM International Conference on AI in Finance, pp. 839–846, 2024.
[38] P. Xia, H. Wang, B. Gao, W. Su, Z. Yu, X. Luo, C. Zhang, X. Xiao, and G. Xu, "Trade or trick? Detecting and

characterizing scam tokens on Uniswap decentralized exchange," Proceedings of the ACM on Measurement and Analysis of Computing Systems, vol. 5, no. 3, pp. 1–26, 2021.
[39] M. K. Hassan, F. A. Hudaefi, and R. E. Caraka, "Mining netizen's opinion on cryptocurrency: Sentiment analysis of Twitter data," Studies in Economics and Finance, vol. 39, no. 3, pp. 365–385, 2022.
[40] R. Thatikonda, J. Ponnala, D. K. Yendluri, M. Kempanna, R. Tatikonda, and A. Bhuvanesh, "The impact of blockchain and AI in the finance industry," in 2023 International Conference on Computational Intelli- gence, Networks and Security (ICCINS), pp. 1–6, IEEE, 2023.
[41] M. Gunathilaka, S. Wickramanayake, and H. M. N. Dilum Bandara, "DeFiTrust: A transformer-based framework for scam DeFi token de- tection using event logs and sentiment analysis," Expert Systems with Applications, vol. 251, 2024, article 123913.
[42] S. El Haddouti, M. Khaldoune, M. Ayache, and M. D. E. K. El Kettani, "Smart contracts auditing and multi-classification using machine learning algorithms: An efficient vulnerability detection in Ethereum blockchain," Computing, vol. 106, no. 9, pp. 2971–3003, 2024.
[43] A. Trozze, B. Kleinberg, and T. Davies, "Detecting DeFi securities violations from token smart contract code," Financial Innovation, vol. 10, no. 1, pp. 1–35, 2024.
[44] T. Igarashi and K. Matsuura, "Scam token detection based on static analysis before contract deployment," in International Conference on Fi- nancial Cryptography and Data Security, pp. 189–206, Cham: Springer Nature Switzerland, 2024.
[45] G. Palaiokrassas, S. Scherrers, I. Ofeidis, and L. Tassiulas, "Leveraging machine learning for multichain DeFi fraud detection," in 2024 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), pp. 678–680, IEEE, 2024.
[46] M. Hafeez and Z. A. Uzmi, "Unveiling market dynamics and strategic interactions in crypto arbitrage," in 2024 6th International Conference on Blockchain Computing and Applications (BCCA), pp. 617–623, IEEE, 2024.
[47] Mohammadagha M. Hyperparameter Optimization Strategies for Tree-Based Machine Learning Models Prediction: A Comparative Study of AdaBoost, Decision Trees, and Random Forest. Decision Trees, and Random Forest (April 11, 2025). 2025 Apr 11.
[48] Mohammadagha M, Najafi M, Kaushal V, Jibreen AM. Machine learning models for reinforced concrete pipes condition prediction: The state-of-the-art using artificial neural networks and multiple linear regression in a Wisconsin case study. arXiv preprint arXiv:2502.00363. 2025 Feb 1.
[49] Ataei S, Ataei ST, Saghiri AM. Applications of Deep Learning to Cryptocurrency Trading: A Systematic Analysis