DOI: 10.17148/IJARCCE.2024.131262

Blockchain Enabled Cybersecurity to Protect LLM Models in FinTech

Kavitha Janamolla[1], Sruthi Balammagary[2], Abubakar Mohammed[3]

School of Computer and Information Sciences, University of the Cumberlands, KY[1,2,3]

Abstract: The financial services industry handles transactions amounting to trillions of dollars daily, necessitating a focus on cost-efficiency, transparency, and security. Cybersecurity is the biggest threat to this industry and Blockchain is the only answer to protect data in the growing FinTech space. Prior to the integration of blockchain technology, intermediaries such as money transfer services, stock exchanges, and payment networks frequently encountered cybercrime. Blockchain technology, initially popularized by cryptocurrencies like Bitcoin, has since become a transformative force across various financial sectors. This technology enhances the industry by providing secure, transparent, and cost-effective transaction protocols through encryption and algorithms. This prose explores the significant advancements blockchain has brought to financial services, emphasizing its role in revolutionizing insurance, asset management, banking, and the stock market. With rapidly increasing use of LLMs in financial sector, blockchain is in the center of data protection and security for this industry in all directives.

Keywords: Blockchain, Financial Services, Cybersecurity, Data Protection, Transaction Transparency, Cost-Efficiency, LLM Security

I. INTRODUCTION

The financial services industry takes part in transactions worth trillions daily. Implementing financial transactions requires prioritizing cost-efficiency, transparency, and security. Before financial institutions introduced the technology into their operations, business intermediaries like money transfer services, stock exchanges, and payment networks suffered ceaseless cybercrime. According to Ali, Ally, and Dwivedi [1], blockchain technology has experienced remarkable endorsement in the financial services industry because of intrinsic capabilities ensuring a cost-effective, transparent, and secure stream of transactions. Blockchain technology began with cryptocurrencies like bitcoin. Today, it has infiltrated all sectors of the financial services industry. Blockchain provides the industry with ways and protocols of recording transactions using encryptions and algorithms. These protocols ensure commercial activities are convenient, irrevocable, and trustworthy to everyone in the blockchain system. Therefore, this prose will expound on the advancements blockchain has had on the financial industry. The discussion will articulate the technology as the primary accelerator of the positive changes in financial services like insurance, asset management, banking, and the stock market.

II. FINTECH USE CASES

a) Quick clearance of payments in stock markets

Blockchain technology is a cloud-based ledger of transactions that is easy to access, tamper-proof, and secure. Blockchain, similar to the internet, has no dominant authority. The record of transactions comprising data blocks with patches of transactions is interlocked and secured with advanced cryptography. This setup promotes rapid settlements in stock markets because it reduces operational costs and transaction time [2]. Blockchain automates compliance using smart contracts, which have an enhanced level of transparency and security [3]. For example, the National Association of Securities Dealers Automated Quotations (NASDAQ) uses the technology to share and issue private securities. The London Stock Exchange and cross-industry institutions are leveraging blockchain to transform the trade of securities in Europe [4]. Major stock exchanges across the globe are also looking to harness the potential of the technology.

b) Asset Management

International trade and business are increasing on a daily basis. Asset management is one of the most lucrative markets, with tens of trillions of dollars expected to be generated by the end of the 2025 fiscal year. The supply chain and asset management network use blockchain to centralize digital systems and provide clients and dealers real-time visibility of resources within the system. Traditional centralized data management solutions laid the foundation for constructing a distributed network of digital ledger systems. Blockchain replaced the traditional complex, time-consuming data management system, providing the asset management sector with direct settlements and trading across boundaries. The technology is helping the sector reduce process delays, increase data accuracy, and cut costs [5]. Besides, the technology has helped circumvent vulnerabilities to misinterpretation, fraud, and errors during the transaction of assets [6]. Funds

DLT is an excellent example of a blockchain-driven funds allotment platform using the intervention in the asset management sector [7].

c) Efficient Payments

Blockchain technology enhances payment security, trust, efficiency, and transparency, reducing detriments imparted to financial services users and firms. Before the inception of blockchain, payments across banks used to take weeks. However, with blockchain, these transactions take place instantly[6]. Digital distributed ledgers and currencies make payment convenient, cheaper, and faster. Central banks across the globe have revamped payments by incorporating distributed ledgers in existing systems. The technology saves substantial amounts of money and time for all parties involved in payment transactions. Besides, blockchain has successfully eliminated the need for back and middle-office staff because it settles payments instantly. The Bank of Canada uses project Jasper to leverage the advantages blockchain provides operational risk and settlement finality. The financial authority of Singapore, project Ubin, is also using the same approach to ease the problem of slow, expensive payments [8].

d) Enhanced compliance processes

Know Your Customer (KYC) is an indispensable requirement for all organizations in the financial services industry because these businesses report and comply with regulations issued by local regulators. The compliance process can be error-prone, labor-intensive, and time-consuming, especially for organizations using traditional systems. Blockchain endows financial institutions with services like KYC-chain to help them streamline their compliance processes [4]. The technology provides financial institutions with real-time KYC updates and empowers efficiency through increasing trust and reducing workload duplication. Blockchain automates client identification by availing a single source of digital credentials, facilitating the smooth interchange of documents between financial institutions and other sources. Digital identification of customers helps maintain data privacy, reduce transaction costs, and automate the account opening process while maintaining all legal requirements.

d) Corruption-free and fair insurance claim management

Blockchain is helping the insurance sector make progressive steps towards the automation of claim processing and sorting using smart contracts. Blockchain facilities like centralized authentication, effortless access to client history, and data sharing across industries have enhanced claim settlement by making it corruption-free [6, 9]. Manual claim settlement involved communication occurring between several stakeholders comprising banks, insurers, brokers, and clients. These interactions were inefficient and time-consuming because they required excessive reconfirmation and crosschecking. With blockchain technology, communication occurs through shared, secured networks, which streamline the process and increase efficiency. Shared ledgers allow all parties in the network to see the history and status of transactions, ensuring resourceful cooperation among business and their clients. LenderBot is an example of how micro-insurance companies leverage the benefits tagged with blockchain technology [7].

III. RISE OF LLMS IN FINTECH

LLMs, such as OpenAI's GPT-4 or Meta’s Llama or Google's Palm, have transformed various industries, including FinTech, by automating tasks that require language understanding. These models are used in several FinTech applications, such as:

Fraud detection: LLMs analyze transactional data and communication patterns to identify potentially fraudulent activities [8, 10].

Customer support: AI-powered chatbots and virtual assistants provide real-time assistance to clients, enhancing customer experiences [10].

Algorithmic trading: LLMs predict market trends, assisting in making informed investment decisions [11].

Risk management: LLMs process vast amounts of financial data to assess and predict risks more accurately [11].

While these capabilities offer significant advantages, the use of LLMs in the financial sector also opens up new vulnerabilities. Cybercriminals are increasingly targeting AI models, attempting to manipulate or steal sensitive information, which could have severe consequences in a financial setting.

IV. CYBERSECURITY CHALLENGES FOR LLMS IN FINTECH

The integration of LLMs into FinTech applications introduces unique cybersecurity challenges:

Data poisoning: Adversaries may manipulate the training data fed into LLMs, resulting in biased or incorrect outputs (see Figure 1). In the FinTech sector, this could lead to flawed risk assessments or fraudulent transactions being overlooked.

```
Training Data --> Block 1 (Stored in Blockchain)
                     |
          Block 2 (New Data Update)
                     |
           Block 3 (Model Update)
                     |
     Blockchain Ledger (Immutable Record)
```

Figure 1. Flowchart showing Immutable Blockchain Record for LLM Model Training [11]

Model inversion attacks: Hackers could reverse-engineer the AI model to extract sensitive data, such as proprietary algorithms or private client information, potentially violating privacy regulations like GDPR.
Adversarial attacks: Cyber attackers can feed malicious inputs into the LLM, causing the model to make erroneous predictions or decisions. In finance, this could lead to incorrect financial advice or investment choices that harm both institutions and clients [12, 13].
Lack of transparency: LLMs are often considered "black boxes," meaning their decision-making processes are difficult to interpret. This opacity raises concerns over accountability and regulatory compliance in financial services [12-14].
Model theft: Cybercriminals may steal or replicate proprietary AI models, which could then be used to exploit financial systems or data.

V. BLOCKCHAIN: A SOLUTION TO LLM SECURITY CHALLENGES

Blockchain technology, which underpins cryptocurrencies like Bitcoin, is gaining attention as a potential solution to mitigate the cybersecurity risks associated with LLMs in FinTech. Blockchain offers several key features that can enhance the security, integrity, and transparency of LLMs:

1. Immutable Record of Model Training and Data

Blockchain's immutable ledger ensures that every change made to an LLM, whether it's an update to the model or the data used for training, is securely recorded. This tamper-proof record makes it easy to trace the history of a model's development, ensuring that it has not been manipulated or poisoned during training [16].
Application: In the event of a dispute or investigation, FinTech companies can use the blockchain to prove that the model has not been tampered with and verify the authenticity of its training data.

2. Decentralized Model Validation

In a traditional setup, a single entity is responsible for verifying the integrity of an AI model. With blockchain, multiple independent parties can participate in validating the model's output or training data [17]. By utilizing a decentralized approach, it becomes more difficult for a single entity to compromise the system.
Application: FinTech firms can use blockchain to establish a consortium of trusted entities to verify the accuracy and fairness of their LLMs. This decentralized validation can prevent fraudulent or malicious actors from altering models undetected.

3. Enhanced Transparency and Auditing

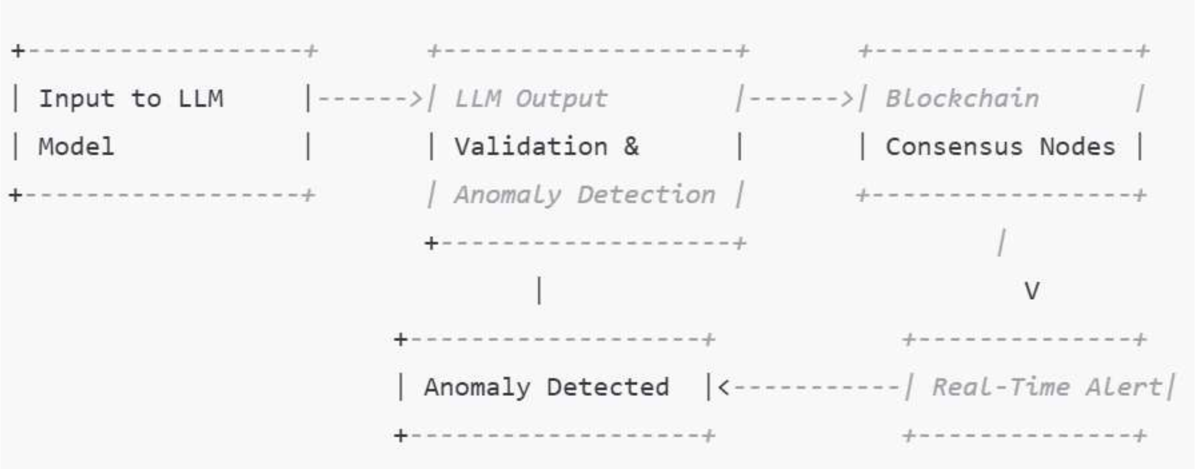
Blockchain's transparent nature allows for real-time tracking of LLMs and their decision-making processes. For highly regulated sectors like FinTech, this feature is particularly crucial for ensuring that models comply with industry standards and regulations. Blockchain can provide a detailed audit trail of how decisions were made, what data was used, and when changes were made to the model.
Application: Regulators can use blockchain to audit LLM decisions and data usage, ensuring that financial institutions remain compliant with laws like the EU's GDPR or the US's Dodd-Frank Act. This level of transparency also builds trust with customers, who can verify that their data is being used responsibly [16, 18].

4. Protection Against Model Theft

Blockchain can be employed to secure the intellectual property (IP) of LLMs. By storing the model's parameters and weights on a blockchain, it becomes more difficult for unauthorized parties to steal or replicate the model. Each time the model is used, its provenance can be verified, ensuring that only authorized users have access.
Application: Financial institutions can protect their proprietary models from theft or unauthorized use by encrypting them and storing the encrypted model on the blockchain [17]. This way, access is restricted, and any attempt to steal the model would be immediately traceable.

5. Secure Data Sharing and Collaboration
In FinTech, data-sharing and collaboration among different entities, such as banks, insurers, and regulatory bodies, are critical for making accurate decisions. Blockchain provides a secure way to share data without revealing sensitive information. The use of smart contracts can automate data access while ensuring that data remains private and secure.
Application: Different financial institutions can share customer data, transaction histories, or market trends with each other via blockchain, while ensuring that the data remains encrypted and that the transactions are auditable. This ensures data privacy and allows the secure, collaborative use of LLMs.

6. Real-time Detection of Malicious Activity
Blockchain networks can leverage consensus algorithms and anomaly detection techniques to identify suspicious activities in real-time (See Figure 2). If an LLM model begins to produce unusual outputs, blockchain's decentralized structure can quickly alert stakeholders to potential issues, such as adversarial attacks or model poisoning [17].



```
+------------------+       +------------------+       +-----------------+
| Input to LLM     |------>| LLM Output       |------>| Blockchain      |
| Model            |       | Validation &     |       | Consensus Nodes |
+------------------+       | Anomaly Detection |      +-----------------+
                           +------------------+                |
                                    |                          v
                         +------------------+          +-------------+
                         | Anomaly Detected |<---------| Real-Time Alert|
                         +------------------+          +-------------+
```

Figure 2. Blockchain-Enabled Real-Time Detection of Malicious Activity

Application: In the event of a cyberattack, such as an adversarial input attack on a trading algorithm, blockchain can automatically flag and alert relevant parties [18]. This ensures that corrective actions can be taken swiftly to minimize financial damage.

VI. CONCLUSION

Blockchain is being progressively adopted by the financial services industry to modernize the worldwide financial system and make it more efficient and secure. The keyways blockchain has advanced the financial services industry have been identified in this discussion. According to this discussion, cross-border settlements are the most profound advancement as blockchain enriches the industry with a transparent, cost-efficient global network. Financial institutions use the technology to drive under costs and provide service seekers with more values like the convenience of easily accessible information and timesaving. Ultimately, trading is the primary business element in the financial services industry, and all successful transactions depend on trust. Blockchain technology provides financial institutions with instruments that build trust between them and their clients. These digital ledgers enable businesses to evaluate whether users are trustworthy. They help provide real-time information on credit status, transactional history, and other information that help determine the efficiency of financial transactions. The financial services industry's next big thing, after the internet, is blockchain technology. Digital ledger technology has the ability to alter financial institutions by improving activity separation, boosting transparency, speeding up settlements, and lowering costs, among other things. Blockchain has provided the market a new digital asset due to the lack of a centralized authority.

REFERENCES

1. Ali, O., Ally, M., & Dwivedi, Y. (2020). The state of play of blockchain technology in the financial services sector: A systematic literature review. International Journal of Information Management, 54, 102199.
2. Arslanian, H., & Fischer, F. (2019). Blockchain as an enabling technology. In The Future of Finance (pp. 113-121). Palgrave Macmillan, Cham.
3. Dhanda, N., & Garg, A. (2021). Revolutionizing the Stock Market With Blockchain. In Revolutionary Applications of Blockchain-Enabled Privacy and Access Control (pp. 119-133). IGI Global.

4. Frikha, T., Chaabane, F., Aouinti, N., Cheikhrouhou, O., Ben Amor, N., & Kerrouche, A. (2021). Implementation of Blockchain Consensus Algorithm on Embedded Architecture. Security and Communication Networks, 2021.
5. Kapsoulis, N., Psychas, A., Palaiokrassas, G., Marinakis, A., Litke, A., & Varvarigou, T. (2020). Know your customer (KYC) implementation with smart contracts on a privacy-oriented decentralized architecture. Future Internet, 12(2), 41.
6. Knezevic, D. (2018). Impact of blockchain technology platform in changing the financial sector and other industries. Montenegrin Journal of Economics, 14(1), 109-120.
7. Lamberti, F., Gatteschi, V., Demartini, C., Pelissier, M., Gomez, A., & Santamaria, V. (2018). Blockchains can work for car insurance: Using smart contracts and sensors to provide on-demand coverage. IEEE Consumer Electronics Magazine, 7(4), 72-81.
8. Treleaven, P., Brown, R. G., & Yang, D. (2017). Blockchain technology in finance. Computer, 50(9), 14-17.
9. Vallabhaneni, R. (2024). Effects of Data Breaches on Internet of Things (IoT) Devices within the Proliferation of Daily-Life Integrated Devices.
10. Janamolla, K. R., & Syed, W. K. (2024). Global Banking Exploring Artificial Intelligence Role in Intelligent Banking to Automate Trading Platform. International Journal of Multidisciplinary Research and Publications (IJMRAP), 6(12), 163–168
11. Khadri Syed, W., & Janamolla, K. R. (2023). Fight against financialcrimes – early detection and prevention of financial frauds in thefinancial sector with application of enhanced AI. IJARCCE, 13(1), 59–64. https://doi.org/10.17148/ijarcce.2024.13107
12. Mohammed, S. (2024). Ai-Driven Drug Discovery: Innovations and challenges. IJARCCE, 13(6).
13. Mohammed, Z. A., Mohammed, M., Mohammed, S., & Syed, M. (2024). Artificial Intelligence: Cybersecurity threats in pharmaceutical IT systems. IARJSET, 11(8). https://doi.org/10.17148/iarjset.2024.11801
14. Dash, B. (2024). Zero-Trust Architecture (ZTA): Designing an AI-Powered Cloud Security Framework for LLMs' Black Box Problems. Available at SSRN 4726625.
15. Zhang, B., Liu, Z., Cherry, C., & Firat, O. (2024). When scaling meets llm finetuning: The effect of data, model and finetuning method. arXiv preprint arXiv:2402.17193.
16. Mohammed, S., Mohammed, N., & Sultana, W. (2024). A Review of AI-powered Diagnosis of Rare Diseases. International Journal of Current Science Research and Review, 7(09).
17. Geren, C., Board, A., Dagher, G. G., Andersen, T., & Zhuang, J. (2024). Blockchain for large language model security and safety: A holistic survey. arXiv preprint arXiv:2407.20181.
18. Mohammed, S., & Panda, N. R. (2024). Block Chain Technology in the Pharmaceutical Supply Chain: Enhancing Transparency and Security.