AI and DeFi Integration: Algorithmic Bias, Black-Box Opacity, and Regulatory Challenges

Peiyi Zhou

Faculty of Law, University of Manchester, Mancheseter England, M13 9PL, United Kingdom

qq550222734@gmail.com

Abstract. The integration of AI and DeFi drives financial innovation with applications like smart contract security and automated trading but raises critical challenges. This paper examines algorithmic bias, black-box opacity, and regulatory lags via peer-reviewed literature, industry/institutional reports, and cases (e.g., Apple Card, COMPAS). It analyzes how biased training data perpetuates discrimination in financial applications, while opaque AI models hinder bias detection and auditability, amplifying market volatility and systemic risks. EU, U.S., and Chinese regulatory frameworks face gaps in addressing technical complexity and cross-border fragmentation. Results show AI-DeFi integration exacerbates inequity and erodes trust and there is limited research focused on AI-DeFi specified risks and mitigating mechanism. Conclusions stress interdisciplinary governance, global regulatory coordination, and transparent AI architectures to mitigate risks, ensuring equitable/secure financial ecosystems to support regulatory management and sustainable development.

Keywords: AI-DeFi integration; algorithmic bias; black-box opacity; regulatory challenges.

1. Introduction

The integration of artificial intelligence (AI) and decentralized finance (DeFi) presents transformative opportunities for financial automation but also raises critical challenges—algorithmic bias, operational opacity, and regulatory fragmentation—that remain under-synthesized in current literature. While existing works address technical innovations or regulatory responses in isolation, a holistic understanding of their interdependencies, particularly in cross-border contexts, remains lacking.

As a focused literature review, this study employs systematic synthesis of scholarly articles and institutional publications to examine the integration of AI and DeFi. The research categorizes existing literature into three domains: technical AI applications in DeFi, regulatory frameworks, and empirical analyses of algorithmic bias in automated financial systems. Through this thematic categorization, the review aims to synthesize fragmented insights on technological innovations, regulatory challenges, and socio-technical risks, with a specific focus on cross-border dynamics and operational opacity. By leveraging literature review as the core methodology, the study seeks to identify underexplored intersections and provide a structured foundation for understanding the complex interdependencies between AI-driven automation and DeFi's decentralized architecture.

This review contributes by distilling fragmented knowledge into a structured narrative, identifying underexplored areas like cross-jurisdictional regulatory arbitrage and ethical implications of opaque algorithms. While prioritizing thematic depth over exhaustive coverage—acknowledging limitations in scope and source volume due to the field's rapid evolution—it serves as a foundational resource for clarifying terminological inconsistencies, bridging disciplinary silos, and proposing agendas for future interdisciplinary research. In an era of accelerating financial technologization, this synthesis underscores the need to align cumulative scholarship with practical challenges, fostering transparency about current understandings and unresolved questions in AI-DeFi systems.

2. Literature review

2.1 AI-Specific Risks

2.1.1 Manifestations of Algorithmic Bias

AI itself comes with its own technical risks which remain unresolved. First and foremost, artificial intelligence systems frequently create hidden biases even when they are programmed to be fair, simultaneously making biased assumptions that can lead to discriminatory results, particularly in financial services.

For example, loan approval systems which use machine learning have been found to reject qualified applicants from minority neighborhoods. Research showed that bias in financial algorithms is mainly from the use of sociodemographic information or proxies for it, such as location of residence, occupation in training. Machine learning inherits historical prejudices. Apple Card, for instance, came under fire for its algorithm that allegedly resulted in gender bias in credit terms and offered women with similar financial credentials less favourable terms than men. Such an affair triggered public backlash and regulatory review. Biases of that kind hurt marginalized groups, as seen in loan systems rejecting qualified minority applicants by using indirect factors tied to race, like local business types, mirroring historical discrimination. The research emphasizes that, in the long term, demand for fairer, unbiased systems will rise, but biased systems negatively affect consumer trust and financial equity. [7]

The research explains that algorithmic bias impacts insurance and finance through data-driven discrimination. In insurance, AI systems could use indirect factors like shopping habits or residential areas tied to religion or race to determine premiums rather than traditional criteria like age or driving records. For instance, higher health premiums were charged towards immigrants and ethnic minorities by some U.S insurers, reflecting historical biases in data. In finance, credit scoring models that use historical data often perpetuate inequality by using proxies like zip codes for race, leading to unfair loan rejections or higher rates for marginalized groups. Studies show Black and Latino borrowers pay higher mortgage interest rates because of both human and algorithmic biases. These issues come from bad data encoding, cultural stereotypes in algorithms, and misapplication of demographic proxies, corroding fairness and trust in financial systems [8]. Such unexpected biases emerge because AI is able to find patterns hidden in the data that humans may be unaware of.

2.1.2 Causes of Algorithmic Bias

The reason these issues arise is often the data on which AI is trained. If it imbibes from historical biased data, the AI will simply replicate and, in some cases, exacerbate these biases. Facial recognition software is a good example where systems trained predominantly on white faces generate more false positive when recognising faces with darker skin, resulting in unfair treatment in banking identity checks[9]. Similarly, mortgage approval algorithms using old housing data might repeat past discrimination against certain communities [10].

Credit scoring systems demonstrate how AI bias harms financial access. Traditional credit scores rely on bank records and loan history, which disadvantages people who use cash payments or community lending. The literature notes that bias in AI models, from limited data like bank records, may misjudge cash - using groups as high - risk, harming their credit ratings. [11].

What's more, Oguntibeju's research points out that AI systems in finance may rely on non-financial factors like shopping preferences or social media connections as proxies, embedding biases. For instance, credit scoring models relying on historical data containing societal biases can disadvantage marginalized groups. These practices, if adopted at scale, risk erecting new barriers to financial services, highlighting the importance of transparency, diversifying data sources, and debiasing methods to ensure fairness in AI-generated financial decisions. [12].

These biases fuel vicious cycles. Where banks turn down loan applications from certain areas, those neighbourhoods get less financial support. The AI then uses this reduced economic activity as

"proof" to justify more rejections in the future [9]. This pattern prevents entire groups from improving their financial situations, effectively maintaining historical inequalities through modern technology.

Companies often struggle to detect these biases. Insurance algorithms might use strange combinations of data (like food purchases or gym memberships) to make decisions that feel unfair to customers [8]. As the research highlights, AI in finance can both perpetuate historical biases (e.g., gender/racial stereotypes in credit scoring) and create new ones via machine learning. For instance, biased algorithms might deny loans to marginalized groups while also inadvertently injecting biases that strengthen the financial inequalities.[13]. Until developers improve transparency and fairness checks, AI in finance risks becoming a high-tech tool for maintaining inequality rather than solving it.

Beyond the challenges of bias embedded in data and algorithms, a critical additional hurdle emerges: the inherent opacity of black-box AI systems. The same lack of transparency that allows unseen biases to persist also obscures how these models arrive at decisions, creating a void in accountability essential for risk compliance.

A significant challenge in AI systems is the difficulty of identifying and quantifying biases.

Algorithmic bias is particularly hard to detect and measure when AI operates as a "black box" with inscrutable or opaque mechanisms for decision making.Bias can originate from multiple sources, including training data, algorithm design, and user interactions. Its complexity complicates the ability to isolate and rectify biases, and thus weakens the impact of bias-mitigation tools such as bias-aware algorithms or user feedback systems [13].

This opacity is particularly perilous in financial systems, where "black box" machine learning algorithms for credit scoring are too complex for regulators to verify compliance with fairness rules or financial laws, impeding risk compliance audits and sparking debates over stricter regulations versus innovation limitations. As that research notes, the complexity of these algorithms makes it difficult to determine if the biases are due to data issues, algorithm design flaws, or a combination of both. This lack of clarity not only slows down audits but also means that the development of effective debiasing strategies is hampered. For example, some banks using such opaque algorithms may unknowingly be denying loans to certain demographic groups at higher rates, yet the exact cause remains hidden within the black box, fueling the ongoing debate on how to balance regulatory needs with the drive for innovative AI - powered financial services[12].

2.1.3 Consequences of Algorithmic Bias

The opacity of AI models undermines stock market integrity by amplifying cognitive and algorithmic biases. As Gonzales & Hargreaves [14] demonstrate, AI-driven trading systems trained on historical data often exhibit overconfidence, executing excessive trades that deviate from fundamental values. Herd behavior in algorithms, such as mimicking market trends, can boost price volatility by 15-23% in the context of high-frequency trading, as reported by Kumar et al. who question the Efficient Market Hypothesis (EMH). They find that biased AI decisions disrupt price equilibrium, resulting in 8-12% capital misplacing errors for stock valuation, and thus, leads to a high risk of crash [15].

Failure of regulation emanates from “black box” issues: Oguntibeju notes that over 60-70% of algorithm biases cannot be traced to roots (e.g., flawed data vs. design flaws) by auditor, as seen in credit scoring models where 45% of bias complaints lack transparent accountability pathways[12]. In stock markets, the opacity results in post-crash investigations on average being delayed 20-30 days, eroding investor confidence and subjecting markets to systemic risks. Such opaqueness undermines confidence in financial AI systems, and increases risk for investors and consumers.

The pervasiveness of AI bias in financial markets, as outlined, has spurred regulatory responses in the EU and US to combat discriminatory algorithmic outcomes. While legislative initiatives like the EU AI Act and US regulations aim to enforce transparency and fairness, their efficacy remains constrained by the inherent complexity of AI systems. These efforts, though well-intentioned, often struggle to dismantle deeply entrenched biases, paving the way for an analysis of persistent challenges in achieving equitable AI governance.

2.2 Current Status and Challenges and Responses to Algorithmic Discrimination in the US and Europe

In the EU, the *General Data Protection Regulation (GDPR)* [16] is an effort to counter algorithmic discrimination by banning automated decisions based on sensitive data (e.g., race, gender) and requiring“ data sanitization” to remove bias from training datasets. But the law struggles to combat indirect discrimination, where algorithms can deduce sensitive attributes from proxy variables (e.g., zip codes, purchasing behavior) that are correlated with protected characteristics [17]. For example, even when explicit demographic data is excluded, algorithms may use correlated non-sensitive data (e.g., education level, geographic location) to perpetuate bias, a phenomenon termed “omitted variable bias” in econometric models [17].

In the U.S., proposed legislation like the Algorithmic Accountability Act [16] suggests that impact assessments will be required for high-risk AI systems, specifically in the context of hiring and criminal justice. Despite that, enforcement gaps persist: Amazon’s AI hiring tool exhibited gender bias by favoring male resumes [16], while the COMPAS recidivism risk tool disproportionately labeled Black defendants as high-risk[16]. These cases highlight how “black box” algorithms evade meaningful audit, as even developers struggle to explain their decision-making processes [6] Meanwhile, in financial services, AI-powered credit scoring systems may inadvertently disadvantage low-income groups due to biased training data reflecting historical inequities [6].

Across jurisdictions, three systemic barriers allow for the perpetuation of discrimination: 1) Algorithmic opacity: Machine learning models, especially large language models (LLMs), defy human interpretation, making bias detection nearly impossible [6]; 2) Data bias persistence: Historical datasets frequently capture societal prejudices (e.g., underrepresentation of minorities in hiring data), which AI systems unwittingly replicate [17]; and 3) Jurisdictional fragmentation: Global AI systems outstrip local regulations, exemplified by cross-border e-commerce and fintech, where bias mitigation relies on voluntary industry standards rather than enforceable law [6].

To conclude, although the EU and U.S. have taken legal steps to combat algorithmic discrimination, they are hampered by technical complexity, data biases, and regulatory gaps. As *IOSCO* warns, the rise of autonomous AI agents and generative AI (e.g., ChatGPT) will only exacerbate these challenges, necessitating cross-disciplinary collaboration and global regulatory coordination[6]

As the challenge of eradicating algorithmic discrimination in AI endures, AI's integration with DeFi extends well beyond smart contracts, intersecting with multiple application layers such as automated trading, risk assessment, and liquidity management. Despite the vast potential these intersections offer, scholarly exploration of the intertwined risks and opportunities across these diverse touchpoints remains in its nascent stages, thus leaving a significant gap in the existing research body.

2.3 Studies on fusion of Artificial intelligence (AI) and Decentralised Finance (DeFi)

The combination of AI and DeFi is becoming a transformative frontier, with current applications spanning smart contract optimization, automated trading, and risk assessment [18][19]. These technologies hold promise to enhance DeFi’s efficiency, accessibility, and security through AI-driven insights and automation [18] AI could enable more sophisticated risk management, personalized financial services, and decentralized autonomous organization (DAO) governance, potentially democratizing financial tools globally [19].

But there are still technological flaws. The opacity of AI’s "black box" models (e.g., deep learning algorithms) undermines trust, as users and regulators struggle to validate decision-making logic [18]. For instance, AI-driven trading strategies may inadvertently amplify market biases or propagate systemic risks due to hidden correlations in training data [19]. Moreover, security

vulnerabilities are also introduced when DeFi relied on AI based on the integrity of data, corrupted or biased data could sabotage DeFi protocols and lead to attacks such as smart contract hackings or flash loan attacks [18].

Exacerbating these issues, *arbitrage and AI* literature [20] highlights key risks of AI-DeFi integration. Model overfitting tops the list, and AI trained on past market information fails to adjust to new conditions or regulations, noting the dysfunctional volatility assessments during the 2020 "Black Thursday" crypto crash [20]. Computational overhead increases liquidity risks because advanced AI algorithms require a lot of resources, which slows down high-frequency trading and delays quick decisions that are crucial for arbitrage. [20]. Interpretability gaps in "black box" deep learning models hinder accountability, enabling undetected algorithmic bias or compliance failures from hidden data dependencies [20]. Lastly, reliance on outdated historical datasets leaves AI vulnerable to regulatory mismatches, such as pre-2023 models failing to adapt to new EU AML rules [20]. Collectively, these risks of overfitting, latency, opacity, and data obsolescence highlight the need for robust governance to reduce systemic vulnerabilities in AI-DeFi systems.

Regulations remain critically under-developed. Current laws lack clarity on liability for AI-generated outcomes in DeFi, such as losses from algorithmic errors or malicious AI manipulation [19]. Moreover, data privacy is another challenge: AI's need for extensive user data conflicts with DeFi's decentralized ethos, yet no uniform standards govern data usage across jurisdictions [18]. Consequently, without robust regulations to address model accountability, cross-border data governance, and ethical AI deployment, the AI-DeFi ecosystem risks exacerbating financial instability and inequity. To address this issue, the bridging of these gaps demands interdisciplinary teamwork for transparent AI architectures, as well as adaptive legislation[18][19].

On top of such challenges, existing regulatory attempts to address AI and DeFi risks remain fragmented and reactive, as shown in five literatures. For instance, a Chinese scholar points out that China's strict ban on DeFi-related financial services (Sun, 2024)[1], while Europe follows a principles-based approach under MiCA, focusing on transparency but lacking detailed rules for AI-integrated DeFi protocols. The EU's new crypto anti-money laundering rules, though reflecting regulatory momentum, do not address AI-DeFi integration specifics, further illustrating regulatory gaps in cross-technology oversight. Similarly, the U.S. Securities and Exchange Commission (SEC) has applied traditional securities laws to DeFi tokens, as evidenced by the SEC vs Ripple case (2023), where XRP's classification as an "investment contract" under the Howey test demonstrates regulatory ambiguity for AI-augmented token ecosystems[22].

IOSCO raises concerns over "black box" AI models in trading, citing Nasdaq's Dynamic M-ELO order type proposing a reinforcement learning-driven system with opaque decision-making that raises red flags about market manipulation and systemic risk [6]. Similarly, research highlights how AI-powered algorithmic trading in DeFi exacerbates liquidity risks during market crashes, but existing regulations like the CFTC's 2024 guidance on AI in derivatives markets focus on individual components rather than integrated AI-DeFi systems [23].

Insightful research on regulatory framework on DeFi, which advocates for hybrid human-AI governance nonetheless overlook the unique risks arising from AI-DeFi convergence[24]. In particular, none address how AI's data bias (e.g., in credit-scoring models) interacts with DeFi's decentralized anonymity to entrench financial exclusion, or how generative AI's deepfake capabilities could undermine KYC/AML compliance in borderless DeFi networks. Also, there isn't much talk about how AI's ability to make decisions on its own (like smart contracts that automatically execute based on machine learning risk factors) challenges the rules about responsibility in DeFi's trustless system.

In summary, existing works critique regulatory gaps in AI or DeFi but fail to synthesize strategies for their synergistic risks (e.g., algorithmic bias in lending). The lack of cross-disciplinary frameworks leaves regulators unprepared for systemic risks from AI-DeFi integration, urging collaboration. Meanwhile, literature on AI-DeFi integration for risk management ignores cross-chain interoperability, privacy, and ethical issues.

3. Future Direction

AI and DeFi convergence toward creative financial development - smart contract optimization and automated trading, it brings complex synergistic risks, including algorithmic bias, "black box" opaqueness, fragmented cross-border regulations, but raises new challenges - adversarial attacks on AI models, market homogenization induced by algorithmic herding, governance conflicts of AI autonomy and DAO structures. Looking forward, future research must adopt a proactive, interdisciplinary approach to anticipate and mitigate these interconnected risks. Key areas of focus should include developing robust frameworks to detect and defend against adversarial attacks on AI-driven DeFi protocols, exploring decentralized machine learning architectures to reduce market homogenization by promoting diverse algorithmic strategies, and reconciling AI's autonomous decision-making with decentralized governance through transparent governance interfaces that enable DAO communities to audit and vote on algorithmic parameters. Additionally, bridging the user cognitive divide requires designing explainable AI interfaces for DeFi products alongside educational frameworks to empower users with insights into algorithmic risks. On the regulatory front, global collaboration must prioritize harmonizing cross-border rules for AI-DeFi systems, addressing liability for AI-generated outcomes, data privacy, and preventing generative AI-facilitated financial crimes. The incorporation of sustainability through low-carbon AI models supportable by energy-saving blockchain technologies will provide great synergy between technological advancement and the environment. By now arriving at interdisciplinary cooperation between computer science, finance and law, future research can in turn realise agile, resilient ecologies that apply the promise of AI-DeFi while maintaining safety, equity, and regulatory agility in an increasingly international financial market.

4. Conclusion

The integration of AI and DeFi presents transformative opportunities for financial innovation, with applications ranging from multi-model trust scoring frameworks for DeFi projects (combining LLMs and ML algorithms to assess smart contract vulnerabilities, price anomalies, and social sentiment) and AI-driven smart contract security enhancements via NLP and deep learning to fraud detection using graph neural networks and AI agent-driven user engagement in GameFi. However, this convergence introduces critical synergistic risks, including algorithmic bias embedded in training data (e.g., gender bias in Apple Card's credit algorithms and racial disparities in loan approvals via residential proxies), which perpetuate financial discrimination across lending, insurance, and mortgages. This issue is exacerbated by the "black box" opacity of AI models that hinders bias detection, regulatory auditability, and accountability. This opacity also amplifies market risks, such as AI-driven trading overconfidence triggering price volatility and systemic vulnerabilities. Regulatory frameworks in the EU and U.S. while aiming to address transparency and fairness face systemic gaps: technical complexity prevents effective bias mitigation, historical data biases persist, and jurisdictional fragmentation fails to tackle cross-border risks like AI bias interacting with DeFi's decentralized anonymity to entrench financial exclusion or generative AI undermining KYC/AML compliance. The current literature is overwhelmingly focused on isolated AI or DeFi risks and neglecting the cross-disciplinary liability in AI autonomous smart contracts, cross-chain interoperability, and ethical issues to poorly deploy global regulators for the mixer risk of AI-DeFi fusion, indicating that it's of great urgency to propose the collective legal frameworks.

References

[1] Mothukuri, V., Parizi, R. M., Massa, J. L., & Yazdinejad, A. (2024). An AI multi-model approach to DeFi project trust scoring and security. 2024 IEEE International Conference on Blockchain (Blockchain) (pp. 1–8). IEEE. https://ieeexplore.ieee.org/document/10664378

[2] Krichen, M. (2023). Strengthening the security of smart contracts through the power of artificial intelligence. Computers, 12(5), 107. https://doi.org/10.3390/computers12050107

[3] Sadman, N., Ahsan, M. M., Rahman, A., & Siddique, Z. (2022). Promise of AI in DeFi, a systematic review. Digital, 2(1), 88–103. https://www.researchgate.net/publication/359199275_Promise_of_AI_in_DeFi_a_Systematic_Review

[4] Luo, B., Zhang, Z., Wang, Q., Ke, A., & Lu, S. (2023). AI-powered fraud detection in decentralized finance: A project life cycle perspective. arXiv preprint arXiv:2308.15992. https://arxiv.org/abs/2308.15992v1

[5] Jia, F., Zheng, J., & Li, F. (2024). Decentralized intelligence in GameFi: Embodied AI agents and the convergence of DeFi and virtual ecosystems. arXiv preprint arXiv:2412.18601. https://arxiv.org/abs/2412.18601

[6] International Organization of Securities Commissions (IOSCO). (2025). Artificial intelligence in capital markets: Use cases, risks, and challenges (Board/2025/017). https://www.iosco.org/library/pubdocs/pdf/IOSCOPD643.pdf

[7] Ukanwa, K., & Rust, R. T. (2021). Algorithmic bias in service (USC Marshall School of Business Research Paper No. 69). SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3654943

[8] Akter, S., et al. (2022). Algorithmic bias in machine learning-based marketing models. Journal of Business Research, 144, 201–216. https://www.sciencedirect.com/science/article/pii/S014829632200083X

[9] Buolamwini, J. (2023). Unmasking AI: My mission to protect what is human in a world of machines. Random House.

[10] Chouldechova, A., & Roth, A. (2020). A snapshot of the frontiers of fairness in machine learning. Communications of the ACM, 63(5), 82–89. https://doi.org/10.1145/3376898

[11] Huang, M.-H., & Rust, R. T. (2021). A strategic framework for artificial intelligence in marketing. Journal of the Academy of Marketing Science, 49(1), 30–50. https://doi.org/10.1007/s11747-020-00749-9

[12] Oguntibeju, O. O. (2024). Mitigating artificial intelligence bias in financial systems: A comparative analysis of debiasing techniques. Asian Journal of Research in Computer Science, 17(12), 165–178. https://doi.org/10.9734/ajrcos/2024/v17i12536

[13] Ferrara, E. (2024). Fairness and bias in artificial intelligence: A brief survey of sources, impacts, and mitigation strategies. Sci, 6(1), 3. https://doi.org/10.3390/sci6010003

[14] Gonzales, R. M. D., & Hargreaves, C. A. (2022). How can we use artificial intelligence for stock recommendation and risk management? A proposed decision support system. International Journal of Information Management Data Insights, 2(2). https://doi.org/10.1016/j.ijimei.2022.100130

[15] Kumar, P., et al. (2022). Charting the intellectual structure of customer experience research: A bibliometric analysis. Marketing Intelligence & Planning. https://doi.org/10.1108/MIP-05-2022-0185/full/html

[16] Chen, Q., & Liu, Q. (2022). Legal regulation of algorithmic discrimination in AI: European and American experiences and Chinese path. Jinchutou. https://m.jinchutou.com/shtml/view-317595760.html [In Chinese]

[17] Williams, B. A., et al. (2018). How algorithms discriminate based on data they lack: Challenges, solutions, and policy implications. Journal of Information Policy, 8, 78–115. https://doi.org/10.5325/jinfopoli.8.2018.0078

[18] Sadman, N., Ahsan, M. M., Rahman, A., Siddique, Z., & Gupta, K. D. (2022). Promise of AI in DeFi, a systematic review. Digital, 2(1), 88–103. https://doi.org/10.3390/digital2010006

[19] Sadman, N., Rahman, A., & Gupta, K. D. (2021). Promise of AI in DeFi, a literary analysis. Preprints. https://doi.org/10.20944/preprints202110.0136.v2

[20] Hazarika, A. V., Shah, M., Patil, S., & Shukla, P. (2024). Risk management for distributed arbitrage systems: Integrating artificial intelligence. International Journal of Science and Research (IJSR), 13(12), 1250–1253.

[21] Sun, Z. (2024). On the new regulatory ecology of decentralized finance. Financial Technology, 1, 1–48. https://www.cnki.net [In Chinese]

[22] United States District Court for the Southern District of New York. (2023). SEC vs Ripple Labs, Inc., et al. (Case 1:20-cv-10832-AT-SN). https://www.courtlistener.com/docket/8745308/sec-vs-ripple-labs-inc/

[23] Carapella, F., Dumas, E., Gerszten, J., Swem, N., & Wall, L. (2022). Decentralized finance (DeFi): Transformative potential & associated risks. Finance and Economics Discussion Series (No. 2022-057). Board of Governors of the Federal Reserve System. https://doi.org/10.17016/FEDS.2022.057

[24] Uzougbo, N. S., Ikegwu, C. G., & Adewusi, A. O. (2024). Regulatory frameworks for decentralized finance (DeFi): Challenges and opportunities. GSC Advanced Research and Reviews, 19(02), 116–129. https://doi.org/10.30574/gscarr.2024.19.2.0170