Financial Engineering and Risk Management (2025)
Clausius Scientific Press, Canada

DOI: 10.23977/ferm.2025.080219
ISSN 2523-2576 Vol. 8 Num. 2

The Application and Challenges of Artificial Intelligence in Preventing Cyber Financial and Blockchain Crimes

Yewei Sun*

Universidad de Murcia, Murcia, Spain
**Corresponding author: 1157485898@qq.com*

Keywords: Finance in the Age of Artificial Intelligence; Preventing Online Financial Crime; Blockchain Technology

Abstract: This paper closely examines the development trajectory of the financial sector in the era of artificial intelligence, conducting an in-depth analysis of the current state, characteristics, and causes of online financial crimes. It focuses on exploring the principles, applications, and challenges of blockchain technology in preventing online financial crimes, aiming to propose practical crime prevention strategies from a financial professional perspective to safeguard the security and stability of the online financial industry in the age of artificial intelligence.

1. Introduction

1.1 Research Background and Significance

Artificial intelligence technology has efficiently embedded itself in all areas of financial services in the past couple of years. From risk evaluation to transaction monitoring, its intelligent analytical capabilities enable financial services to more quickly and effectively assess risky or anomalous behaviors. This affects operational efficiency and changes the operational model of the financial services industry. At the same time, online financial services, including mobile payments and internet borrowing, are growing rapidly. There are more and more users using these simple services for their everyday consumption and investment purposes, thereby further confirming the role of the financial system in facilitating economic activities. With the digitization of financial activities increasing, the sophistication of cybercrime is also increasing. Blockchain technology and its distributed ledger and immutable characteristics provide new ways to track transaction paths and prevent fraudulent activity. Researching the applications of blockchain technology has become an important part of protecting financial security.

1.2 Current State of Domestic and International Research

Research institutions from several countries around the world are trying hard to find actionable ways to connect artificial intelligence and blockchain technology to prevent financial crime. Banks in several European and American countries have already implemented transaction monitoring solutions based on machine learning (ML) algorithms. These technologies can automatically review

public ledger records on blockchains and identify abnormal fund flow patterns, such as routing funds through multiple layers of cryptocurrency transfers closely correlated to money laundering patterns. This suggests that technological innovation can provide new tools for financial regulation across countries. In comparison, domestic academia has been more active in theoretical engagement in this space. Several university research institutes have published research that exemplifies using smart contracts for anti-fraud purposes, and financial institutions have begun testing behavioral analysis models for risk control on online lending platforms. However, there are significant challenges to existing research - most notably, obvious data silos and lack of real-world scenarios. For example, there are currently no effective models for sharing risk-related information between different fintech companies, which in some cases, ultimately undermines the overall effectiveness of the prevention and control framework [1].

1.3 Research Methods and Innovative Contributions

This research systematically examines important academic literature on AI-driven anti-fraud technologies around the world, conducts comprehensive analysis of representative financial crimes involving blockchain, collects data points from partner financial institutions to review real-world risk warning effectiveness, and compares the applicability of technical solutions across different countries. In the paper's interventions, we introduce a dynamic behavioral analysis model to assess fund flow patterns, examine smart contract audit solutions in low value, high-frequency transaction situations, and consider collaborative or joint governance structures as a way to work out data silos between financial institutions. These solutions create tangible, operational technical avenues to ameliorate the gaps and delays in response time of existing systems.

2. Characteristics of Financial Development in the AI Era

2.1 Current Applications of AI Technology in the Financial Sector

Currently, banks and other financial companies use artificial intelligence programs as a regular part of their operations for processing credit approvals. AI systems autonomously deliver credit report assessments as well as predictive models of risk exposure based on users' historical transaction data matched with behavior data. In securities trading markets, intelligent algorithms that scan for abnormal price movements can swiftly pinpoint apparent market manipulation of price behaviors. Intelligent customer service systems intended for consumers are now capable of resolving the majority of inquiries and complaints by reviewing and analyzing previously unseen telephone conversations with representatives while relating specific phrases or indicators for any potential risk exposures. Financial institutions manage the risk at the back end with artificial intelligence risk control programs that leverage the theory and practical application of machine learning to deliver scoring models that analyze users' transaction behaviors. When suspicious account transfer behaviors (significantly outside of normal patterns) are detected, they will automatically trigger verification of the behaviors. Collectively, these artificial intelligence applications are fundamentally reshaping the way financial institutions deliver financial services and products by refining business processes through increased automation and improved proactivity to risk preventative measures.

2.2 Innovation in Financial Business Models in the AI Era

Driven by artificial intelligence technology, financial institutions are progressively establishing personalized service models centered on customer needs. Various financial service platforms utilize

intelligent algorithms to analyze users' historical transaction data, forming precise customer profiling systems that generate investment portfolio recommendations aligned with individual risk tolerance levels. This personalized service model has spurred widespread adoption of smart investment advisory tools. These tools automatically adjust asset allocation ratios in response to market fluctuations, enabling investors with varying capital scales to access professional wealth management services. Concurrently, risk control systems incorporate multi-factor verification protocols. Upon detecting abnormal login activity, they immediately activate facial recognition procedures and flexibly initiate manual review for high-risk transactions. The insurance sector leverages driving behavior analytics to develop real-time premium pricing models, integrating actual mileage and driving habits into premium calculations. These innovations not only diversify financial service offerings but also propel traditional operations toward dynamic, intelligent transformation from standardized processes [2].

2.3 New Developments in Financial Markets in the AI Era

Artificial intelligence technology is driving continuous upgrades to financial market infrastructure. Electronic trading systems can now process millions of orders simultaneously, significantly reducing the time required to match trading instructions. Ordinary investors can now allocate assets across borders through mobile applications, making the buying and selling of various financial products as convenient as everyday online shopping. Lowered market entry barriers have attracted more individual investors to participate in securities trading, while zero-commission policies introduced by some platforms have further stimulated market activity. Regulators are leveraging data analytics tools to track cross-market capital flows, identifying suspicious activities in linked accounts that traditional oversight methods struggle to detect. Both trading frequency and participant numbers in financial markets are growing rapidly, shifting from traditional centralized venues to a 24/7 global interconnected model.

3. Current Status and Characteristics of Online Financial Crime in the AI Era

3.1 Primary Types of Online Financial Crime

Online financial crimes are becoming increasingly diverse, with criminals often posing as bank customer service representatives to send phishing links and obtain user account information. Fraud rings exploit social media platforms to create fake investment groups, luring victims into illegal fundraising activities with promises of high returns. Some criminals establish fraudulent wealth management platforms impersonating legitimate institutions, using forged qualification documents to deceive investors out of their funds. During payment processing, illegal settlements occur through the theft of merchant interfaces, with criminals transferring illicit funds by fabricating transaction backgrounds. In the virtual currency sector, money laundering activities exploit blockchain's anonymity features, with criminals using coin mixing services to obscure fund flows.

3.2 Emerging Features of Online Financial Crime in the AI Era

Fraudsters are using machine learning to identify user behavior patterns to improve the targeting of their scams. Crime is becoming more sophisticated across platforms; transfers of funds can mean rapidly switching between several different payment methods. Payment fraud is an intelligent crime, with fraudsters oftentimes engaging in small test transactions to replicate normal behavior before engaging in large levels of fraud. Some criminal enterprises open corporate accounts in the names of stolen identities and use AI-enabled forged documents to circumvent remote verification.

Fraudsters also evolve continuously, and we have seen criminal methods adapting evasion strategies in automated fashion based on countermeasures in place for the payment system. Further, cybercriminal operations have advanced concealment and adaptability of technology.

3.3 Analysis of Causes Behind Online Financial Crime in the AI Era

The rapid advancement of fintech has significantly lowered the technical barriers for cybercrime, with various automated attack tools proliferating across internet platforms. Criminal organizations exploit vulnerabilities in remote account verification systems, registering numerous shell company accounts using stolen identities. The proliferation of anonymous payment tools like virtual currencies provides covert channels for illicit fund transfers, while discrepancies in cross-border payment systems create practical challenges in tracing capital flows. Data-sharing mechanisms among some financial institutions remain underdeveloped, and inter-institutional risk control coordination suffers from information transmission delays. The pace of regulatory technology development has yet to keep up with the evolution of new criminal methods, necessitating continuous refinement and adjustment of certain risk prevention rules [3].

4. Overview of Blockchain Technology and Its Application Principles in Finance

4.1 Fundamental Concepts and Core Principles of Blockchain Technology

Blockchain approaches transactions and records as a single ordered chain of records, using a chain format, where each node or participant maintains a full set of the history. Hash or hashing algorithms are used to generate unique corresponding codes for each block–modifying any single block invalidates the subsequent block's code, creating a natural method of related tampering. The consensus method to achieve agreement through the network of nodes to the new blocks invalidates any abnormal behavior created by a single node from a majority. The distributed ledger method enables all the participants to view a record of the transaction history, while asymmetric cryptography is used to offload account information. Each block is a new generation of records stacked with encoded verification from the previous block, creating a series of subsequently trusting blocks through each link design.

4.2 Advantages of Blockchain Technology in Financial Applications

The immutable characteristics of blockchain technology provides built-in protection against tampering of financial transaction records because any change to a record will be immediately visible across the network of computers. Its distributed ledger design allows all parties to share synchronized copies of transaction data, preventing an individual player from unilaterally tampering with the ledger. Smart contract capabilities facilitate the execution of the agreed-upon terms of contracts automatically, allowing for funds to be transferred or rights to be distributed when agreed-upon conditions are satisfied. Overall, blockchain-based technology will significantly improve the efficiency of cross-border payments by allowing participants to author trusted individual transfers peer-to-peer and eliminating the time delays or errors involved with using intermediaries in international payments. In the example of supply chain finance, digital ledger participants can access a shared legitimate ledger that tracks the status of accounts receivable in real-time. Similarly, insurance companies can utilize smart contracts to automatically process claims for eligibility, tremendously reducing the time required to perform traditional manual claims processing.

4.3 Application Scenarios of Blockchain Technology in Finance

In the trade finance sector, multiple banking institutions utilize blockchain platforms to process letter of credit transactions, enabling real-time transmission and verification of electronic documents. Corporate clients complete accounts receivable financing through digital bill systems, while creditors can trace the complete circulation history of each bill. Cross-border payment networks leverage distributed ledger technology to establish direct connectivity channels, streamlining traditional multi-step remittance processes into peer-to-peer transfers. In supply chain finance scenarios, upstream and downstream enterprises share a common trusted ledger, enabling real-time visibility into order statuses and capital flows. Asset custody operations incorporate smart contracts to automatically execute fund transfer instructions, triggering interest distributions and principal repayments upon meeting predefined conditions. Regulatory authorities leverage blockchain systems to access real-time transaction data, implementing dynamic monitoring of capital flows among financial market participants [4].

5. Application of Blockchain Technology in Preventing Online Financial Crime

5.1 Blockchain Applications in Fund Flow Monitoring and Anti-Money Laundering

Blockchain technology provides a transparent and traceable solution for monitoring fund flows, with its distributed ledger recording the complete transaction path for every transaction. Financial institutions utilize this technology to establish a mapping between customer identities and transaction addresses, effectively identifying covert multi-layered fund transfers. Regulators leverage blockchain networks to access real-time transaction data, implementing dynamic monitoring of abnormal fund flow patterns. Smart contracts automatically trigger alerts upon detecting transactions exhibiting money laundering characteristics, synchronizing relevant data to anti-money laundering monitoring systems. Financial institutions share risk account information while safeguarding commercial confidentiality, forming a collaborative prevention mechanism. Blockchain's immutability ensures the authenticity of transaction records, providing a reliable chain of evidence for subsequent investigations [5].

5.2 Role of Blockchain in Financial Data Security Protection

Blockchain technology constructs a financial data protection system through a distributed storage architecture, where participating nodes collectively maintain complete copies of transaction records, forming a decentralized data management ecosystem. Financial institutions employ asymmetric encryption algorithms to establish a dual-verification mechanism. Public keys encrypt transmitted data while private keys decrypt access, effectively controlling the scope of sensitive information disclosure. Hash algorithms generate unique digital fingerprints for raw data. Any minor modification triggers a verification failure alert, enabling prompt detection of unauthorized tampering. Enterprises leverage smart contracts to define tiered authorization rules, restricting personnel access to business materials within their designated scope, thereby achieving granular data governance. Timestamp functionality marks each operation with precise temporal coordinates, creating a continuous, irreversible audit trail. Blockchain networks maintain data consistency among nodes through consensus algorithms, making it nearly impossible for any single participant to alter information confirmed across the entire network. This integrated technology suite establishes a secure, multi-party oversight network for financial data, ensuring full traceability throughout its lifecycle [6].

5.3 Blockchain Applications in Financial Regulation

Regulators leverage blockchain systems to establish novel oversight models, accessing financial institutions' transaction data in real time through distributed ledgers. Regulatory sandbox mechanisms permit innovative operations to undergo testing within controlled environments, with regulators setting risk thresholds via smart contracts and implementing dynamic controls. Financial institutions embed compliance requirements into smart contract clauses, enabling automated execution of anti-money laundering transaction screening and large transaction reporting obligations. Blockchain evidence platforms provide immutable audit trails for regulatory inspections, with permanent records generated for every data retrieval operation. Cross-departmental regulatory collaboration leverages consortium blockchain technology to establish data-sharing channels, facilitating joint investigations while safeguarding commercial secrets. Regulators leverage smart contracts' automated execution to conduct compliance audits, with predefined rules triggering risk assessment reports. Blockchain timestamps assist regulators in reconstructing transaction timelines to accurately identify patterns of anomalous activity. Distributed ledger technology enables all nodes to jointly maintain regulatory data, effectively preventing regulatory blind spots caused by unilateral data tampering.

6. Challenges and Countermeasures in Using Blockchain Technology to Prevent Online Financial Crime

6.1 Challenges and Countermeasures at the Technical Level

Blockchain systems face scalability bottlenecks that constrain their ability to process massive volumes of financial transactions. Network congestion frequently causes transaction confirmation speeds to slow significantly. Developers are exploring sharding solutions, which divide the entire network into multiple independently operating subregions to distribute data storage pressure. Security vulnerabilities in smart contract code may be exploited maliciously. Attackers can trigger contract flaws by constructing abnormal transactions to illegally acquire assets. The code audit process requires introducing a mechanism for independent review by multiple experts to identify and fix potential logical errors before contract deployment. Interoperability barriers persist in cross-chain transactions due to inconsistent standards, frequently causing technical compatibility issues when transferring assets between different blockchain networks. Industry organizations are advancing efforts to establish a universal technical standards framework, defining fundamental specifications and security requirements for cross-chain communication. Financial institutions must ensure smooth transitions between legacy and new platforms during system upgrades to prevent disruptions to normal service workflows caused by architectural changes [7].

6.2 Challenges and Countermeasures at the Legal and Regulatory Level

The current legal framework exhibits lag in addressing blockchain-based financial innovations, with existing regulations struggling to fully encompass new technological applications such as smart contracts. Cross-border criminal cases span multiple jurisdictions, where divergent regulatory standards create obstacles for mutual investigations and evidence admissibility. The automated execution of smart contracts sparks disputes over legal liability attribution, while losses stemming from contractual code defects lack clear rules for determining responsibility. Legislative bodies must expedite the development of specialized regulations to clarify the legal status of smart contracts and delineate the rights and responsibilities of all parties involved. Regulatory technology tools require effective integration with legal procedures, and judicial standards for admitting

blockchain-based evidence need unified standardization. International regulatory cooperation organizations are advancing cross-border data exchange mechanisms to enable joint oversight while respecting national data sovereignty requirements. Judicial authorities should equip themselves with specialized technical personnel to enhance investigative and evidence-gathering capabilities for blockchain-related crimes. Industry self-regulatory bodies can establish ethical guidelines for technology application to guide market entities in the standardized use of blockchain technology.

6.3 Challenges and Countermeasures at the Market Promotion Level

Enterprises currently face high initial investment costs during blockchain system transformation, with significant R&D resources required to integrate data between existing business platforms and new blockchain systems. Ordinary users encounter cognitive barriers in understanding blockchain technology's operational principles, while complex operational workflows reduce user adoption willingness. Differences in blockchain standards adopted by various financial institutions necessitate overcoming technical compatibility issues for data interoperability between systems. Industry consortiums can drive the establishment of universal technical frameworks, reducing development costs and time consumption for system integration. Service providers should design simplified user interfaces, encapsulating technical complexity within backend operational workflows. Professional training institutions need to offer technical application courses for corporate employees to enhance practitioners' operational capabilities with blockchain systems. Government departments may consider providing policy support such as tax incentives to alleviate the financial burden of adopting new technologies for small and medium-sized enterprises. Industry associations can organize best practice case-sharing events to promote mature, replicable business models and application solutions.

7. Conclusions and Outlook

7.1 Summary of Research Findings

The deep application of artificial intelligence technology in the financial sector has given rise to new forms of cybercrime. Malicious actors now leverage algorithmic tools to analyze user transaction patterns, meticulously designing highly targeted fraud schemes. Blockchain's distributed ledger technology offers a novel approach to addressing these challenges. Its immutable nature ensures the authenticity and reliability of transaction records, enabling complete traceability of every fund flow. Smart contracts further enhance risk prevention capabilities by automatically executing anti-money laundering checks based on predefined conditions, significantly improving the efficiency of identifying suspicious transactions. Faced with massive data processing demands, the introduction of sharding technology effectively alleviates system operational pressure, ensuring the stability of blockchain networks when handling high-frequency transactions. The legal community is actively exploring standards for adjudicating smart contract disputes, establishing a reasonable institutional framework for new technology applications. Regulatory bodies worldwide are gradually overcoming enforcement barriers caused by jurisdictional differences through cross-border collaboration mechanisms. Enhanced user experience is equally noteworthy. Streamlined operational designs enable ordinary users to effortlessly navigate blockchain services, clearing obstacles for technological adoption [8]. These practical achievements form a complete closed-loop—from technical implementation and institutional safeguards to application promotion—laying a solid foundation for building a secure financial system in the digital age.

7.2 Research Gaps and Future Directions

This study identifies persistent lag in recognizing the dynamic characteristics of cyber financial crimes in the AI era. The continuous evolution of criminal methods makes it challenging for existing monitoring models to comprehensively cover emerging fraud patterns. Blockchain technology demonstrates significant effectiveness in tracking fund flows. However, the insufficient standardization of smart contracts limits their role in cross-platform risk prevention. Cross-border regulatory collaboration mechanisms lack unified data exchange standards, and judicial differences among nations continue to constrain the efficiency of joint law enforcement. Future research should focus on developing dynamically updated risk identification algorithms, establishing industry standards for smart contract security audits, and promoting the formation of an internationally accepted regulatory data-sharing framework. Financial institutions need to deepen cooperation with technology companies to more precisely translate practical business needs into technical solutions. The development of regulatory technology should emphasize alignment with existing legal frameworks, providing a moderately permissive regulatory environment for new digital financial activities. These exploratory directions will contribute to building a more resilient financial security defense system.

References

[1] Zhong H .The Integration of Artificial Intelligence and Blockchain: Applications and Challenges in Economic Security and Data Privacy[J]. ITM Web of Conferences, 2025, 73:03011.

[2] Vubangsi M , Nyuga G , Al-Turjman F .Exploring the Intersection of Artificial Intelligence and Blockchain Technology in Complex Systems: A Systematic Review[C]//International Conference On Artificial Intelligence Of Things For Smart Societies.Springer, Cham, 2024:25.

[3] Marcus S ,Milind T .The implications of national blockchain infrastructure for financial crime[J]. Journal of Financial Crime,2024,31(2):236-248.

[4] Chen J , Bao F , Li C ,et al.The Application and Ethics of Artificial Intelligence in Blockchain: A Bibliometric-Content Analysis[J]. Journal of Global Information Management, 2023, 31(7):6.

[5] Zhang N .A Review of Security Research on the Internet of Things, Based on Artificial Intelligence and Blockchain[J]. Frontiers in Computing and Intelligent Systems, 2022:7-9.

[6] Rachavelias G M .Online financial crimes and fraud committed with electronic means of payment—a general approach and case studies in Greece[J]. ERA Forum,2019,19(3):339-355.

[7] MİYNAT M ,DURAMAZ S .Karapara Aklama Aracı Olarak Yeni Bir Mali Suç: Siber-Aklama(New Financial Crime As A Black Money Laundering Tool: Cyber-Laundering)[J]. Yönetim ve Ekonomi,2013,20(1):315-325.

[8] C. G ,K. J .Rain Drop Service and Biometric Verification Based Blockchain Technology for Securing the Bank Transactions from Cyber Crimes Using Weighted Fair Blockchain (WFB) Algorithm[J]. Cybernetics and Systems, 2023, 54(4): 550-576.