PENINSULA PUBLISHING LLC

SHIFRA
Vol. (2026), 2026, pp. 1–61
ISSN: 3078-3186

Research Article

A Survey on Securing Smart Finance using Artificial Intelligence and Blockchain

Guma Ali [1,*], Otim Emmanuel[1], Maad M. Mijwil[2], Bosco Apparatus Buruga[3], Aida Vafae Eslahi [4], Ioannis Adamopoulos [5]

[1] *Department of Computer and Information Science, Faculty of Technoscience, Muni University, Arua, Uganda*

[2] *College of Administration and Economics, Al-Iraqia University, Baghdad, Iraq*

[3] *Department of Library and Information Services, Muni University, Arua, Uganda*

[4] *Medical Microbiology Research Center, Qazvin University of Medical Sciences, Qazvin, Iran*

[5] *Department of Public Health Policy, Sector of Occupational and Environmental Health, School of Public Health, University of West Attica, Athens, Greece*

ARTICLEINFO

Article History
Received 3 Oct 2025
Revised: 24 Nov 2025
Accepted 23 Dec 2025
Published 10 Jan 2026

Keywords
Smart finance,
artificial intelligence,
blockchain,
cybersecurity,
fraud detection,
secure transactions.

ABSTRACT

The rapid digitalization of financial services has given rise to smart finance ecosystems that integrate FinTech platforms, Internet of Things (IoT) devices, cloud infrastructures, and decentralized applications. While these systems enhance automation, operational efficiency, and financial inclusion, their highly distributed, data-intensive architectures introduce critical security, privacy, and trust challenges. In this context, artificial intelligence (AI) and blockchain have emerged as complementary technologies capable of addressing these challenges through intelligent decision-making, advanced threat detection, data integrity, and transparent operations. This survey provides a comprehensive review of recent research on securing smart finance systems using AI- and blockchain-based approaches. The survey comprehensively analyzed research published between 2023 and 2026 using the Scopus database, focusing on the keywords "AI," "blockchain," and "smart finance." The analysis reveals extensive use of AI-driven security mechanisms, including credit scoring and risk assessment, transaction monitoring and fraud detection, anti-money laundering (AML) and know-your-customer compliance, identity verification, cyber threat detection, smart contract security analysis, behavioral biometrics, insurance fraud detection, and market risk prediction. In parallel, the survey examines blockchain-enabled security solutions, including secure payment and settlement systems, cross-border remittances, AML and counter-terrorism financing frameworks, digital identity management, smart contracts, asset tokenization, decentralized finance, auditability, and secure interbank communication. The integration of AI and blockchain offers significant advantages, including improved fraud detection accuracy, enhanced transparency and traceability, stronger data integrity, automated compliance, real-time threat response, and increased system resilience. Despite these benefits, key challenges persist, particularly in scalability, privacy preservation, interoperability, regulatory and ethical compliance, energy efficiency, explainability, and post-quantum security. The survey concludes by outlining future research directions and design guidelines for developing secure, scalable, and trustworthy smart finance systems that effectively leverage the integration between AI and blockchain.

1. INTRODUCTION

The global financial sector is undergoing rapid transformation driven by digitalization and the integration of advanced technologies, including AI, blockchain, cloud computing, and big data analytics. These developments have enabled smart finance, a modern paradigm that improves efficiency, transparency, and inclusivity across digital banking, mobile payments, robo-advisory services, and decentralized finance (DeFi) ecosystems [1][2].

Digital payments are expanding globally due to real-time payment infrastructures, AI-enabled systems, widespread adoption of mobile and digital wallets, and financial inclusion initiatives. Global digital payment transaction values are

*Corresponding author email: a.guma@muni.ac.ug
DOI: https://doi.org/10.70470/SHIFRA/2026/001

projected to reach approximately US$12.55 trillion by 2027 [3]. The number of digital payment users is expected to grow to 3.81 billion by 2030, while the digital payments market is forecast to expand from US$4.97 trillion in 2025 to US$26.53 trillion by 2032, reflecting a compound annual growth rate (CAGR) of 13.63% [4]. Real-time payments are expected to account for 27.8% of global electronic transactions by 2027 [5]. Concurrently, cash usage continues to decline globally, reaching approximately 80% of its 2019 levels, with annual reductions of about 4% [4]. Digital banking adoption has surpassed 3.6 billion users worldwide by 2025, driven by increasing accessibility and usability of mobile platforms. As a result, the global digital banking market is projected to reach US$107.1 billion by 2030. Adoption patterns vary significantly across regions. The Far East and China lead with approximately 805.1 million active users, followed by the Middle East and Africa (387.3 million), Europe (361.7 million), North America (240.1 million), and Latin America (109 million) [5][6]. Together, these trends indicate a sustained global shift toward digital financial ecosystems and highlight the growing role of smart finance in economic growth and financial inclusion.

Smart finance enhances financial systems by embedding advanced digital technologies that improve efficiency and reduce transaction and financing costs. Automation of data collection, credit assessment, compliance verification, and contract execution is particularly impactful in supply-chain finance, agriculture, and green finance [7][8]. Blockchain-based transparency further enables traceable, immutable, and auditable records, reducing information asymmetry, strengthening trust, and mitigating fraud and greenwashing risks in sustainable finance [9][10]. AI-driven analytics and real-time monitoring strengthen risk management, fraud detection, and proactive compliance by continuously analyzing heterogeneous data sources [11][12]. In addition, smart contracts, IoT-enabled systems, and digital payment infrastructures reduce administrative overhead, accelerate cross-border transactions, and support faster, more inclusive financial services [13]. Through digital platforms and personalized AI-driven services, smart finance expands financial inclusion, enhances customer experience, supports sustainable development, and enables innovative financing models for smart and green city infrastructure [14].

Despite these advantages, increasing digital interconnectedness has significantly expanded the attack surface of financial systems. Smart finance platforms face diverse cybersecurity threats, including data privacy breaches, insider threats, phishing and social engineering attacks, advanced persistent threats (APTs), identity theft, malware and ransomware, distributed denial-of-service (DDoS) attacks, credential stuffing, brute-force attacks, man-in-the-middle (MitM) attacks, zero-day exploits, biometric spoofing, and data poisoning attacks targeting AI models [15-19]. These threats increase operational and regulatory compliance costs, undermine financial stability, disrupt operations, and cause direct financial losses. More critically, they erode user trust and slow the adoption of smart finance solutions [20-22].

Most smart finance systems, including digital banking platforms, DeFi applications, and digital wallets, continue to rely on traditional security mechanisms. These include perimeter-based controls such as firewalls and conventional intrusion detection systems; cryptographic techniques such as Secure Sockets Layer (SSL) and Transport Layer Security (TLS), end-to-end and database encryption, and tokenization; rule- or signature-based fraud detection; password-, Personal Identification Number (PIN)–based and Short Message Service (SMS)–based authentication; and centralized system architectures [23-26]. However, these approaches adapt poorly to evolving threats, provide limited protection against insider and social engineering attacks, and offer insufficient real-time threat visibility. Centralized architectures introduce systemic vulnerabilities, while conventional authentication and detection methods remain susceptible to credential-based attacks. Furthermore, complex key management, limited safeguards for AI-driven components, and high operational and compliance costs constrain their effectiveness.

To address these limitations, the integration of AI and blockchain has emerged as a foundational approach to secure, smart finance. AI supports credit scoring, risk analysis, automated trading, market surveillance, transaction monitoring, fraud detection, and compliance with AML and know-your-customer (KYC) requirements. It also enhances identity verification, cyber-threat detection, network security, and customer interactions through AI-powered chatbots, while supporting insurance fraud detection, portfolio risk prediction, smart contract analysis, behavioral biometrics, and document forensics [11]. Machine learning, deep learning, natural language processing, reinforcement learning, and federated learning enable proactive identification and mitigation of cyber threats and financial fraud [11]. Blockchain complements these capabilities through decentralization, immutability, transparency, and cryptographic security, enabling secure payments, cross-border transfers, fraud prevention, AML/CTF compliance, digital identity management, smart contracts, asset tokenization, supply-chain finance, auditability, and regulatory reporting across DeFi and interbank networks [27].

The combined use of AI and blockchain enhances fraud detection, ensures data integrity, strengthens identity and access control, automates compliance, and enables real-time threat response. This integration supports secure inter-institutional data sharing, improves system resilience, streamlines financial operations, and underpins emerging financial models such as decentralized finance, tokenization, and digital assets [27][28].

This review is motivated by the growing complexity of digital and decentralized financial systems, which amplifies cybersecurity risks. Financial institutions process large volumes of sensitive data across distributed infrastructures that involve APIs, smart contracts, and cross-chain interactions, significantly increasing the potential attack surface [29][30]. The limitations of traditional static security mechanisms exacerbate these risks. Consequently, this review examines how

the synergistic integration of AI and blockchain can strengthen the security, resilience, and trustworthiness of smart finance systems.

This survey aims to:

- Provide a comprehensive overview of smart finance by covering its fundamental concepts, evolution, features, operation, system architecture, and applications.
- Examines the primary cybersecurity threats, attacks, and challenges facing smart finance systems.
- Reviews AI techniques employed to enhance the security of smart finance.
- Analyzes the role of blockchain technology in safeguarding these systems.
- Explores the integration of AI and blockchain for securing smart finance.
- Identifies existing challenges and limitations and outlines future research directions for implementing AI and blockchain in smart finance security.

The survey is structured as follows: Section 2 outlines the materials and methods adopted for the study. Section 3 provides an overview of smart finance, including the enabling technologies and key benefits. Section 4 examines cybersecurity threats, attacks, and challenges affecting smart finance systems. Section 5 examines AI and its role in securing smart finance, and its benefits, while Section 6 focuses on blockchain technologies, their security applications, and advantages. Section 7 discusses the integration of AI and blockchain, highlighting hybrid architectures, their security benefits, case studies, and real-world implementations, and comparative analysis of existing solutions. Section 8 critically analyzes the limitations and challenges of integrating AI and blockchain for smart finance security. Section 9 outlines future research directions, and finally, Section 10 concludes the survey by summarizing key findings and contributions.

2. MATERIALS AND METHODS

This study employs a structured and comprehensive survey methodology to review and synthesize existing research on securing smart finance ecosystems through the integration of AI and blockchain technologies. The methodology adheres to established systematic literature review guidelines to ensure transparency, reproducibility, and methodological rigor. The primary objective is to analyze, classify, and critically evaluate state-of-the-art AI- and blockchain-enabled approaches that enhance security, privacy, trust, and resilience in smart financial systems. Specifically, the survey seeks to (i) identify prevailing security challenges in smart finance ecosystems, (ii) examine how AI and blockchain technologies individually and jointly address these challenges, and (iii) highlight open research gaps and promising future research directions. By consolidating recent advances, the study aims to provide a structured understanding of how these technologies contribute to secure and trustworthy smart finance infrastructures.

A comprehensive literature search was conducted across multiple reputable digital libraries to ensure broad interdisciplinary coverage. The selected databases included Emerald Insight, PLoS ONE, Frontiers, ACM Digital Library, Wiley, Nature, Springer, ScienceDirect, MDPI, IEEE Xplore Digital Library, and Google Scholar, chosen for their extensive collections in computer science, financial technology, cybersecurity, and distributed systems. This multi-source strategy reduced database bias and improved coverage of both foundational and emerging research.

The search strategy used controlled keywords and Boolean operators to identify relevant studies. Representative search strings included: “smart finance” AND “security”; “artificial intelligence” AND “blockchain” AND “finance” OR “AI-based fraud detection” AND “blockchain” OR “financial cybersecurity” AND “distributed ledger” OR “machine learning” AND “blockchain security.” To further enhance recall, related terms and synonyms such as FinTech, digital finance, deep learning, and distributed ledger technology were also incorporated into the search process.

Explicit inclusion and exclusion criteria were defined to ensure relevance, consistency, and methodological rigor. Included studies explicitly addressed security-, privacy-, trust-, risk-management-, or fraud-prevention-related issues in smart finance, financial technology, or digital finance. Eligible publications focused on the application or evaluation of AI techniques, such as machine learning, deep learning, natural language processing, reinforcement learning, and federated learning and/or blockchain mechanisms, including smart contracts, distributed ledgers, and consensus protocols. In addition, eligible studies were required to be published in peer-reviewed journals, reputable conference proceedings, or authoritative academic outlets. They needed to clearly describe their technical approaches, system architectures, algorithms, or evaluation methodologies, and to examine at least one security-related aspect, such as data integrity, privacy preservation, authentication, access control, fraud detection, or regulatory compliance. The review covered diverse smart finance applications, including digital payments, supply-chain finance, green finance, DeFi, banking systems, and financial data management. Only full-text studies published in English between January 2023 and January 2026 were considered.

Studies were excluded if they focused solely on traditional finance, economics, or accounting without a substantive component in smart finance, AI, or blockchain security. Additional exclusions applied to works that discussed AI or blockchain in finance but did not address security, privacy, trust, or risk. Non-peer-reviewed materials, such as editorials, opinion pieces, blog posts, white papers, patents, tutorials, and technical reports, were also excluded, along with studies lacking clear model descriptions, architectural details, algorithmic explanations, or validation procedures. Further

exclusions included high-level discussions without sufficient analytical depth, duplicate or minimally extended versions of prior work, non-English publications, inaccessible full texts, and studies published before January 2023.

To ensure consistency across selected studies, the review adopted a standardized data extraction protocol. Extracted information included publication details, application domain, security objectives, AI techniques employed, blockchain characteristics, evaluation metrics, key findings, and reported limitations. Mendeley, a reference management tool, was used to support systematic tracking, deduplication, and categorization of the literature. The methodological quality of the included studies was assessed using adapted quality assessment checklists derived from established systematic literature review guidelines. Evaluation criteria covered clarity of objectives, methodological soundness, adequacy of evaluation, and relevance to smart finance security. Each study was rated on a predefined scale (e.g., low, medium, or high quality), and only studies meeting a minimum quality threshold were included in the final synthesis to enhance the reliability and robustness of the findings.

Throughout the review process, reasons for exclusion were documented at each stage, and the retained studies were organized in a consistent format to facilitate accurate data extraction. To further minimize selection bias and improve reliability, a test–retest approach was used, in which randomly selected papers were reassessed at different stages of the review.

A Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) flow diagram was used to illustrate the stages of identification, screening, eligibility, and inclusion. From an initial set of 3,900 retrieved publications, 2,915 were excluded during title screening. Of the remaining 985 studies, 693 were excluded after abstract review, leaving 292 full-text articles for in-depth analysis. These studies specifically examined the integration of AI and blockchain technologies for securing smart finance ecosystems. Figure 1 presents the PRISMA flow diagram summarizing this systematic selection process.

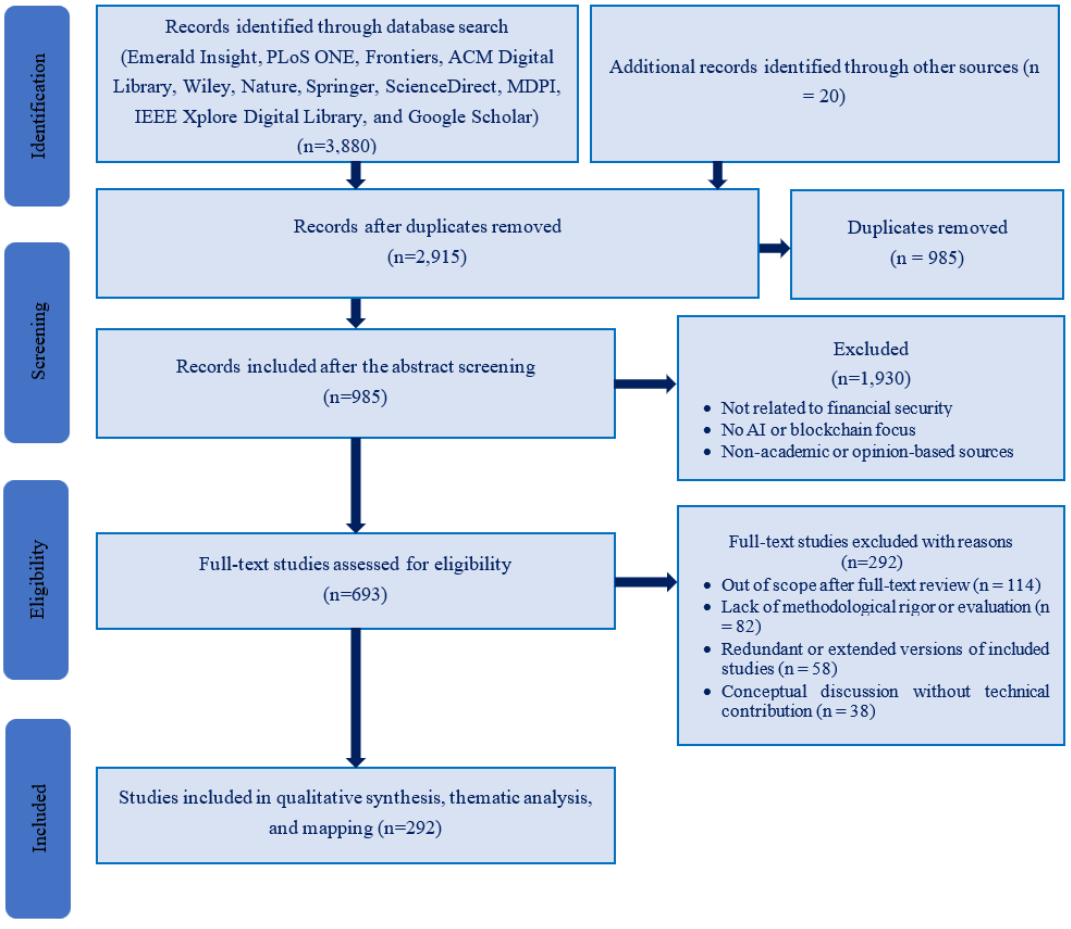

Fig. 1. The PRISMA flow diagram presents the systematic selection process.

Finally, 292 publications were systematically evaluated for their relevance to the study objectives. These were sourced from multiple scholarly databases, including 2 from Emerald Insight, 1 from PLoS ONE, 3 from Frontiers, 2 from ACM Digital Library, 1 from Wiley, 8 from Nature, 7 from Springer, 5 from ScienceDirect, 15 from MDPI, 37 from IEEE Xplore Digital Library, and 211 from Google Scholar. Each publication was categorized and critically assessed to ensure alignment with the study's aims. Figure 2 illustrates the distribution of the reviewed studies across the selected publication categories.

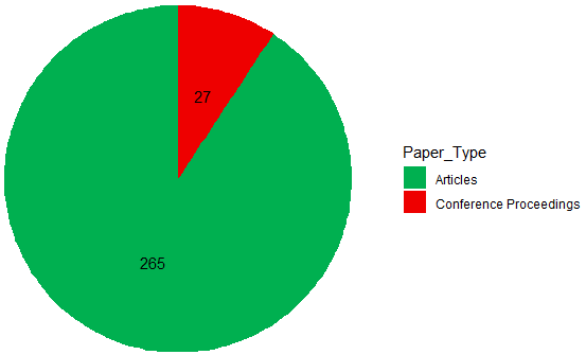

Fig. 2. Shows the categories of research papers selected for the study.

Figure 3 illustrates the digital databases consulted to retrieve the research papers included in this survey, providing a clear overview of the primary sources used to identify, screen, and select the relevant literature.

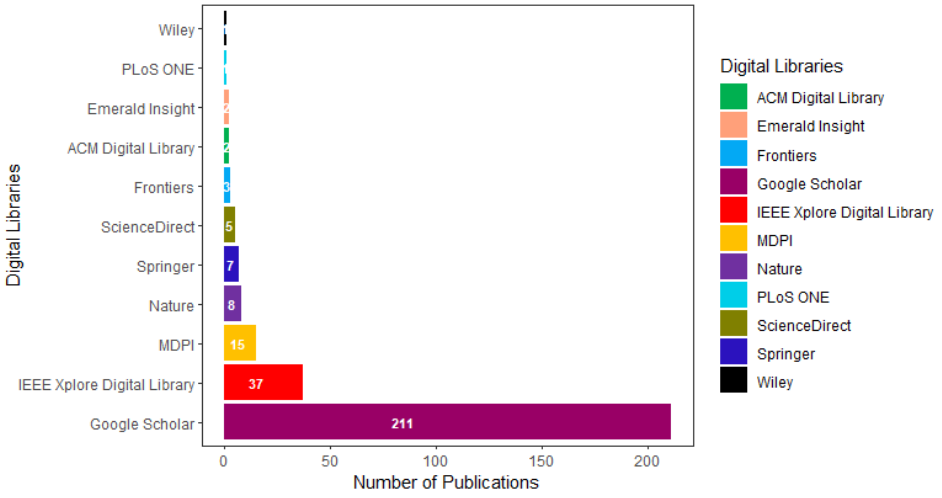

Fig. 3. Depicts the digital databases used to retrieve the selected research papers for the survey.

Figure 4 presents the distribution of research paper sources across major digital libraries, clearly illustrating how the selected studies are allocated among the different repositories.

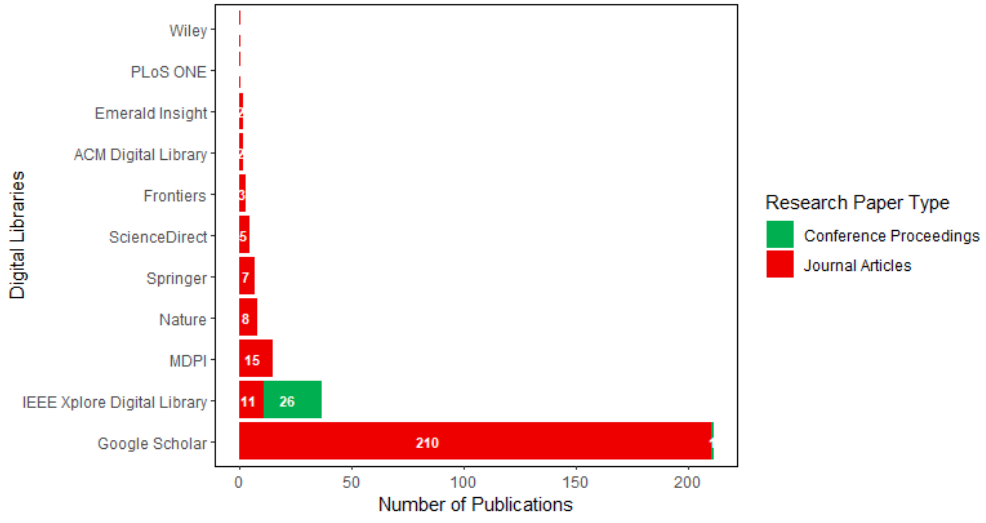

Fig. 4. Depicts the distribution of research paper sources based on digital libraries.

Figure 5 presents the distribution of the selected papers across digital libraries, organized by year of publication.

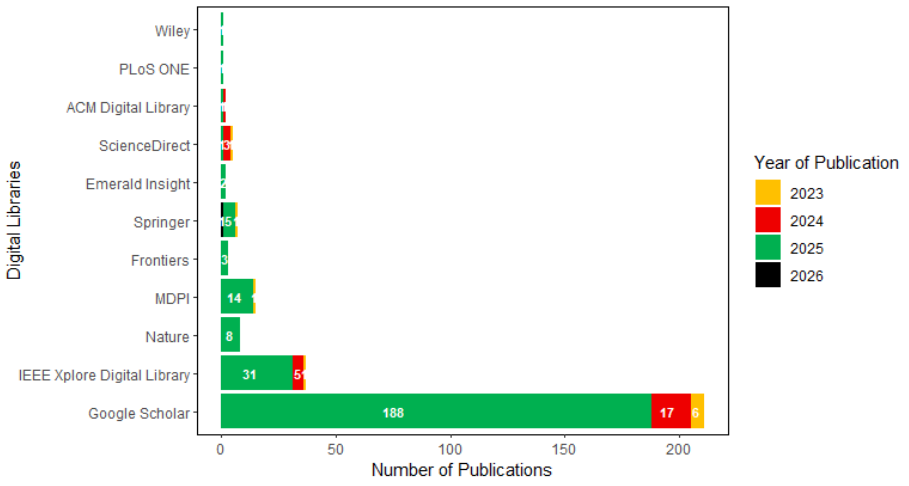

Fig. 5. Depicts the distribution of selected papers by digital libraries based on the year of publication.

A standardized data-charting form was developed and piloted to ensure the systematic extraction of relevant information from each included study. The extracted variables comprised bibliographic details (authors, publication year, and venue), study type (empirical, simulation, conceptual, review, or policy/standards), and domain focus (AI, blockchain, or smart finance). Additional fields captured blockchain architecture (e.g., private, public, or consortium) and the AI techniques employed, such as machine learning, deep learning, computer vision, and natural language processing. The charting process also recorded reported smart finance benefits, key findings and contributions, stated limitations, future research directions, and each study's relevance to smart finance cybersecurity. Four reviewers independently extracted data, after which the results were cross-verified to enhance accuracy and consistency across the dataset.

Following data extraction, a qualitative synthesis approach was applied to summarize and interpret findings across the selected studies. The literature was analyzed comparatively to identify recurring methodologies, strengths, limitations, and emerging trends in AI- and blockchain-enabled financial security solutions. To support a structured synthesis, the reviewed studies were organized into thematic categories. This thematic mapping enabled the identification of dominant research areas and underexplored topics in smart finance cybersecurity. This review relied exclusively on previously published literature and did not involve human participants, personal data, or proprietary datasets. Consequently, formal ethical approval was not required. All sources were appropriately cited to acknowledge original contributions and to uphold academic integrity.

Despite the rigorous methodology, this survey has several limitations. Limiting the review to English-language publications may have excluded relevant studies published in other languages. Moreover, the rapid evolution of AI and blockchain technologies may reduce the long-term applicability of some findings. Finally, although methodological consistency was emphasized, qualitative synthesis inherently involves interpretive judgment, which may introduce some subjectivity.

3. BACKGROUND AND CONTEXT

3.1. Fundamentals of Smart Finance

Smart finance is an emerging paradigm in which financial decision-making is increasingly delegated to data-driven, automated, and AI-enabled systems across banking, capital markets, and decentralized finance. Afifah et al. [31] and Hou and Feng [32] describe smart finance as a technology-driven financial model that integrates intelligent algorithms, decentralized infrastructures, and data-centric architectures to deliver adaptive, secure, and efficient financial services. At a functional level, smart finance embeds digital intelligence into financial processes to support predictive analysis, automated execution, and continuous operational optimization. By combining advanced digital technologies with traditional financial systems, it enhances efficiency, strengthens security, and improves the quality and speed of financial decision-making.

Core to smart finance is the use of AI, including machine learning, deep learning, natural language processing, reinforcement learning, and federated learning, alongside blockchain and distributed ledger technologies. These capabilities are complemented by cloud computing, big data analytics, the IoT, edge computing, 5G connectivity, robotic process automation (RPA), RegTech solutions, secure payment platforms and digital wallets, and advanced cybersecurity technologies. Emerging paradigms such as quantum computing, augmented reality, and virtual reality further expand the technological foundation of smart finance [9][11][33]. Together, these technologies improve risk management, operational performance, and service delivery across banking, investment, and payment ecosystems.

Advanced analytics and AI enhance fraud detection, credit scoring, robo-advisory services, and market forecasting, while blockchain enables secure, transparent, and immutable transaction records for cross-border payments, asset tokenization, and interbank settlements. Big data platforms transform large volumes of structured and unstructured data into actionable insights that support real-time decision-making, risk assessment, and customer personalization. In parallel, IoT technologies supply real-time data for usage-based insurance, asset tracking, localized fraud detection, and low-latency transaction monitoring. RPA further automates routine operations, compliance checks, and regulatory reporting, leading to substantial reductions in operational and compliance costs. Digital payment technologies play a central role by enabling instant, contactless, and cross-border transactions. At the same time, advanced cybersecurity solutions protect financial systems through biometric authentication, AI-driven threat detection, and secure transaction processing, reinforcing trust and system resilience. Looking ahead, quantum computing, augmented reality, and virtual reality are expected to drive the next phase of smart finance innovation. These technologies are anticipated to advance portfolio optimization, risk analysis, and cryptography-resistant security, while also enabling immersive customer engagement, financial education, and enhanced data visualization [34-38]. Figure 6 illustrates smart finance.

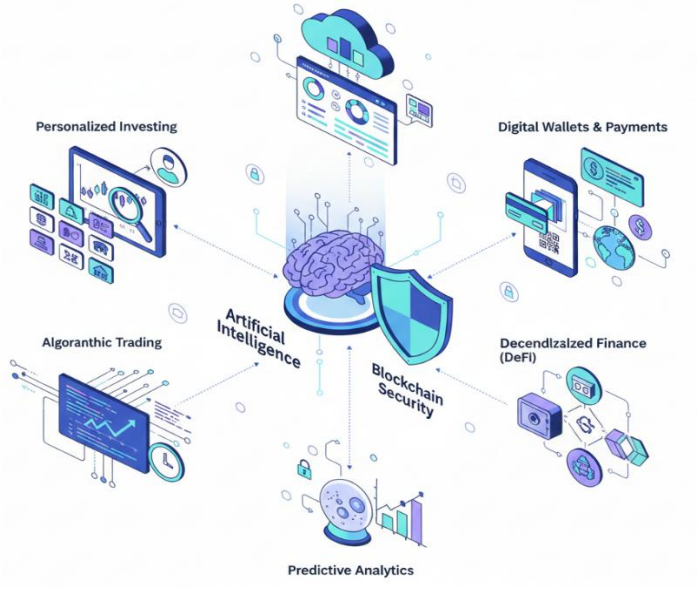

Fig. 6. Illustrates smart finance.

3.2. Evolution of Smart Finance

The evolution of smart finance can be viewed as a sequence of distinct yet interconnected stages shaped by technological innovation and corresponding changes in financial service delivery and governance. Over time, financial systems have gradually transitioned from manual, transaction-centered operations to intelligent, data-driven, and increasingly autonomous ecosystems. This progression reflects not only technological advancement but also structural shifts in how financial activities are organized, regulated, and accessed.

3.2.1. Traditional finance (pre-digital era)

In the pre-digital era, financial systems relied almost entirely on manual operations and paper-based processes. Banking activities took place primarily in physical branches, using ledgers, cash, and face-to-face interactions, with minimal automation. Risk management and investment decisions depended largely on historical records, professional judgment, and intuition rather than analytical or predictive models. As a result, transactions, clearing, and accounting processes were labor-intensive, slow, and highly error-prone. These inefficiencies led to high operational costs and limited accessibility, particularly for small or geographically remote clients [39][40]. Financial services were dominated by heavily regulated intermediaries, such as banks and insurers, operating within vertically integrated infrastructures and legal monopolies. Manual accounting systems and rigid document flows constrained transparency, scalability, and institutional responsiveness [40].

3.2.2. Digital finance (1980s–2000s)

The emergence of digital finance from the 1980s through the early 2000s marked the first major technological transformation of the financial sector. The adoption of computers, telecommunications, and the Internet enabled automated accounting, electronic fund transfers, ATMs, and web-based banking platforms. Stock exchanges transitioned to electronic trading systems, improving transaction speed and market transparency. During this period, credit cards, debit cards, and early online payment platforms became widespread, significantly reducing informational and transactional costs. However,

this transformation was driven mainly by incumbent financial institutions that used information and communication technologies to improve efficiency and global reach rather than to fundamentally disrupt existing business models [41][42]. Although data storage and basic analytics supported customer profiling and risk assessment, decision-making remained largely reactive and under human control. Nonetheless, digital finance laid the technological foundation for later FinTech innovations and expanded access to financial services.

3.2.3. FinTech and automated finance (2008–2015)

Following the global financial crisis, the period between 2008 and 2015 witnessed the rapid rise of FinTech and increased automation in financial services. FinTech start-ups and technology-driven firms leveraged mobile technologies, platform economics, algorithms, and data analytics to challenge traditional financial intermediaries. Innovations such as peer-to-peer lending, crowdfunding, robo-advisory services, and mobile payment applications reduced entry barriers and broadened financial inclusion. At the same time, algorithmic and high-frequency trading systems enabled high-speed, high-volume transactions executed according to predefined strategies. These developments lowered transaction costs, automated credit scoring and underwriting, and improved risk management and customer interactions by reducing information asymmetries [43]. This period also saw the emergence of Regulatory Technology (RegTech) and Supervisory Technology (SupTech), reflecting growing regulatory concerns related to financial stability, consumer protection, and supervisory capacity in increasingly automated markets.

3.2.4. Smart finance with AI and big data (2015–2022)

From approximately 2015 to 2022, advances in AI, machine learning, cloud computing, and big data analytics ushered in the era of smart finance. Financial systems moved beyond simple channel digitization toward data-driven, intelligent, and highly personalized services [39][44]. Machine learning models enabled predictive insights into credit risk, market dynamics, and customer behavior, while real-time fraud and anomaly detection systems strengthened financial security. AI-powered chatbots, recommendation engines, and robo-advisors further enhanced service personalization and operational efficiency [44-46]. In parallel, big-data-driven digital inclusive finance platforms, such as Alipay and WeChat Pay, significantly expanded service coverage and depth, particularly in underserved regions. However, these platforms also introduced new default, fraud, policy, and operational risks [41][47]. Meanwhile, blockchain and decentralized finance technologies enabled smart contracts, decentralized payments, and new digital asset markets, increasingly challenging traditional financial intermediaries and governance structures [39][44].

3.2.5. Next-generation smart finance (2023–present)

Since 2023, next-generation smart finance has emphasized real-time intelligence, system autonomy, and ecosystem-level integration. AI-driven systems now support continuous risk monitoring and adaptive strategy adjustment, while decentralized finance platforms rely on smart contracts to deliver trustless and automated financial services. Embedded finance further integrates payments, lending, and insurance into non-financial platforms, creating seamless, context-aware user experiences. Recent research envisions smart finance ecosystems that combine AI, machine learning, blockchain, IoT, 5G/6G, digital twins, augmented reality, virtual reality, quantum computing, and metaverse technologies to enable hyper-personalized, real-time, and largely autonomous financial services [39][44][46]. These developments align with a broader shift toward technology-oriented financing characterized by greater precision, agility, and security [46]. At the same time, ongoing research highlights persistent challenges related to cybersecurity, data privacy, systemic risk, and financial inclusion, as well as the need for adaptive regulatory and supervisory frameworks, including central bank digital currencies and sustainable or green FinTech architectures [39][44][45][47]. Figure 7 illustrates the phases of smart finance evolution.

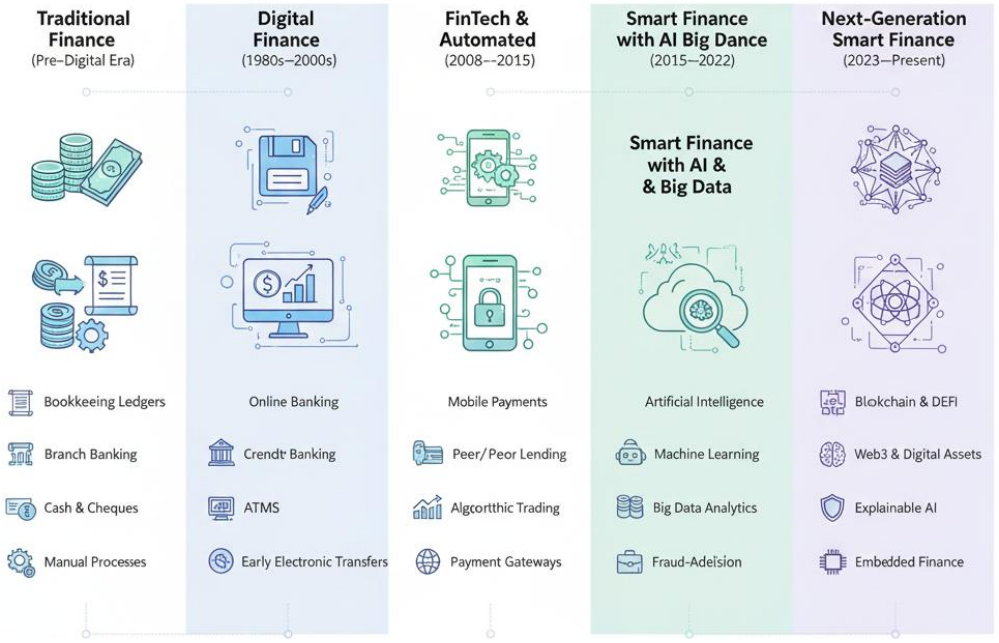

Fig. 7. Illustrates the phases of smart finance evolution.

3.3. Features of Smart Finance

Smart finance integrates automation, AI, and data-driven analytics to streamline core financial tasks, including budgeting, expense tracking, invoicing, reporting, and payments. By reducing manual intervention, these systems minimize human error while improving efficiency and consistency across financial operations. AI-driven algorithms automatically categorize transactions, forecast cash flows, and generate real-time insights through dashboards and intelligent models. This continuous visibility into revenues, expenditures, liquidity, and investment performance supports informed decision-making, early anomaly detection, and proactive risk management. Building on these capabilities, machine learning techniques analyze user behavior, spending patterns, and financial goals to deliver personalized recommendations. These include tailored investment strategies, savings plans, debt management guidance, and credit optimization, while predictive analytics enhance strategic planning by estimating cash flows, investment returns, and credit risks using historical and market data. Security remains a foundational component of smart finance platforms. Advanced encryption, multi-factor authentication, and AI-based fraud detection systems continuously monitor transactions, safeguard sensitive data, and support regulatory compliance. To further strengthen trust and transparency, many smart finance solutions incorporate blockchain technology. Immutable records, smart contracts, and secure peer-to-peer transactions enhance traceability, enable decentralization, and reduce reliance on intermediaries. In parallel, integrated digital wallets and payment services support instant and cross-border transfers, contactless payments, loyalty programs, micro-investments, and unified expense management. These features enable seamless and flexible financial interactions across diverse use cases. AI-driven robo-advisors also expand access to cost-effective investment management by optimizing portfolio allocation based on individual risk tolerance and prevailing market conditions. At the same time, automated compliance and reporting tools simplify adherence to tax, anti-money laundering, and audit requirements through real-time monitoring and traceable records. Finally, interoperability with broader FinTech ecosystems, including banking APIs, accounting systems, and e-commerce platforms, enables seamless data exchange and unified financial workflows. This integration reinforces an efficient, transparent, and fully connected smart finance environment [48-52].

3.4. Operation of Smart Finance

Smart finance relies on interconnected digital components that collect, process, and analyze financial data in real time to enable automated, data-driven decision-making. The workflow begins with comprehensive data acquisition from internal sources such as bank accounts, transaction histories, payroll, and expense systems; external sources including market data, credit scores, investment indices, and regulatory updates; and, in advanced use cases, IoT and sensor data applied to areas such as insurance and credit risk assessment. The system then preprocesses the raw data by cleaning to remove errors and duplicates, normalizing to standardize formats such as currencies and timestamps, and extracting features to derive meaningful indicators, including cash flow patterns, spending behavior, and credit utilization. AI-driven analytics subsequently analyze the refined data using descriptive methods to summarize historical performance, predictive models to forecast trends and risks, and prescriptive techniques to recommend optimal actions for investments, budgeting, or risk mitigation. Guided by these insights, smart finance systems support automated decision-making via rule-based or adaptive

transaction execution, alert and recommendation generation, and dynamic policy adjustments, such as modifying credit limits or portfolio strategies. Risk management and regulatory compliance are integrated throughout the process through real-time fraud detection, continuous assessment of credit and market risks, and automated adherence to reporting and legal requirements. The system communicates outcomes through intuitive reporting and visualization tools, including customized dashboards, scenario simulations, and transparent visual insights that facilitate informed decisions by diverse stakeholders. Finally, continuous learning mechanisms enable ongoing system improvement by updating machine learning models with new data, monitoring performance, and optimizing processes to enhance accuracy, efficiency, and overall financial outcomes. Figure 8 illustrates the steps involved in smart finance.

Fig. 8. Illustrates the processes involved in smart finance.

3.5. System Architecture for Smart Finance

Smart finance systems are designed to process large-scale financial data, automate complex workflows, ensure security and regulatory compliance, and provide intelligent decision support. Their architectures are typically modular, scalable, and data-driven, enabling seamless integration of financial services such as payments, lending, investment management, risk analysis, and fraud detection. To achieve these capabilities, smart finance systems are commonly structured into layered architectures, each addressing a specific functional concern.

3.5.1. Data layer

The data layer forms the foundation of the smart finance system by collecting, storing, and managing heterogeneous financial data from multiple sources. These sources include transaction systems, customer profiles, market feeds, IoT devices, and external regulatory databases. The layer supports both structured and unstructured data while enforcing data integrity, availability, and consistency through strong governance mechanisms. To accommodate high data volume and velocity, the data layer typically relies on distributed databases, data lakes, and lakehouse architectures that enable efficient downstream access. Extract–Transform–Load (ETL) pipelines and streaming technologies such as Kafka support both batch and real-time data ingestion and normalization [53]. In smart green supply chain finance and Environmental, Social, and Governance (ESG) analytics, this layer integrates multi-source ESG and operational data with blockchain technologies to ensure traceability and immutability [54]. It also manages schemas, data quality, and sustainability and regulatory metadata, including data sovereignty, retention, and lineage [53].

3.5.2. Integration and middleware layer

Building on the data foundation, the integration and middleware layer enables interoperability among internal components and external services. It provides standardized interfaces, APIs, and message brokers that abstract system heterogeneity, support loose coupling, and enhance architectural flexibility. This layer manages data transformation, routing, and protocol translation across legacy systems, microservices, cloud platforms, and third-party partners. In financial institutions, middleware underpins real-time transaction processing, trade execution, and regulatory reporting by ensuring reliable messaging, routing, and failover mechanisms that preserve transaction integrity [55][56]. It also supports high availability and disaster recovery and increasingly incorporates AI-enhanced monitoring and intelligent routing capabilities [55][56].

3.5.3. Analytics and intelligence layer

The analytics and intelligence layer transforms raw financial data into actionable insights through advanced analytics, machine learning, and AI. It supports critical functions such as risk assessment, fraud detection, credit scoring, financial forecasting, ESG risk analysis, and personalized recommendations. By combining real-time and batch analytics, this layer enables both immediate operational decisions and longer-term strategic planning. Digital finance and DeFi architectures integrate AI-driven pipelines, including anomaly detection, optimization algorithms, and simulation engines, to deliver predictive and prescriptive decision support [57-59]. In AI-driven accounting systems, explainability, bias mitigation, and continuous model monitoring are essential components that ensure analytical outputs remain transparent, robust, and reliable [59].

3.5.4. Transaction layer

The transaction layer governs the execution, validation, and recording of financial operations while enforcing atomicity, consistency, isolation, and durability (ACID) properties. It supports payments, fund transfers, settlements, and smart contract execution, with low latency and high availability being critical for real-time financial operations. In DeFi and tokenization environments, this layer includes smart contracts, consensus mechanisms, and execution engines that manage minting, redemption, and on-chain settlement processes [57]. Smart payment frameworks further incorporate validation engines, tokenization logic, and blockchain-backed audit trails to securely sign, order, and commit transactions at high throughput [60].

3.5.5. Security and compliance layer

The security and compliance layer spans the entire architecture to protect systems against cyber threats and ensure adherence to financial regulations. It implements cryptographic controls, authentication and authorization mechanisms, encryption, and key management to preserve data confidentiality and integrity. In addition, this layer enforces compliance with data protection laws, AML policies, and KYC requirements through continuous monitoring, auditing, and risk assessment. In AI-driven finance systems, blockchain-based audit trails, privacy-by-design principles, and real-time compliance monitoring support regulatory frameworks such as the General Data Protection Regulation (GDPR) and sector-specific financial regulations [53][59]. Smart payment systems integrate Payment Card Industry Data Security Standard (PCI DSS), Revised Payment Services Directive (PSD2), and GDPR compliance modules, secure API gateways, multi-factor or biometric authentication, and behavioral risk engines for real-time threat detection [60]. Emerging architectures further combine blockchain, AI, and quantum-resilient cryptography to deliver tamper-evident logs, adaptive threat analytics, and post-quantum security foundations [61-63].

3.5.6. Application layer

The application layer delivers business logic and user-facing functionality by translating system capabilities into domain-specific financial services. It hosts digital banking platforms, investment and lending systems, payment interfaces, risk and treasury dashboards, and DeFi portals. By orchestrating inputs from the data, analytics, and transaction layers, applications deliver cohesive, user-centric workflows. Modular design enables rapid feature development, scalability, and customization for diverse user groups. In green supply chain finance, this layer provides tailored tools that will allow suppliers, buyers, and financiers to make financing decisions and access ESG insights [54]. In digital finance transformation and smart payment systems, applications integrate accounting, reporting, fraud management, and customer service workflows augmented by embedded AI recommendations [59][60].

3.5.7. Infrastructure layer

The infrastructure layer provides the computational, networking, and storage backbone of the smart finance system. It typically consists of hybrid or cloud-native environments that host data pipelines, AI workloads, middleware services, and transaction engines [53][59]. Virtualization, containerization, and orchestration technologies enable elastic scaling, automated management, and efficient resource utilization. Financial architectures often combine on-premises and cloud resources, including Spark clusters, Hadoop ecosystems, and machine learning platforms, to meet performance, security, and jurisdictional requirements [53]. High-availability clusters, disaster recovery configurations, and performance-optimized storage further ensure stringent uptime and latency guarantees for core transaction and analytics workloads [55][56].

3.5.8. Interaction and feedback layer

The interaction and feedback layer connects the system with stakeholders, such as customers, financial institutions, and regulators, through intuitive user interfaces, dashboards, and reporting tools. By enhancing transparency and usability, this layer helps build trust while exposing APIs for external integration. Beyond interaction, the layer captures user behavior, expert input, and operational feedback, which are fed back into the analytics layer to support continuous learning and adaptive decision-making. Financial and cybersecurity frameworks emphasize interactive dashboards, visual analytics, alerting mechanisms, and configuration tools that allow operators to inspect events and adjust policies in real time [60][63]. Human–AI collaboration platforms further incorporate expert validation loops and structured feedback channels to refine models and decision rules, thereby improving system robustness in dynamic, volatile financial environments [64]. Figure 9 illustrates the layers of the smart finance system architecture.

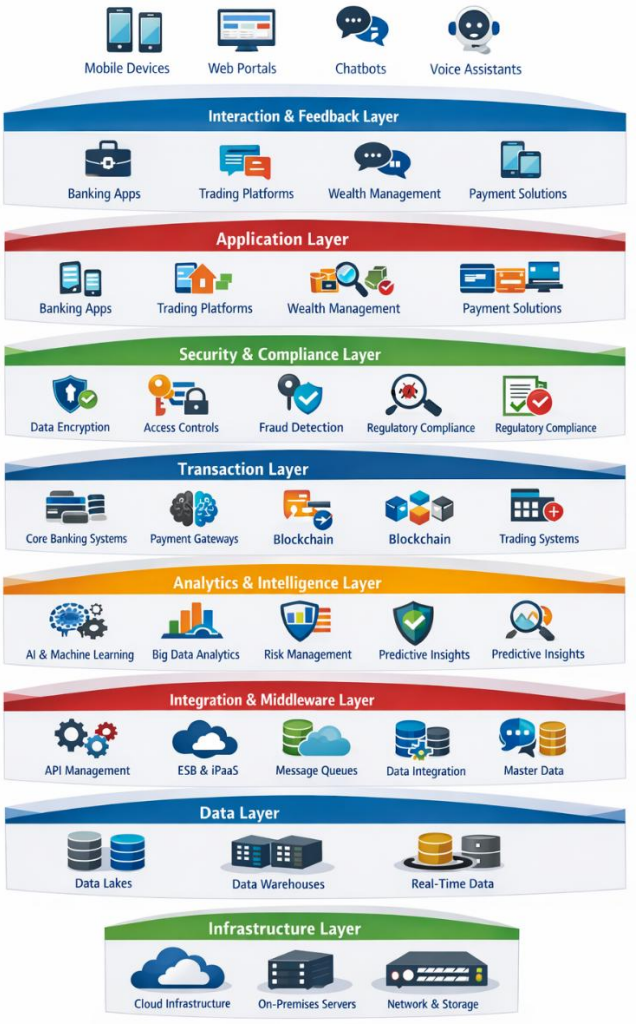

Fig. 9. Illustrates the layers of the smart finance system architecture.

3.6. Applications of Smart Finance

Smart finance is applied across multiple financial domains, including:

3.6.1. Personalized financial advisory

Smart finance leverages AI and machine learning to deliver tailored financial advice based on individual spending patterns, investment goals, and risk tolerance. Digital advisors, or robo-advisors, can recommend investment portfolios and dynamically adjust strategies without human intervention. Platforms such as Betterment and Wealthfront provide personalized retirement planning and automatically rebalance portfolios to optimize returns. AI-powered personal financial advisors (PFAs) analyze income, expenses, risk profiles, goals, and market data to generate real-time, customized plans for budgeting, saving, tax optimization, and investing [65-68]. Systems like Capit-AI and FinAID track expenses, visualize spending, recommend mutual funds or tax-saving products, and deliver alerts via chatbots and dashboards, lowering costs and improving access compared with traditional human advisors [69].

3.6.2. Automated investment management

AI-driven platforms monitor markets, execute trades, and manage portfolios automatically, reducing human error and enabling high-frequency, data-driven trading. AI-based trading systems analyze large datasets to identify optimal buy/sell opportunities in real time. Robo-advisors and AI portfolio optimizers construct and rebalance portfolios using quantitative algorithms informed by behavioral finance models [66][67][69]. These systems continuously adjust asset allocations based on market movements and user risk profiles, forecast returns using machine learning, and execute trades autonomously to maximize risk-adjusted performance while aligning investments with long-term objectives.

3.6.3. Risk assessment and fraud detection

Predictive analytics and pattern recognition enable smart finance systems to detect high-risk transactions and fraudulent activity, enhancing credit scoring and reducing financial losses. AI-powered banking systems can flag unusual transactions within seconds, preventing fraud. Machine learning and deep learning techniques improve anomaly detection beyond traditional statistical models, enabling near-real-time alerts and proactive risk mitigation [70-72]. Federated learning and privacy-preserving models allow institutions to collaborate on fraud detection without sharing raw customer data, maintaining confidentiality while improving accuracy [70].

3.6.4. Credit scoring and lending

AI enhances credit scoring by incorporating alternative data such as social behavior, mobile activity, and transaction history. FinTechs like Tala and Zest AI use machine learning to provide loans to individuals with limited credit history, expanding access for "unbanked" and thin-file borrowers [73][74]. AI-driven scoring improves default prediction, enables real-time credit decisions, and supports peer-to-peer and platform-based lending models, though it raises concerns regarding data privacy, bias, and transparency [73][74]. Blockchain-based credit recommenders can further automate loan terms and embed borrower history on-chain.

3.6.5. Blockchain-based payments and DeFi

Blockchain technology enables fast, transparent, and secure cross-border payments, reducing costs and reliance on intermediaries. Platforms like Ripple enable near-instant international payments with lower fees, while smart contracts provide tamper-resistant, decentralized ledgers [75][76]. These systems reduce settlement times from days to minutes and enhance auditability and fraud resistance. DeFi platforms extend these benefits by providing lending, borrowing, and trading services without the need for traditional intermediaries. Platforms such as Aave and Compound automate transactions and enforce rules transparently through smart contracts. AI-enhanced DeFi systems, including DeFiSentinel, integrate federated learning-based risk assessment and deep-learning fraud detection to strengthen security [31][70][72]. Smart contracts also automate collateral management, interest payments, and liquidations, though scalability, security, and regulatory challenges remain.

3.6.6. Insurance automation (InsurTech) and regulatory compliance (RegTech)

AI optimizes insurance operations by supporting data-driven underwriting, claims processing, and fraud detection. Platforms like Lemonade use AI chatbots to process claims instantly, reducing operational costs and improving customer experience. AI models segment risk, personalize premiums, flag suspicious claims, and smart contracts encode policy terms to trigger automatic payouts, enhancing efficiency and responsiveness [31][71][72][77]. Similarly, RegTech leverages AI and blockchain to automate regulatory reporting, monitor transactions, and maintain compliance. Machine learning enables near real-time detection of suspicious activity, automated reporting, and dynamic supervision, shifting compliance from manual audits to proactive, data-driven oversight [78-80], which reduces costs, improves accuracy, and enhances transparency, though risks such as cyberattacks and algorithmic bias remain.

3.6.7. Predictive analytics, digital wallets, and mobile banking

Predictive analytics enables smart finance platforms to forecast investment opportunities, optimize cash flow, and support strategic planning. By analyzing historical transactions, behavioral data, and macroeconomic indicators, AI systems classify users, predict income and spending, and simulate future scenarios, improving savings, risk management, and capital allocation [81-83]. AI wealth advisors provide real-time, explainable recommendations that enhance financial literacy and savings behavior [69]. Digital wallets and mobile banking platforms offer seamless, low-cost payments, savings, and investment options, often integrated with AI-based budgeting and fraud monitoring [84-86]. These tools promote financial inclusion, particularly in emerging markets, by lowering barriers to access and enhancing user control.

3.6.8. Peer-to-peer lending, crowdfunding, and wealth management optimization

P2P lending and crowdfunding platforms connect borrowers directly with investors, disintermediating traditional banks. AI-driven credit evaluation, risk rating, and soft information signals improve capital allocation, expanding access to credit while raising regulatory and consumer protection considerations. AI-enabled wealth management platforms, such as BlackRock's Aladdin, track portfolios, optimize taxes, and diversify investments in real time. These systems integrate robo-advisors, behavioral profiling, and machine learning models (e.g., clustering, XGBoost, random forests, Long Short-Term Memory) to construct personalized portfolios, automate rebalancing, and manage risk under dynamic market conditions [81][69]. By democratizing access to professional-grade advisory services, they enhance diversification and financial resilience for retail investors [69][87].

3.6.9. Real-time accounting, expense management, and sustainable finance

AI-powered accounting tools automate bookkeeping, invoicing, and reporting, improving accuracy and efficiency. Platforms like QuickBooks and Xero categorize transactions, detect anomalies, and provide dashboards for continuous

monitoring [83][86]. Integration with IoT and real-time transaction feeds allows faster financial close cycles, earlier risk detection, and up-to-date insights into financial health. Smart finance also supports sustainable and ethical investing by tracking ESG metrics and ensuring compliance with green or moral standards. AI and blockchain facilitate ESG reporting, environmental risk assessment, and monitoring of ethical conduct, while RegTech ensures regulatory compliance in areas such as cyber risk and financial crime [78][80]. These innovations emphasize emerging research priorities in green finance and FinTech sustainability.

3.6.10. Financial inclusion

Smart finance expands access for underserved populations through mobile banking, AI-based credit scoring, and microloans. Platforms like M-Pesa enable millions to send, receive, and save money via mobile phones, transforming financial access in regions such as Sub-Saharan Africa. Digital wallets, mobile banking, robo-advisors, and low-cost investment apps reduce barriers to saving and investing, turning previously passive users into active participants. Outcomes, however, depend on infrastructure, regulation, and financial literacy [84][85][87].

4. CYBERSECURITY THREATS, ATTACKS, AND CHALLENGES IN SMART FINANCE

Smart finance introduces numerous technological advancements; however, the emergence of these technologies also brings increasingly complex and multifaceted security vulnerabilities that must be carefully addressed to ensure system robustness and trustworthiness. Below are brief descriptions of the key cybersecurity threats, attacks, and challenges hindering the safe and sustainable adoption of smart finance.

4.1. Data privacy risks, data breaches, and information leakage

Smart finance systems handle vast volumes of personal, transactional, and behavioral data, making privacy protection both critical and complex. Unauthorized access, misuse, or leakage can severely undermine user trust and damage organizational reputation. Studies show that increased data sharing across digital platforms amplifies privacy-breach risks, particularly when regulatory safeguards are weak [88]. The deployment of AI-driven analytics, open banking APIs, cloud infrastructure, and mobile applications expands the attack surface, which exposes sensitive information, including account credentials, geolocation data, biometric identifiers, and behavioral patterns, to risks from over-collection, opaque processing, misconfigured cloud or API services, insider threats, and insecure mobile apps [18][89]. Documented breaches caused by cloud misconfigurations and vulnerable smart contract code demonstrate that failures in encryption, access control, and governance can lead to financial fraud, identity theft, regulatory penalties, and long-term erosion of trust in digital financial ecosystems [18][89].

4.2. Malware and ransomware attacks

Malware attacks involve malicious software, such as trojans, spyware, keyloggers, and ransomware, designed to infiltrate financial systems or customer devices. These attacks capture credentials, manipulate transactions, or establish backdoor access. Financial institutions are prime targets due to the direct monetary value of compromised systems and their dependence on continuous availability. Reports indicate a steady rise in banking trojans and mobile malware variants. Ransomware, which encrypts and often exfiltrates data to extort payment, disrupts core banking operations, ATMs, payment processing, and customer portals. Threats such as WannaCry and banking trojans like Emotet demonstrate how attackers steal credentials and initiate fraudulent transactions [90][91]. Recent trends reveal evolving ransomware ecosystems, including cloud-focused and double- or triple-extortion attacks, with sector-specific impacts on banks [18][90][92].

4.3. Distributed denial-of-service (DDoS) attacks

DDoS attacks overwhelm financial platforms with excessive traffic, rendering services unavailable and disrupting online banking, digital payments, trading platforms, and DeFi systems. These attacks cause operational downtime, financial losses, and reputational damage. The real-time dependence of smart finance systems increases vulnerability, and DDoS-for-hire services targeting financial institutions are on the rise globally. DDoS campaigns can distract IT teams while perpetrators engage in fraud, as seen in the Bangladesh Bank Heist (2016). Attacks on online brokerage platforms can freeze trading and disrupt markets. As financial services migrate online and to the cloud, volumetric and application-layer DDoS attacks against web portals, APIs, and crypto exchanges have become primary threats, often combined with extortion or used to mask fraud and data theft [18][90].

4.4. Credential stuffing and brute-force authentication attacks

Credential stuffing exploits reused usernames and passwords from prior breaches, using automated tools to gain unauthorized access. Weak or absent multi-factor authentication increases susceptibility [29]. Large-scale account compromises have occurred when attackers reused credentials from non-financial breaches, including the 2021 Robinhood incident. Brute-force attacks systematically attempt password or PIN combinations, targeting platforms lacking strong

password policies, rate limiting, or account lockout mechanisms, such as mobile banking apps and ATMs [93]. Weak authentication, password reuse, and human factors remain core vulnerabilities, resulting in unauthorized access, fraudulent transfers, and identity theft [18][89].

4.5. Man-in-the-Middle (MitM) attacks

MitM attacks intercept or alter communications between users and financial platforms to steal credentials, manipulate transactions, or inject malicious data. They often exploit unsecured public Wi-Fi, weak encryption, poor certificate validation, or inadequate session management, including SSL-stripping to downgrade HTTPS connections. The expansion of mobile, IoT, open-banking, cloud, and DeFi services increases exposure. Compromised APIs, gateways, proxies, or relays enable credential interception, message replay, or fraudulent transaction injection before data reaches back-end systems or smart contracts [18][90][94].

4.6. Identity theft

Identity theft involves unauthorized use of personal data to impersonate individuals for financial gain. Attackers exploit stolen information and social engineering to create fraudulent accounts, launder money, or access existing services. Smart finance systems aggregate rich customer data, including identity documents, payment credentials, transaction histories, biometric identifiers, and behavioral profiles. Breaches or misuse facilitate identity takeover, and compromised attributes are often difficult or impossible to revoke [18][89]. Non-compliance with privacy regulations further intensifies individual and organizational risks.

4.7. Biometric spoofing attacks

Biometric spoofing uses fake fingerprints, facial images, voice recordings, or AI-generated deepfakes to bypass authentication systems. As smart finance increasingly relies on biometrics, spoofing poses a growing threat [95][96]. Attackers may use high-resolution photos, 3D masks, fabricated fingerprints, or voice synthesis. Weak liveness detection allows spoofed traits to bypass security controls, and compromised biometric data is irreversible, creating persistent identity risks in digital finance ecosystems [16][18].

4.8. Advanced persistent threats (APTs)

APTs are highly sophisticated, targeted attacks where adversaries maintain long-term, stealthy access to financial systems. They exfiltrate sensitive data, manipulate transactions, or disrupt operations, often exploiting zero-day vulnerabilities and lateral network movements [97]. Campaigns such as Carbanak/FIN7 illustrate the impact of APTs, including the monitoring of employee activity and the manipulation of ATMs to steal over US$1 billion. Spear-phishing and compromised vendors are common vectors, highlighting threats that traditional perimeter defenses cannot prevent [18][98][99].

4.9. Insider threats

Employees, contractors, and partners with authorized access can pose significant risks through negligence, lack of awareness, or intentional misuse [93]. Insider threats include data theft, fraudulent transactions, privilege abuse, and system tampering. Weak access controls, insufficient monitoring, and inadequate segregation of duties enable long-running fraud, as demonstrated in cases in Bangladesh (2014) and Europe (2019). Combined human- and system-focused controls, including least-privilege access and anomaly-based behavior analytics, are essential to mitigate these risks [100-102].

4.10. DNS spoofing/hijacking

DNS spoofing or hijacking redirects users from legitimate financial websites to malicious ones, allowing attackers to steal credentials and private keys or to authorize fraudulent transactions. Attackers achieve this by poisoning DNS caches or hijacking domain registrar accounts [103][104]. Even security-conscious users can be deceived if spoofed domains and TLS certificates appear legitimate, making DNS-layer manipulation a critical vector for phishing and account-takeover attacks in online banking [17][98][105].

4.11. Router and network exploits

Compromised routers and network infrastructure enable attackers to intercept, modify, or inject malicious traffic into financial communications through ARP poisoning, default credentials, or firmware vulnerabilities. Vulnerable home or corporate routers serve as entry points for MitM attacks or lateral movement toward core banking systems [18][105][106]. Misconfigured routers, VPNs, and API gateways further expose cloud- and hybrid-networked financial services, while network-layer weaknesses are exploited in DDoS campaigns to disrupt services or conceal fraud [16][98][103][104][107].

4.12. Rogue Wi-Fi hotspots

Attackers set up unsecured or malicious Wi-Fi networks near financial institutions or public spaces to trick users into connecting. Unsuspecting customers risk MitM attacks that expose credentials, crypto keys, or transactional data.

Techniques include mimicking legitimate networks to intercept or modify unencrypted traffic, allowing malware injection or credential capture [98][103-105].

4.13. Social engineering and phishing attacks

Social engineering exploits human psychology, using phishing, vishing, and deepfake impersonation to deceive staff and customers [108]. Phishing remains highly prevalent, targeting credentials, one-time passwords, and financial information via email, SMS, phone, or fake websites. AI-generated phishing amplifies risk by creating personalized messages that bypass traditional defenses. Attackers target users' wallets and employees, often leading to data breaches, SWIFT fraud, and irreversible cryptocurrency losses [18][103][104]. Social engineering continues to dominate credential theft, APT intrusions, ransomware, and broader banking-related breaches [17][98][104].

4.14.Privilege escalation

Privilege escalation occurs when attackers gain unauthorized higher-level access, often moving from regular accounts to administrative roles by exploiting vulnerabilities, misconfigured roles, or weak access controls, which enables fraudulent transactions, exposure of confidential analytics, or loss of administrative control [16][105][106]. Attackers typically begin with low-level access via phishing, malware, or misconfigured systems. Weak internal access controls, poor role-based permissions, and unpatched systems facilitate both horizontal and vertical escalation, underpinning insider threats and APT campaigns [18][105][106].

4.15.Cryptojacking

Cryptojacking involves unauthorized use of computing resources to mine cryptocurrency, degrading performance and increasing operational costs [16]. Financial servers, cloud VMs, endpoints, and ATMs are common targets [18][98][106]. Attackers inject mining scripts into financial websites or infect endpoints. Because cryptojacking manifests as subtle resource anomalies, AI- and anomaly-based monitoring is recommended for detection and mitigation in financial cybersecurity frameworks [16][106].

4.16.AI algorithm manipulation

Smart finance increasingly relies on AI for credit scoring, fraud detection, and automated trading, but adversarial attacks can manipulate algorithms by feeding biased or crafted data [109]. Such manipulation can distort predictions, approve fraudulent loans, or trigger losses in automated trading. Adversarial inputs can deceive AI models used in fraud detection, intrusion detection, KYC, and trading, bypassing controls and increasing misclassification rates. For example, adversarial perturbations can raise the misclassification rate of Convolutional Neural Networks to 86.8% under C&W, illustrating vulnerabilities in AI-driven financial defenses [110-112].

4.17.Synthetic identity fraud

Synthetic identity fraud combines real and fabricated personal information to bypass verification systems, allowing account creation, credit access, or money laundering. In smart finance, synthetic identities exploit digital wallets, neo-banks, and DeFi platforms, often evading automated AI-based checks [113]. Attackers use stolen information with fabricated attributes, sometimes generated via Generative Adversarial Networks, to create plausible identities that circumvent KYC/AML controls. Generative AI and deepfake media further undermine authentication, contributing to substantial financial losses and reputational damage [22][114].

4.18.Data poisoning attacks on AI models

Data poisoning attacks involve injecting malicious or misleading data into AI training datasets to degrade model performance or induce erroneous outputs. In smart finance, these attacks can compromise fraud-detection models, distort credit risk assessments, and manipulate algorithmic trading systems for example, making fraudulent transactions appear "normal" or skewing stock market predictions [115]. Malicious samples subtly shift learned decision boundaries, allowing models to maintain accuracy on clean validation data while undermining intrusion- and fraud-detection pipelines [112][116]. Large-scale meta-analyses report that such attacks succeed in 42% of deployed AI systems, highlighting their significant threat to financial AI security [117].

4.19.Adversarial machine learning attacks

Adversarial attacks manipulate input data to deceive AI models into making incorrect predictions, posing significant risks to financial security systems. They can allow fraudulent transactions to evade detection or trigger false alerts [97]. These attacks exploit subtle, carefully crafted inputs to mislead AI in applications such as automated trading, loan approvals, and fraud detection. Examples include altering transaction patterns to bypass fraud detection, tricking credit scoring systems into approving high-risk loans, or modifying trading signals to induce erroneous trades. Evasion, poisoning, and inference attacks can also target AI-based cyber-defense tools, directly manipulating fraud-detection and risk-scoring algorithms to undermine trust and enable undetected transactions [63][101][111][113].

4.20. Zero-day exploits

Zero-day exploits target previously unknown software or hardware vulnerabilities for which no security patches exist. Financial institutions are particularly vulnerable, as attackers can compromise core banking applications, trading platforms, or cloud services before they are detected or remediated. For instance, unpatched flaws in mobile banking apps can enable credential theft, while vulnerabilities in blockchain smart contracts can allow attackers to drain digital assets. Signature-based controls are ineffective against such attacks, prompting the use of AI-driven anomaly detection and hyper-automation to predict and contain them [118]. Machine learning, deep learning, and federated learning-based intrusion detection systems are increasingly essential, as traditional Intrusion Detection Systems (IDS) cannot detect unknown zero-day exploits [119].

4.21. Account takeover attacks

Account takeover attacks occur when attackers gain unauthorized access to legitimate user accounts using stolen credentials, phishing, malware, or credential stuffing. These attacks enable fraudulent fund transfers, unauthorized loan applications, and identity misuse [120]. Phishing and credential stuffing exploit login information, while attackers in crypto exchanges transfer cryptocurrency to their own wallets. The rise of mobile banking and Generative-AI–enabled phishing (emails, SMS, vishing) has expanded the attack surface, increasing the success of social-engineering attacks [114]. Deepfakes synthetic voice or facial identities can bypass biometric and video-KYC controls, further enabling fraudulent logins and high-risk financial operations [22][114].

4.22. Vulnerabilities in cloud environments

Financial institutions increasingly rely on cloud computing for scalability, data storage, and AI processing. However, this reliance introduces significant security risks, including misconfigured servers, insecure APIs, insufficient access controls, and vulnerabilities in shared multi-tenant environments [121]. Misconfigured storage, such as open AWS S3 buckets, can expose sensitive financial data. Compromised cloud-hosted AI services may enable model manipulation or the theft of proprietary algorithms, and insider threats may allow provider personnel to access confidential information. The multi-tenant nature of cloud infrastructure also facilitates lateral movement from a compromised client instance, increasing exposure across organizations. Scarcity, fragmentation, and concept drift of financial data further complicate AI security in cloud-scale SOCs and payment platforms [101][118].

4.23. Blockchain security limitations

Despite offering transparency, immutability, and decentralization, blockchain remains vulnerable to various security threats. 51% attacks, in which an entity controls the majority of network hash power, can enable double-spending, as seen in Ethereum Classic (2019), resulting in US$1.1 million in losses. Smart contract bugs, such as those exploited in the 2016 Decentralized Autonomous Organization hack, can lead to fund drainage and fraud [22]. Other risks include private key theft, consensus manipulation in early Proof-of-Stake (PoS) systems, oracle tampering, flash loan attacks, governance flaws, and privacy leaks from public blockchain transparency. In 2022, 60% of DeFi incidents were linked to smart contract vulnerabilities that AI-based auditing could have detected pre-deployment [113]. Blockchain's immutability complicates reversing fraudulent transactions, while scalability and energy constraints challenge secure adoption in high-volume financial applications [22][122].

4.24. Smart contract exploits

Smart contracts automate financial transactions but remain vulnerable to coding errors, logic flaws, and design weaknesses, making rigorous auditing essential (Kumar & Mensah, 2024). Common vulnerabilities include reentrancy attacks, integer overflow/underflow, unchecked external calls, flash-loan exploits, and oracle manipulation, which have caused major losses in incidents like the Decentralized Autonomous Organization hack (2016), Parity multisig wallet freeze (2017), and bZx and Harvest Finance attacks (2020) [94][123][124]. DeFi platforms are particularly vulnerable due to complex contract interactions, where attackers exploit lending pools, price oracles, or temporary logic inconsistencies. Detection and mitigation rely on static and dynamic analysis, formal verification, multi-tool auditing, and secure development lifecycles. Yet automated repair tools address only 29–74% of exploits, leaving residual risk. Immutability prevents straightforward patching, often requiring migrations or "circuit breaker" mechanisms, highlighting the need for advanced expertise and rigorous security practices [94][125][126].

4.25. IoT vulnerabilities

Financial IoT devices, including smart ATMs, wearable payment devices, and connected Point-of-Sale systems, are exposed to weak authentication, unencrypted communications, outdated firmware, and poorly configured networks [127-129]. These vulnerabilities enable unauthorized access, data interception, and device hijacking. They also expand the attack surface for botnets, DDoS attacks, and MitM exploits, disrupting services and compromising user data, as seen in the Mirai botnet (2016, 2017). Heterogeneous protocols and constrained resources amplify these risks. Advanced deep-learning

intrusion detection methods, e.g., Convolutional Neural Network – Bidirectional Long Short-Term Memory – Gated Attention Mechanism (CNN–BiLSTM–GAM), achieve >96% accuracy in detecting malicious IoT traffic, yet scalability and adaptability remain key obstacles in operational financial environments [127][128].

4.26. Regulatory and compliance challenges

Rapid smart finance innovation often outpaces regulatory frameworks, creating complex legal and compliance risks, particularly in emerging or cross-border contexts. Regulatory gaps, unclear rules for blockchain products, and challenges with Coin Offerings (ICOs), combined with cross-border AML/KYC obligations, complicate compliance with GDPR, PCI DSS, and PSD2. Non-compliance can lead to fines, legal action, and reputational damage. Fragmented oversight across jurisdictions, cloud platforms, open-banking APIs, and DeFi amplifies audit gaps, data privacy breaches, and systemic risks. Institutions must align FinTech innovations with evolving data protection, cyber-resilience, and global security standards [101][102][130][131]. Cross-border accountability, consistent implementation of a framework, and addressing skills and cost constraints remain significant challenges, as weak governance magnifies regulatory penalties and operational vulnerabilities.

4.27. Third-party security weaknesses

External service providers cloud platforms, API partners, and FinTech vendors are integral to smart finance ecosystems. Weaknesses in these services, including poorly secured APIs, misconfigured cloud storage, and insufficient auditing, create supply chain vulnerabilities that affect all components of smart finance [19][101][102]. High-profile incidents like the SolarWinds attack (2020), the SWIFT Bangladesh breach, and the Capital One cloud compromise illustrate how attackers exploit trust relationships and interconnected systems. Robust third-party risk management, continuous vendor monitoring, and strict contractual security requirements are critical to safeguarding financial ecosystems.

4.28. Automated fraud bots

Automated bots exploit vulnerabilities in financial platforms to conduct large-scale attacks, including credential stuffing, transaction fraud, and payment manipulation. These bots often circumvent rate limits and overwhelm monitoring systems. In smart finance, AI-driven bots can rapidly initiate fraudulent transfers, send personalized phishing messages, and manipulate marketplaces. For example, the 2021 surge in credential stuffing resulted in millions of unauthorized withdrawals. Adversaries leverage high-frequency transaction environments, while defenders deploy machine learning on network telemetry and user behavior to detect algorithmic fraud and insider misuse at scale [101]. In metaverse-style financial ecosystems, bots like DeepFakeBot, FraudGPT, and MirageBot execute AI-enabled scams, deepfake impersonation, and automated smart-contract or payment fraud, adapting to defenses and emphasizing the need for behavioral analytics and real-time response automation [101][126].

4.29. Legacy system vulnerabilities

Many financial institutions still operate legacy systems, including core banking, credit, and payment platforms, which were not designed to withstand modern cyber threats. These systems are vulnerable to buffer overflows, unpatched software, and weak encryption [101][102][131]. Unsupported software and outdated protocols often serve as initial footholds for attackers, as demonstrated by the Equifax breach (Apache Struts) and the 2019 Capital One compromise. Legacy systems also struggle to integrate securely with modern digital platforms, cloud services, and DeFi interfaces, creating gaps, configuration errors, and shadow-IT surfaces. Limited encryption and audit capabilities further heighten data breach risks. Legacy debt remains a structural vulnerability, compromising both technical security and regulatory compliance across the financial sector.

As digital financial services expand, they generate vast and complex data streams that traditional security mechanisms struggle to monitor. AI-based security solutions are increasingly essential, analyzing transactional, behavioral, and network data to detect abnormal activities and potential breaches in real time while maintaining the integrity of digital financial ecosystems.

5. ARTIFICIAL INTELLIGENCE IN SECURING SMART FINANCE

5.1. Overview of Artificial Intelligence

Artificial intelligence is a branch of computer science that focuses on designing and developing systems capable of performing tasks that typically require human intelligence. These tasks include learning from data, logical reasoning, problem-solving, perception, pattern and image recognition, natural language understanding, and decision-making. AI systems use computational models, algorithms, and mathematical frameworks to process information, interact with their environment, and adapt their behavior based on experience, enabling autonomous or semi-autonomous operation [132][133]. By leveraging core techniques such as machine learning, deep learning, natural language processing, computer vision, and federated learning, AI can analyze large and complex datasets, including financial and security-related data, to identify patterns, predict future states, and detect anomalies without explicit task-specific programming. This data-driven

capability enables AI to transform raw data into actionable intelligence, automate large-scale, repetitive processing tasks, and support accurate, efficient, and informed decision-making. As a result, AI enhances reliability, productivity, security, and overall operational efficiency while reducing time and resource consumption [134][135].

In the context of smart finance, AI applies machine learning, deep learning, and other data-driven techniques to automate, personalize, and optimize financial decision-making across banking, capital markets, and FinTech services [31][136]. Advanced computational models and algorithms improve decision-making, risk management, customer engagement, and operational efficiency. Machine learning enables financial systems to process large volumes of structured and unstructured data, uncover patterns, and generate predictive insights for tasks such as credit scoring, fraud detection, and algorithmic trading. Deep learning, a subset of machine learning, employs multilayer neural networks to capture complex relationships in financial data, supporting applications such as sentiment analysis, anomaly detection, and real-time market prediction. Natural language processing allows AI systems to interpret and extract insights from textual and voice data derived from customer interactions, regulatory documents, and news feeds. This capability supports automated customer service, regulatory compliance, and risk monitoring. Reinforcement learning further enhances smart finance by optimizing sequential decision-making, such as portfolio management and dynamic pricing, through interaction with simulated or historical environments. Additional techniques, including ensemble learning, clustering, and graph analytics, enhance fraud prevention, AML detection, and network-based risk assessment by integrating multiple models and uncovering hidden transactional patterns. Collectively, these AI capabilities enable smart finance systems to achieve greater accuracy, efficiency, and adaptability, facilitating the transition from legacy financial infrastructures to modern, data-driven services. Figure 10 illustrates the role of artificial intelligence in smart finance.

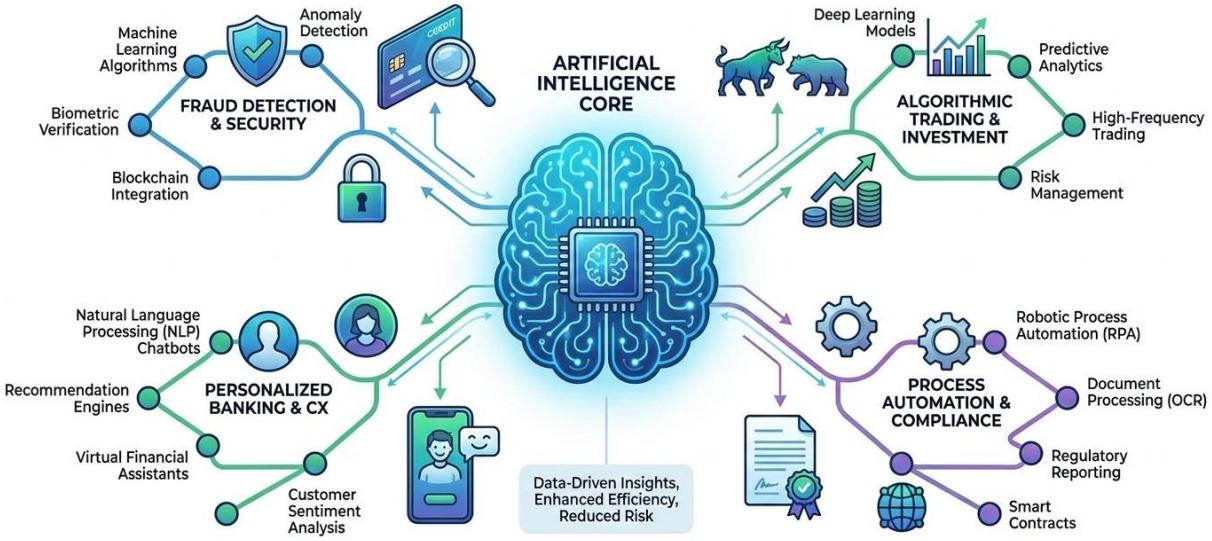

Fig. 10. Illustrates the role of artificial intelligence in smart finance.

5.2. Artificial intelligence techniques in Smart Finance

AI techniques are central to the development of smart finance, fundamentally transforming how financial systems analyze data, manage risk, and support decision-making. Key methods, including machine learning, deep learning, natural language processing, reinforcement learning, and federated learning, enable financial platforms to extract insights from large-scale data, adapt to dynamic market conditions, and enhance predictive and analytical capabilities. Collectively, these approaches form the technological backbone of smart finance, driving more intelligent, efficient, and data-driven financial services while maintaining the integrity of existing financial processes.

5.2.1. Machine learning

Machine learning develops statistical models and algorithms that enable computers to learn from data without being explicitly programmed. By leveraging data mining, computational statistics, and mathematical optimization, machine learning systems identify hidden patterns, generate predictions, and support decision-making. As these systems process increasing volumes of data, they continuously improve, becoming more accurate and capable of automating tasks traditionally performed by humans. Machine learning encompasses four fundamental paradigms supervised, unsupervised, semi-supervised, and reinforcement learning each offering distinct strategies for solving complex problems [137]. However, the effectiveness of machine learning depends heavily on the quality, diversity, and representativeness of training datasets, which can present challenges in real-world deployment.

In cybersecurity, machine learning is critical for detecting, preventing, and mitigating threats. Algorithms analyze large-scale datasets to uncover patterns and anomalies that indicate malicious activity. Supervised learning models identify known threats, while unsupervised approaches detect previously unseen anomalies. Techniques such as clustering and

classification enhance intrusion detection, network security, and traffic monitoring by identifying suspicious behavior. Consequently, machine learning strengthens cybersecurity across phishing detection, malware analysis, endpoint protection, and identity and access management, adapting to evolving attack strategies to improve digital asset safety [132-135].

Machine learning also enhances the resilience of critical infrastructure systems. By analyzing historical performance data, machine learning algorithms can detect early indicators of equipment failure, reducing service interruptions. Intrusion detection systems further benefit from machine learning by continuously learning from network traffic and system logs to identify emerging threats in real time. Supervised models, such as ensemble bagging trees, k-nearest neighbors, decision trees, support vector machines, and random forests, detect anomalies using labeled datasets, whereas unsupervised techniques, such as clustering and autoencoders, identify anomalies without predefined labels. This adaptability enables proactive defense against sophisticated cyberattacks.

In smart finance, machine learning extracts patterns from historical financial data to support predictions and decisions without explicit programming. Algorithms analyze large datasets to enhance decision-making, detect anomalies, and automate processes. For example, credit scoring models assess borrower risk by analyzing loan performance, transaction histories, and demographics, while machine learning-based fraud detection systems identify unusual transactions in real time. Common techniques include supervised methods such as regression and decision trees, unsupervised clustering for market segmentation, and ensemble methods like random forests and gradient boosting. Machine learning models are widely applied to credit scoring, fraud detection, algorithmic trading, and asset pricing, predicting outcomes such as default/non-default and fraudulent/legitimate transactions [138][139]. A hybrid LightGBM and extremely randomized trees model, for instance, predicts ICO token returns in smart-city financing with an R^2 of 0.814, highlighting token supply and Bitcoin returns as key drivers of performance [14]. Systematic reviews confirm that machine learning improves credit assessment, fraud detection, and market forecasting while emphasizing challenges in data quality, interpretability, and ethics [138].

5.2.2. Deep learning

Deep learning, a subset of machine learning, uses multi-layered neural networks to model complex, non-linear relationships in data [137]. These networks automatically extract hierarchical features from raw data, reducing the need for manual feature engineering. Typical architectures include input, hidden, and output layers, where data is transformed through hidden layers before reaching the output. This structure allows deep learning to handle high-dimensional data, detect intricate patterns, and improve predictive performance. Despite its accuracy, deep learning requires substantial computational resources and often functions as a "black box," necessitating optimization for both performance and interpretability [132-135].

In cybersecurity, deep learning enables the detection of sophisticated threats that conventional techniques may miss. Convolutional and recurrent neural networks identify complex attack patterns and zero-day vulnerabilities, while deep learning-based IDSs employ architectures such as gated recurrent units, bidirectional long short-term memory networks, and short-term memory networks. Deep learning enhances user authentication, malware detection, phishing prevention, and network anomaly detection, learning from large volumes of unstructured data to improve detection rates and reduce false positives.

In finance, deep learning excels at processing high-dimensional and unstructured data, including images, text, and time series. Recurrent neural networks and long short-term memory models predict stock prices based on historical trends and market sentiment, while convolutional neural networks support automated document processing and fraud detection. Deep learning improves accuracy in risk modeling, market forecasting, and customer behavior analysis compared with traditional machine learning. Integrating economic indicators and real-time sentiment into long short-term memory and recurrent neural network architectures yields more accurate stock and volatility forecasts, aiding investment and portfolio management decisions [138][140][141].

Advanced frameworks combining long short-term memory and one-dimensional convolutional neural networks with portfolio optimization strategies (mean–variance, risk parity, max drawdown) deliver superior risk-adjusted returns, as seen in Vietnamese equity markets. Long short-term memory-based portfolios outperform convolutional neural networks in both predictive accuracy and stability [142]. Emerging "deep finance" research leverages recurrent neural networks, long short-term memory networks, convolutional neural networks, and transformers for market prediction, risk analytics, algorithmic trading, and credit risk management, highlighting deep learning's ability to model complex financial systems and support informed investment strategies.

5.2.3. Natural language processing

Natural language processing (NLP) enables machines to understand, analyze, and generate human language. It consists of natural language generation (NLG) for producing coherent text and natural language understanding (NLU) for interpreting language. NLP combines supervised and unsupervised machine learning with rule-based approaches to analyze communications across emails, social media, and multimedia platforms. Core algorithms include tokenization, named

entity recognition (NER), and word embeddings, which extract insights from unstructured data for tasks such as sentiment analysis, speech recognition, translation, and text summarization.

In cybersecurity, NLP detects phishing attempts, social engineering, and malware by analyzing large communication datasets. It also supports identity and access management, automates incident response, and facilitates behavioral analysis, enhancing cybersecurity defenses [132-135].

In finance, NLP transforms unstructured textual data, such as news articles, reports, social media posts, and earnings call transcripts, into actionable insights. Applications include sentiment analysis to anticipate market reactions, automated compliance monitoring, and chatbots for customer support. Transformer-based architectures like Bidirectional Encoder Representations from Transformers (BERT) and Generative Pre-trained Transformer (GPT) improve financial text understanding and data-driven decision-making. Empirical studies report NLP achieves sentiment prediction accuracy of 92%, reduces processing time by 45%, and extracts critical metrics from reports with over 94% accuracy, supporting early risk detection and forecasting [143-145]. NLP-driven stock prediction models help investors reduce research time and improve accuracy, promoting adoption in inclusive finance contexts [146]. Generative NLP models are also increasingly applied in financial research for tasks such as chart analysis and coding, though concerns remain regarding bias, reliability, and ethics [145].

5.2.4. Reinforcement learning

Reinforcement learning enables agents to learn optimal strategies through interaction with their environment, using rewards and penalties as feedback. Agents adjust their behavior over time based on performance rather than explicit instructions. Reinforcement learning includes model-based, value-based, and policy-based approaches, with algorithms such as Q-learning, Deep Q-Networks (DQN), SARSA, Dyna-Q, and Monte Carlo methods.

In cybersecurity, reinforcement learning addresses dynamic challenges by enabling adaptive, proactive defenses. Reinforcement learning-driven intrusion detection systems evolve with emerging threats and optimize resource allocation for efficient risk mitigation. Threat intelligence platforms powered by reinforcement learning analyze diverse data sources to anticipate potential cyberattacks, enhancing network security, malware defense, and incident response [134][135].

In finance, reinforcement learning optimizes portfolio management, algorithmic trading, and risk mitigation by learning sequential decision policies. Reinforcement learning agents adjust asset allocation to maximize returns while minimizing risk, supporting high-frequency trading and dynamic market response. For example, a deep reinforcement learning model for agricultural finance, integrating data denoising, Long Short-Term Memory time-series modeling, and DQN learning, achieved ~45% annualized returns with a 35% lower maximum drawdown than benchmarks [147]. Reinforcement learning also enhances DeFi security, with deep reinforcement learning algorithms such as DQN and Proximal Policy Optimization (PPO) detecting vulnerabilities in Ethereum bytecode, thereby reducing financial risk [148]. Applications in energy finance further demonstrate reinforcement learning's suitability for volatile, constrained markets, optimizing trading, forecasting, and option valuation [149][150].

5.2.5. Federated learning

Federated learning (FL) enables collaborative machine learning without centralizing sensitive data. Models are trained locally on decentralized datasets, preserving privacy, improving regulatory compliance (e.g., GDPR), reducing network congestion, and enhancing efficiency [134]. In finance, FL enables multiple institutions to develop shared models for fraud detection or credit risk assessment without exposing customer data. This approach improves model generalization, reduces bias, and preserves privacy. Security and auditability are enhanced through techniques such as secure aggregation, differential privacy, and blockchain integration [37][138].

Practical applications demonstrate FL's effectiveness. In smart-finance architectures, banks collaboratively train risk and decision models, using blockchain for immutable transaction logs and smart contracts for participation automation, achieving ~95% prediction accuracy [37]. The DeFiSentinel framework integrates FL into decentralized finance, attaining MSE of 0.021 and R^2 of 0.96 for risk scoring, with a deep neural network achieving ~92% precision and 91.7% F1-score for fraud detection [70]. Vertical FL frameworks for cross-bank corporate financing combine differential privacy, homomorphic encryption, and improved FedAvg algorithms, achieving an AUC of 0.785 and a 12.4% F1-score improvement for cash-flow indicators [151]. Overall, FL bridges financial data silos, enabling collaborative modeling while maintaining strict data protection standards [152]. Figure 11 illustrates the artificial intelligence techniques in smart finance.

Fig. 11. Illustrates the artificial intelligence techniques in smart finance.

5.3. Artificial Intelligence Techniques for Security

AI techniques have become essential for enhancing security in both digital and physical systems. By leveraging machine learning, deep learning, and pattern recognition, AI can detect anomalies, identify threats, and respond to attacks in real time. Techniques such as supervised and unsupervised learning, reinforcement learning, and neural networks enable systems to process vast amounts of data, uncover complex patterns, and anticipate potential security breaches. In cybersecurity, AI automates tasks including threat detection, malware classification, intrusion detection, and fraud prevention, often surpassing traditional rule-based approaches in efficiency and accuracy. As cyber threats grow increasingly sophisticated, AI-driven security solutions offer adaptive, proactive, and scalable defenses that respond dynamically to emerging risks.

5.3.1. Machine learning for fraud detection

Machine learning is now a cornerstone of fraud detection in financial systems, enabling the identification of unusual patterns and behaviors in transactional data. In smart finance, models analyze large volumes of structured and unstructured data, including credit card transactions, banking logs, and user activity, to detect fraudulent activity effectively. Supervised learning remains the primary approach, with models such as Logistic Regression, Decision Trees, Random Forests, Gradient Boosting, and Light GBM trained on labeled datasets containing both legitimate and fraudulent transactions. These models classify new transactions based on observed patterns, achieving higher accuracy and reliability than traditional rule-based methods [153].

Financial fraud datasets are often highly imbalanced, with fraudulent transactions representing only a small fraction of records. To address this, unsupervised techniques such as Isolation Forests, Autoencoders, and clustering methods detect anomalies without requiring explicit fraud labels. Hybrid models that combine supervised classification with anomaly detection have demonstrated superior performance, achieving higher precision and fewer false positives by capturing both known and emerging fraud patterns. Machine learning applications in financial fraud now cover a broad range of scenarios, including credit card fraud, identity theft, insider threat monitoring, and forensic accounting [154]. Supervised models are trained on labeled “fraud” versus “legitimate” records, while unsupervised and semi-supervised approaches focus on detecting anomalies within largely legitimate datasets [155-157].

In large-scale financial markets, ensemble methods, such as stacking Linear Regression, Decision Trees, Random Forests, Gradient Boosted Trees, Support Vector Machines, and Neural Networks, achieve approximately 95% accuracy, 93% recall, and 94% F1-score. These methods outperform individual models and remain robust even when real-world transaction volumes exceed 1 million records [155]. Other studies report that Random Forest and similar ensemble models

can reach 98–99% accuracy with reduced false positives, making them suitable for real-time credit card and online payment fraud detection [156]. Consequently, banks and payment platforms widely deploy machine learning models for real-time transaction and account risk scoring [155][157][158].

Despite these advances, challenges remain, including class imbalance, noisy or incomplete data, and evolving fraud tactics. Recent research emphasizes solutions such as resampling, cost-sensitive learning, and feature engineering. There is also growing attention on explainable and privacy-preserving machine learning approaches, including federated learning, to meet regulatory requirements and maintain user trust in smart financial systems [156-158].

5.3.2. Deep learning for anomaly detection

Deep learning uses multi-layered neural networks to automatically extract features and detect complex anomalies that traditional methods may overlook. By learning non-linear, temporal, and high-dimensional patterns in transaction streams, deep learning can identify subtle deviations indicative of fraud or other anomalous activity [47][153].

Several deep learning architectures have proven effective for financial anomaly detection. Autoencoders reconstruct input data; large reconstruction errors signal anomalies. Recurrent Neural Networks and Long Short-Term Memory networks excel at detecting temporal irregularities in sequential data, such as sudden spikes in account activity. Convolutional Neural Networks, applied to structured or semi-structured data, capture spatial or relational anomalies. Hybrid models, such as Convolutional Neural Networks combined with Gated Recurrent Units (GRUs) with attention mechanisms or Deep Random Forests that pair Convolutional Neural Network feature extraction with Random Forest classification achieve high F1 scores and AUC values (92–97%) while scaling to real-time banking environments and handling imbalanced, high-dimensional datasets [159][160].

Deep learning also extends to sparsely labeled or novel scenarios. Autoencoders trained on normal transactions can detect anomalous activity, including fraud, through reconstruction errors. In blockchain and cryptocurrency networks, these models achieve recall rates around 98–99% [159-163]. Graph Neural Networks (GNNs) applied to transaction graphs where wallets are nodes and flows are edges effectively detect money laundering, phishing scams, and Ponzi schemes, achieving F1 scores near 0.92 and outperforming traditional methods [159][162][164].

Adaptive approaches, such as deep reinforcement learning with Deep Q-Networks and transfer learning, optimize fraud-response policies while leveraging pre-trained feature extractors. These methods often outperform Random Forest and XGBoost baselines in AUC-ROC and computational efficiency, making them suitable for cloud-based smart finance platforms where transaction patterns evolve rapidly [165]. Challenges remain in interpretability and computational cost. High model complexity and resource demands must be balanced against security benefits. Nonetheless, deep learning frameworks, Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), Long Short-Term Memory networks (LSTMs), autoencoders, Generative Adversarial Networks (GANs), and hybrid models, offer robust, scalable, and automated approaches to anomaly detection, particularly when traditional methods struggle with high-dimensional, non-linear, or temporal patterns [11][159][160][163].

5.3.3. Natural language processing for phishing and social engineering detection

Natural language processing enables computers to analyze and understand human language, making it critical for detecting phishing emails, social engineering attacks, and fraudulent communications across email, SMS, chat applications, and imitation websites. Modern NLP models analyze content, formatting, metadata, and context to identify high-risk messages and impersonations of legitimate entities [153]. Transformer-based models, including Bidirectional Encoder Representations from Transformers (BERT), Robustly Optimized BERT Pretraining Approach (RoBERTa), and Distilled BERT (DistilBERT), excel at capturing semantic context and subtle language variations beyond keyword filtering. These models achieve high accuracy in phishing detection and are widely integrated into secure email gateways and e-banking systems to flag suspicious messages and support analyst triage. As cybercriminals increasingly leverage AI to generate highly realistic and personalized phishing content, NLP-based defenses remain a critical component of financial cybersecurity.

NLP supports detection across text- and voice-based channels, including emails, websites, chat platforms, and calls. For instance, studies using Naive Bayes, Support Vector Machines, and Random Forest classifiers on cleaned email datasets have shown Support Vector Machine-based NLP models achieving approximately 98% accuracy, precision, recall, and F1-score in phishing detection [166]. Adversarially trained NLP models and continuous monitoring are increasingly necessary to identify AI-generated phishing, deepfake text, and synthetic identities [114]. Multimodal AI frameworks now combine pre-trained transformers with deepfake voice recognition and behavioral biometrics, achieving high detection accuracy and minimal false positives in enterprise and transactional environments [167]. Broader research emphasizes integrating NLP-driven fraud detection, voice forensics, and behavioral signals to proactively detect targeted phishing attacks, including CEO fraud and deepfake scams, before significant financial losses occur [114][167].

Beyond threat detection, NLP also supports complaint and sentiment analysis. Multitask models applied to social media and customer complaints enable regulators and financial institutions to identify emerging fraud schemes and abusive practices, potentially preventing large-scale incidents. By combining semantic understanding with contextual and

behavioral insights, NLP has become an indispensable tool for proactive, predictive defense in modern smart finance systems [168]. Figure 12 illustrates the artificial intelligence techniques for security.

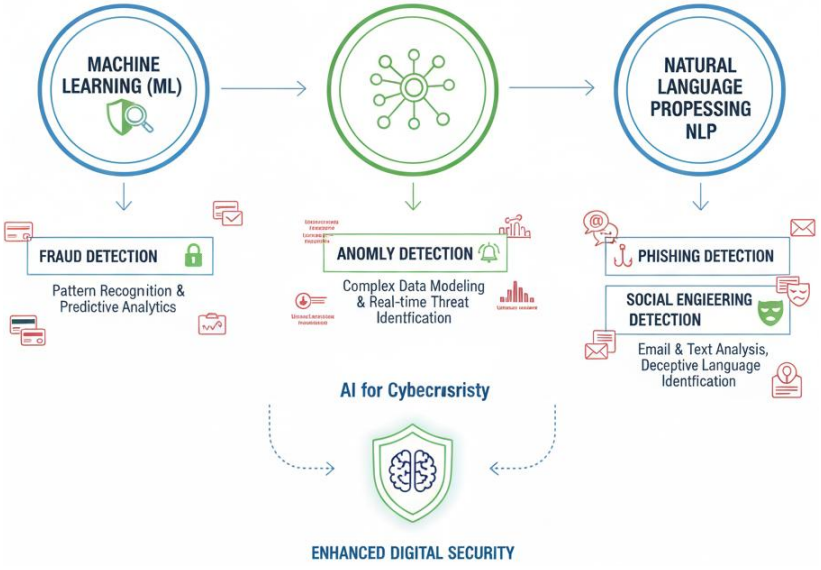

Fig. 12. Illustrates the artificial intelligence techniques for security.

5.4. Artificial Intelligence Applications in Securing Smart Finance

AI is transforming the security landscape of smart finance by enabling proactive detection and prevention of financial threats. As reliance on digital platforms grows, financial systems are increasingly vulnerable to sophisticated cyberattacks, fraud, and phishing schemes. By leveraging machine learning, deep learning, natural language processing, reinforcement learning, and predictive analytics, AI can detect anomalous behaviors, identify fraudulent transactions, and strengthen authentication mechanisms. Continuous analysis of large volumes of financial data not only enhances security but also improves operational efficiency, ensures regulatory compliance, and reinforces user trust in digital financial services. Key AI applications in securing smart finance are briefly explained below.

5.4.1. Credit scoring and risk analysis

AI enables financial institutions to predict customer risk with higher precision by analyzing diverse data sources, including behavioral, transactional, and alternative data. Machine learning algorithms examine spending patterns, consistency of incoming funds, mobile phone usage, and other aspects of a customer's digital presence. These methods allow institutions to assess creditworthiness more accurately than traditional statistical models. Beyond conventional credit bureaus, global examples illustrate AI's transformative impact. Equity Bank in Kenya uses machine learning to create behavioral risk profiles for its digital lending platforms, drawing on mobile wallet activity and repayment histories. This approach provides millions of previously unbanked or underbanked customers access to credit without collateral or paper-based documentation while maintaining healthy non-performing loan ratios. Similarly, Standard Chartered Bank's global digital lending program evaluates loan applications within minutes by analyzing card spending, usage trends, and repayment behavior. Real-time monitoring enables dynamic interest rate adjustments, stabilizing the credit portfolio. AI models further enhance credit scoring by incorporating structured and unstructured data beyond traditional credit histories. Algorithms assess financial behavior, spending patterns, and social signals to predict default risk.

FinTech's such as Zest AI employ Random Forest and Gradient Boosting models to generate dynamic credit scores, enabling more inclusive lending. Advanced deep learning platforms, including BSCNN-based CSRA-DPLP-BSCNN, process Buy-Now-Pay-Later (BNPL) and e-commerce data, apply filtering techniques, and predict default risk with ~98% accuracy (ROC≈0.95), supporting near-real-time lending decisions for thin-file borrowers [169]. Systematic reviews show AI/machine learning models improve default-prediction accuracy by ~15% over traditional scoring while promoting financial inclusion [170]. Optimized models have reduced non-performing loan losses by up to 30 percentage points, although misjudgment rates of 28% in underserved segments highlight risks from biased data and "black-box" models [171]. Regression-based AI risk models further provide continuously retrained probability-of-default estimations, enhancing responsiveness to macroeconomic and portfolio shifts [172]. Adoption, however, remains constrained by organizational, environmental, and regulatory factors, with governance and readiness often outweighing purely technological considerations [173].

5.4.2. Automated trading security and market surveillance

Traditional methods for monitoring trades struggle to keep up with the volume and complexity of modern electronic markets. AI algorithms address this by analyzing order books, market microstructure, and historical trading behavior to detect anomalies such as insider trading, spoofing, and market manipulation. LSEG, for example, uses machine learning to monitor equities and derivatives, flag unusual trading patterns, and provide real-time alerts for regulatory compliance. JP Morgan similarly employs AI to differentiate legitimate algorithmic strategies from suspicious activity. AI reduces detection latency, enabling more effective identification of sophisticated manipulation and improving market stability. Techniques such as deep learning and anomaly detection flag unusual spikes in stock volumes, indicating potential pump-and-dump schemes. Advanced systems detect high-frequency trading anomalies with 97.5% accuracy and <1% false positives, processing ~150,000 trades per second with ~15 ms latency [174]. Combining supervised and unsupervised learning, NLP, and network analytics, AI detects spoofing, front-running, and coordinated schemes, improving detection rates by 20–30% for certain manipulations [174][175]. Ethical challenges remain, including privacy of traders, confidentiality of strategies, cross-border data governance, and model explainability, prompting exploration of federated learning, differential privacy, and explainable AI solutions [175][176].

5.4.3. Transaction monitoring and fraud detection

AI-powered fraud detection has become essential as cybercriminals adopt increasingly sophisticated tactics. Machine learning models evaluate device identifiers, geolocation, transaction velocity, spending patterns, and biometrics to distinguish legitimate transactions from fraud [177]. Mastercard's Decision Intelligence platform scores every transaction in real time using cardholder behavior, device intelligence, and merchant history, reducing false declines and proactively preventing fraud. In Africa, Flutterwave leverages AI-based anomaly detection to flag unusual merchant or customer activity, while Standard Bank uses behavioral analytics to mitigate SIM-swap fraud, account takeovers, and unauthorized transfers. AI employs supervised learning for known fraud patterns and unsupervised deep learning for novel anomalies. Techniques such as Long Short-Term Memory networks, autoencoders, and Isolation Forests detect temporal fraud patterns with high precision, minimizing false positives and latency [178][179]. Hybrid unsupervised methods leveraging contextual features achieve ~99.2% accuracy, enabling scalable, real-time analysis with limited labeled data. End-to-end AI ecosystems that integrate feature engineering, explainable models, and ID verification address class imbalance, privacy, and emerging fraud tactics [180][181].

5.4.4. Anti-money laundering and know your customer compliance

AI enhances AML and KYC processes by detecting hidden financial networks, analyzing complex transactions, and flagging suspicious behaviors. Unlike traditional methods, AI reduces false positives and focuses on high-risk cases [95]. HSBC, for instance, cut false-positive alert rates by up to 60% through AI-based monitoring, uncovering unusual fund movements and connections among seemingly unrelated accounts. Barclays UK automates document extraction, sanction-list screening, and biometric verification to streamline onboarding while ensuring regulatory compliance. Nigerian FinTechs, such as Kuda Bank, use AI-driven ID authentication to prevent onboarding fraud. Hybrid classifiers integrating Support Vector Machines, K-Nearest Neighbors, and Random Forests on on-chain features achieve >99% accuracy in detecting suspicious transactions, demonstrating AI's role in tracing illicit crypto flows and sanctions evasion [182][183]. Surveys highlight explainable AI and bias control as critical for regulatory acceptance in AML/KYC and sanctions screening [170][180].

5.4.5. Customer authentication and identity verification

AI strengthens digital identity verification by combining biometrics, behavioral analytics, and liveness detection. Beyond traditional face or fingerprint recognition, AI assesses facial texture, micro-expressions, voice patterns, and user-specific behavioral signatures. Mastercard Identity Check implements AI-powered facial biometrics and real-time liveness detection for online transactions. Revolut uses facial recognition and document-scanning algorithms to enhance onboarding efficiency, while Capitec Bank in South Africa applies AI-driven facial verification to reduce impersonation and account takeover risks. Behavioral biometrics continuously authenticate users during sessions, tracking keystrokes, mouse movements, device handling, and navigation patterns. Systems like BioCatch detect account takeover attempts in real time with ~97.9% accuracy, 95.6% precision, and 93.4% recall [184]. Multimodal, low-friction monitoring triggers step-up authentication only when anomalies occur, and federated learning emerges as a privacy-preserving solution [185][186].

5.4.6. Cyber-threat detection and network security

AI enhances cybersecurity by detecting malware, intrusions, and abnormal network behaviors. Financial institutions such as Wells Fargo and FNB South Africa employ neural network-based anomaly detection to monitor millions of endpoints in real time, automating responses like account suspension, credential reissuance, or device isolation. AI classifies network traffic and identifies unusual access patterns, with platforms like Darktrace alerting institutions to potential intrusions. Integrated AI architectures, combining real-time financial data processing, DevSecOps practices, and observability,

maintain secure, fault-tolerant pipelines. Graph neural networks and time-series models enforce governance, access control, and trade data security [187][188].

5.4.7. AI-powered chatbots and secure customer interaction

AI chatbots improve customer support while providing security oversight. Bank of America's Erica analyzes historical behavior to detect unusual spending patterns and alerts customers to potential fraud. Ecobank's virtual assistant monitors interactions across Africa for signs of social engineering, preventing manipulation. Real-time NLP, anomaly detection, and Large Language Model-enabled architectures integrate risk and fraud controls, compliance monitoring, logging, and identity verification [176][187].

5.4.8. Insurance fraud detection

AI underpins insurance fraud detection by reviewing claims, analyzing imagery, and identifying data inconsistencies. Discovery Insure in South Africa evaluates telematics, accident reports, and claim narratives to detect discrepancies between reported incidents and actual driving behavior. Allianz Global Insurance uses AI for document verification and medical-claims analysis, outperforming traditional systems in identifying inflated, duplicated, or falsified claims. Machine learning models, including XGBoost, Random Forests, neural networks, and autoencoders, achieve ~87% accuracy in simulated datasets [189]. Ensemble models that combine Bi-Long Short-Term Memory (Bi-LSTM) and Random Forests improve robustness on imbalanced life-insurance datasets, while generative models, including Generative Adversarial Networks (GANs) and Variational Autoencoders (VAEs), address class imbalance and enhance anomaly detection [190][191].

5.4.9. Portfolio, investment, and market-risk prediction

AI predicts market trends, portfolio risks, and investment opportunities by analyzing historical prices, financial news, and social sentiment. BlackRock's Aladdin platform employs machine learning to assess macroeconomic indicators, geopolitical events, and portfolio history, enabling proactive trading adjustments [115]. Long Short-Term Memory and Transformer architectures capture long-term and non-linear dependencies in asset returns, yielding higher Sharpe and Sortino ratios than classical approaches [192]. Hybrid Long Short-Term Memory–AutoRegressive Integrated Moving Average (LSTM–ARIMA) models achieve up to 92.7% accuracy in market-risk prediction, supporting proactive risk management [193]. Real-time portfolio rebalancing, robo-advisory, and anomaly-based compliance monitoring further illustrate AI's role in modern asset management [194].

5.4.10. Smart-contract and blockchain security

AI complements blockchain adoption by auditing smart contracts, monitoring DeFi activities, and detecting anomalies. IBM uses AI to analyze smart contract logic and identify vulnerabilities pre-deployment, while DBS Bank monitors blockchain transaction flows to flag suspicious wallets and prevent money laundering [28]. Deep learning and Generative Adversarial Network-assisted architectures achieve up to 97.6% accuracy in detecting smart-contract malware. Explainable AI frameworks halt execution upon violation detection, reaching 99.68% accuracy with >99% precision/recall [195][196]. Broader surveys highlight AI's role in optimizing consensus mechanisms, intrusion detection, and privacy-preserving federated learning in blockchain systems [197].

5.4.11. Behavioral biometrics for continuous authentication

Behavioral biometrics use machine learning to monitor keystrokes, mouse movements, smartphone handling, and navigation patterns for continuous authentication [115]. Unlike static biometrics, these systems verify user identity during sessions. ING Bank tracks app interactions to identify impostors, while Westpac and other Australian banks detect unauthorized account access, enhancing security without reducing convenience. Multimodal approaches combining behavioral, device, network, and transactional data achieve ~97.9% accuracy, substantially lowering false positives [184][185]. Federated learning is being explored to preserve privacy while updating global models [186].

5.4.12. Loan application fraud and document forensics

AI evaluates loan applications for synthetic identities, data inconsistencies, and counterfeit documents. NLP and visual forensics validate employment letters, bank statements, and ID documents [97]. KCB Kenya uses AI to detect altered documents, while RBC in Canada identifies synthetic identity fraud via cross-record analysis. Intelligent document processing automates extraction, cross-checking, and anomaly detection, reducing approval times by up to 70%, improving document-based fraud detection by 50%, and lowering compliance costs by ~40% [198][199].

5.4.13. Algorithmic trading security

AI safeguards automated trading systems against market manipulation, spoofing, and insider trading. Goldman Sachs uses AI-driven systems to monitor trades in real time, flag suspicious activity, and enforce compliance rules. Machine learning-based market-risk prediction identifies abnormal volatility or price manipulation that could affect algorithmic trading

systems [192][193]. Continuous-learning architectures, behavioral monitoring of traders, and workstation usage tracking mitigate rogue-trader risks and compromised terminals [184][185]. Real-time transaction-monitoring models using Random Forests, gradient boosting, Long Short-Term Memory networks, and graph neural networks detect irregular trading behaviors and account takeovers, complementing broader AI fraud frameworks in financial services [199][200].

5.5. Benefits of Using Artificial Intelligence in Securing Smart Finance

Below are brief descriptions of some of the benefits attained while using AI to secure smart finance.

5.5.1. Fraud detection and prevention

AI excels at identifying abnormal patterns in financial transactions that may indicate fraud. Machine learning algorithms analyze historical data to detect anomalies in real time. For example, banks like JPMorgan Chase use AI to flag unusual credit card transactions, preventing fraudulent withdrawals or purchases. AI models detect subtle deviations from normal customer behavior, such as atypical transaction amounts or locations. By learning complex, evolving attack patterns from large datasets, AI shifts fraud management from reactive to proactive. Advanced techniques, including deep learning, graph analytics, and autoencoders, identify subtle anomalies, such as rapid multi-account transfers or unusual merchant networks, and outperform traditional rule-based systems in accuracy and recall [58][180][201]. For instance, graph neural networks combined with autoencoders achieve high precision and recall in real-time credit-card fraud detection [202]. Platforms used by PayPal, Visa, and JPMorgan leverage deep learning and big data analytics to detect complex, low-signal fraud at scale [203][204].

5.5.2. Real-time threat monitoring

AI enables continuous monitoring of networks and systems, detecting potential cyber threats in real time and reducing financial breach risks. Platforms like Darktrace use unsupervised machine learning to identify unusual activity, including unexpected logins or data exfiltration, and alert security teams immediately. Modern AI systems continuously score every transaction and behavior stream with near-zero downtime, enabling instant blocking or step-up verification rather than batch reviews [205-208]. This approach has improved fraud detection rates from approximately 66% in rule-based systems to over 90%, while reducing detection time from hours to minutes [206][207].

5.5.3. Enhanced identity verification

AI strengthens authentication by leveraging biometric data, behavioral patterns, and multi-factor verification. Banks such as HSBC employ AI-driven facial recognition and fingerprint scanning to restrict account access to authorized individuals, mitigating identity theft risk. AI enhances KYC and onboarding through multimodal biometrics, including face, voice, and behavior, and automated document analysis, reducing incidents of identity theft and synthetic identities [180] [208-210]. Natural language processing and computer vision validate documents and cross-reference external digital traces, while frameworks combining facial recognition, behavioral biometrics, and geolocation detect deepfake-enabled and synthetic identity fraud more accurately than traditional password-based methods [211].

5.5.4. Predictive risk management

AI analyzes large datasets to anticipate potential risks such as credit defaults and market fluctuations, enabling proactive mitigation. AI-driven credit scoring models, such as Zest AI, predict loan default likelihood, helping lenders make informed decisions and stabilize financial systems. Machine learning–based predictive analytics estimate credit, market, and fraud risk, supporting proactive control over limits, pricing, and exposure [58][71][207]. AI credit scoring and early-warning models flag likely defaulters and at-risk portfolios before losses materialize. Integrated frameworks can jointly model fraud and credit risk to optimize approvals and collections in real time [58][207].

5.5.5. Automated regulatory compliance

AI simplifies compliance with complex financial regulations by continuously monitoring transactions and generating reports, minimizing human error and legal risk. Platforms like Ayasdi help banks detect suspicious transactions for AML compliance, reducing auditor workload while ensuring regulatory compliance. RegTech systems leverage AI to interpret regulations, monitor obligations, and map them to transaction and customer data, automating AML/KYC checks and reporting [58][210][212]. AI-enhanced ERP and cloud compliance platforms automate KYC/AML processes, risk scoring, and control testing while maintaining detailed audit trails and preserving explainability for model-risk and transparency requirements in credit and fraud decisions [180][212].

5.5.6. Advanced threat intelligence

AI analyzes cyberattack trends and threat intelligence to identify emerging risks and recommend mitigation strategies. Financial institutions employ AI platforms to detect ransomware and attacks targeting ATMs or payment systems. By aggregating internal and external data, including behavioral logs, blockchain flows, and dark-web intelligence, AI continuously updates threat models alongside attacker tactics [201][204][206]. Tree-based and graph-based models in

decentralized finance highlight risk clusters associated with rug pulls or wash trading, while AI trained on large-scale card and cryptocurrency datasets detects botnets, AI-generated phishing, and cross-platform money-laundering paths that evade static rules [201][204].

5.5.7. Secure automated transactions

AI enhances the security of automated financial operations, including smart contracts and algorithmic trading, by monitoring for errors or malicious activity. In DeFi, AI algorithms monitor smart contracts on the blockchain for irregular behavior, preventing unauthorized transfers or exploits. Smart contracts integrated with AI decision engines enable tamper-resistant, self-executing workflows with embedded risk checks [70][206][210]. Cryptographic smart contracts enforce transaction rules, while AI performs anomaly detection and risk scoring before execution, strengthening integrity and reducing fraud. AI-driven payment processors also adjust risk thresholds and routing in real time to minimize fraud and false declines [206][207].

5.5.8. Adaptive authentication systems

AI-driven authentication systems dynamically adjust security requirements based on risk assessment, balancing security and user experience. For instance, PayPal increases verification measures, such as OTPs or biometric checks, when unusual behavior is detected. Behavioral biometrics and geolocation analyses modulate multi-factor authentication for high-risk situations while maintaining seamless access for low-risk behavior [180][206][208][210].

5.5.9. Efficient cybersecurity resource allocation

AI helps financial institutions prioritize security resources by identifying high-risk areas and vulnerabilities. By scoring risk at transaction, user, and portfolio levels, AI directs human and technical resources to the most critical events, improving efficiency [58][71][180][207]. Triage systems present top-risk alerts to analysts, reducing alert fatigue and investigation backlogs. Predictive risk scores also guide strategic allocation of monitoring intensity, capital buffers, and incident-response capacity across products and regions [58][71][213].

5.5.10. Continuous learning and improvement

AI systems continually learn from new data, evolving threats, and user behaviors, enhancing security over time. Fraud detection systems like Mastercard's Decision Intelligence improve with each flagged transaction, reducing false positives and strengthening future protection. Machine learning models retrain on emerging fraud patterns, market conditions, and user behaviors, transforming security into a self-improving capability. Unsupervised models, such as clustering and autoencoders, detect previously unseen fraud schemes and provide insights to supervised detectors [201]. Reinforcement-learning engines and real-time transaction monitors continuously refine policies, minimizing fraud and false positives without manual rule updates [201] [205-207].

Blockchain technology further strengthens AI in securing smart finance by providing a decentralized, transparent, and tamper-resistant ledger. Its distributed architecture ensures immutability and verifiability of records, reducing the risk of fraud and unauthorized access. When integrated with AI, blockchain enables secure data sharing, real-time fraud detection, and enhanced regulatory compliance. Together, these technologies establish a robust, intelligent, and resilient framework that safeguards sensitive information and reinforces trust in digital financial ecosystems.

6. BLOCKCHAIN IN SMART FINANCE SECURITY

6.1. Overview of Blockchain Technology

Blockchain technology, introduced by Satoshi Nakamoto in 2008, is a decentralized and distributed ledger that chronologically records transactions in cryptographically linked blocks. Each block contains a header with metadata timestamp, previous block hash, current block hash, and Merkle root and a body storing validated transactions authenticated through digital signatures [214-218]. By immutably linking blocks, blockchain prevents retroactive alterations without achieving consensus across the network, thereby enhancing data integrity, security, and transparency [215-218].

Blockchain's core features decentralization, immutability, transparency, security, consensus mechanisms, smart contracts, traceability, tokenization, and anonymity support diverse applications [214-219]. Systems are categorized by access control: public blockchains allow open participation but may compromise privacy; private blockchains restrict access to authorized users, enhancing confidentiality; consortium blockchains combine selected governance with decentralization; and hybrid blockchains integrate public and private elements for selective transparency [219]. Operating over peer-to-peer networks, blockchain distributes storage and processing across nodes, where consensus algorithms validate blocks and digital signatures authenticate transactions. Miners or validators receive rewards through Proof-of-Work (PoW), Proof-of-Stake (PoS), or Proof-of-Authority (PoA), incentivizing honest participation and preventing unauthorized actions [218]. Smart contracts extend functionality by automatically executing predefined agreements, reducing the need for intermediaries, and enhancing transparency.

These foundational properties directly enable blockchain's transformative role in smart finance. As a distributed ledger, blockchain records transactions across multiple nodes, eliminating unilateral control, enhancing trust, and preserving data integrity. Immutability prevents unauthorized modifications, reducing fraud and simplifying auditing and regulatory compliance. Cryptographic mechanisms, including hashing and public–private key encryption, protect transaction data and user identities while mitigating risks associated with centralized systems.

Smart contracts further streamline financial operations by automating payments, enabling real-time settlement, and enforcing rules, lowering costs and improving speed, accuracy, and efficiency in lending, insurance, and asset management. Blockchain also facilitates secure, auditable data sharing among banks, FinTech firms, regulators, and customers, promoting interoperability and privacy in applications such as cross-border payments, trade finance, and collaborative fraud detection. Integration with AI and big data analytics enhances predictive modeling, risk assessment, and real-time decision-making, providing high-quality, reliable data for financial intelligence systems.

Consequently, blockchain is emerging as a foundational infrastructure for smart finance data-driven, automated, and AI-enabled delivering decentralized, tamper-resistant ledgers and programmable smart contracts across banking, capital markets, decentralized finance, green finance, and smart-city initiatives [2][10][75][220][221]. By reinforcing decentralization, security, transparency, and automation, blockchain improves operational efficiency, system resilience, and stakeholder trust, enabling innovative financial services and sustainable long-term growth without altering core financial infrastructure. Figure 13 illustrates blockchain in smart finance.

Fig. 13. Illustrates blockchain in smart finance.

Blockchain-based smart finance relies on three foundational concepts distributed ledger technology, consensus mechanisms, and smart contracts that collectively enable secure, transparent, and automated financial systems. These technical pillars distinguish blockchain architectures from traditional centralized financial models by decentralizing trust, ensuring agreement among participants, and allowing programmable transaction execution. Together, they underpin innovations such as electronic assets, decentralized financial institutions, and automated regulatory compliance systems, driving the progressive transformation of financial infrastructure over time [30].

6.1.1. Distributed ledger technology

Distributed ledger technology (DLT) underpins blockchain systems by maintaining a shared, synchronized database across independent nodes rather than a single centralized authority. Each transaction is consistently recorded across multiple identical ledger copies in different locations. The absence of a central control point prevents any single entity from altering the complete record set, significantly reducing the risk of data manipulation [97]. Transactions are cryptographically linked, creating an immutable, chronological record, while consensus mechanisms ensure that entries are added only after participants validate their legitimacy, eliminating the need for trusted intermediaries and guaranteeing a uniform ledger state across nodes [34].

DLT's decentralized architecture enhances fault tolerance and resilience because the failure or compromise of a single node does not compromise the overall system integrity. By increasing transparency, traceability, and auditability, DLT supports

secure transaction verification, fraud detection, financial reporting, regulatory compliance, risk management, and dispute resolution [152]. In smart finance, DLT enables decentralized storage of financial transactions, asset ownership records, and contractual agreements, facilitating secure multiparty computation and trusted data sharing among banks, FinTech firms, and regulators. Its core properties immutability, cryptographic integrity, and transparency reduce fraud and discrepancies while providing real-time, auditable transaction histories [34][222][223].

DLT underpins applications such as banking, supply-chain finance, DeFi, tokenized assets, and central bank digital currencies (CBDCs). These technologies accelerate settlement, lower counterparty and operational risk, and enable new financial instruments [222-225]. In contrast, advances in performance, energy efficiency, and embedded application logic support sophisticated financial applications, including DeFi protocols and non-fungible tokens (NFTs), widespread adoption in mainstream finance remains constrained by scalability, interoperability, and regulatory uncertainty [34][223][224].

6.1.2. Consensus mechanisms

Consensus protocols enable distributed blockchain nodes to agree on the validity and order of transactions, ensuring security, reliability, and trust in environments where participants may not fully trust one another [34]. These mechanisms directly affect blockchain security, throughput, energy efficiency, and decentralization, which are critical for financial applications that require speed, resilience, and regulatory compliance. Proof of Work (PoW), the original consensus mechanism introduced with Bitcoin, validates blocks through computationally intensive puzzles. While secure, its high energy consumption and low throughput limit its suitability for enterprise financial systems. Proof of Stake (PoS) improves scalability by selecting validators based on token holdings, though it can concentrate power among wealthier stakeholders. Delegated Proof of Stake (DPoS) enables token holders to elect delegates for fast transaction validation, suitable for retail payments, but the small number of delegates may raise transparency concerns. Other mechanisms, including Practical Byzantine Fault Tolerance (PBFT) and Proof of Authority (PoA), cater to consortium and private blockchains, offering rapid agreement and low-latency operations while balancing centralization risks [30]. Emerging protocols, such as Proof-of-Activity-and-Delegation (PoAD) and AI-augmented consensus, improve throughput, reduce latency, and enhance energy efficiency, while social-capital–based approaches aim to strengthen fairness and decentralization [226][227]. Collectively, these mechanisms secure transaction validation, prevent double-spending, and support reliable, compliant financial operations across both permissionless and permissioned blockchain environments [34][228][229].

6.1.3. Smart contracts

Smart contracts are self-executing programs that automatically enforce predefined rules when conditions are met, reducing the need for intermediaries, lowering administrative costs, and enhancing transactional speed, transparency, and trust [9][10][75]. In finance, they encode agreements, such as loan terms, insurance policies, and payment schedules, directly into executable code, which enables automated payments, escrow management, insurance claims processing, and compliance reporting while cryptographically verifying execution accuracy [152].

Smart contracts guarantee immutability, fostering trust and reducing the risk of disputes. Advances in auditing and formal verification have accelerated adoption, particularly in digital entrepreneurial finance, tokenized equity, and decentralized investment platforms. In cross-border payments, they automate settlement, integrate programmable KYC/AML and CBDC rules, and enable real-time gross settlement, payment-versus-payment (PvP), and delivery-versus-payment (DvP), enhancing both speed and auditability [230]. In federated-learning–enabled smart finance, smart contracts coordinate participation, incentives, and access control, supporting privacy-preserving model training and immutable recording of contributions [37][70].

DeFi platforms rely heavily on smart contracts for lending, exchanges, derivatives, and liquidity pools, boosting efficiency and security while facing scalability, energy, and regulatory challenges [36][70][223]. Integrating AI allows adaptive contracts that optimize execution, adjust to regulatory changes, detect fraud in real time, and support decentralized governance and risk management [70]. Regulatory scholarship emphasizes techno-legal standardization to ensure cross-border smart contract automation aligns with diverse legal systems, supports interoperability, KYC/AML compliance, and integrates with legacy infrastructures such as SWIFT [75][230].

Distributed ledger technology, consensus mechanisms, and smart contracts collectively establish a secure and efficient foundation for smart finance. By enabling decentralized trust, ensuring data integrity, and automating financial processes, these technologies facilitate intelligent, scalable, and resilient financial ecosystems that support seamless, transparent, and reliable operations across diverse applications. Figure 14 illustrates distributed ledger technology, consensus mechanisms, and smart contracts as foundational concepts of blockchain in smart finance.

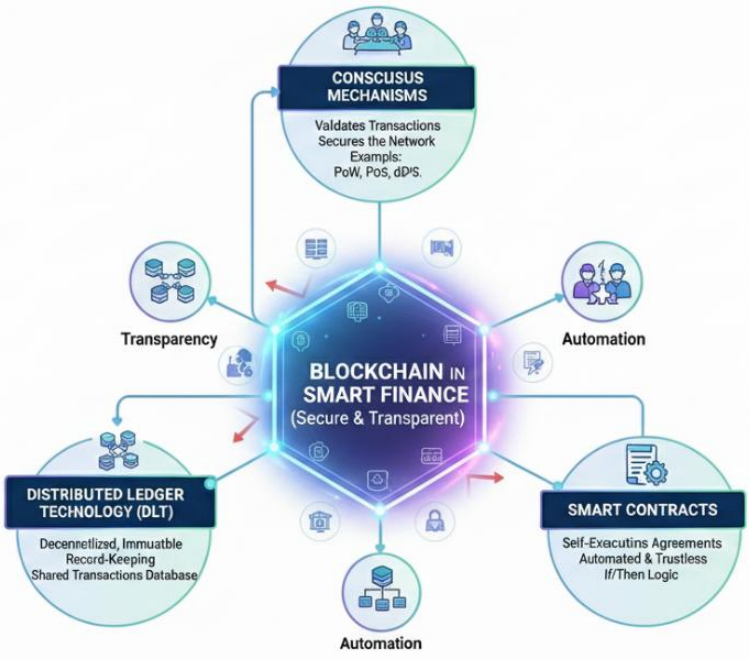

Fig. 14. Illustrates distributed ledger technology, consensus mechanisms, and smart contracts as foundational concepts of blockchain in smart finance.

6.2. Blockchain Applications in Securing Smart Finance

Blockchain technology underpins modern financial security by ensuring transparency, traceability, immutability, and cryptographic integrity. By providing verifiable, tamper-resistant transaction records, it enhances trust and accountability across financial systems, enabling secure, reliable operations across diverse applications. Below are the brief descriptions of key applications of blockchain in securing smart finance, with supporting examples.

6.2.1. Secure digital payments and settlements

Blockchain eliminates the need for intermediaries, enabling fast, secure transactions through decentralized validation. Settlement times are reduced from days to seconds, account reconciliation delays are minimized, and the risk of fraud or double-spending is reduced [28]. Consequently, major financial institutions increasingly adopt blockchain solutions for international transfers. By enhancing transparency and reducing disputes, these solutions improve customer confidence. Cryptographically signed transactions are immutably recorded, ensuring authenticity and non-repudiation. Blockchain-based payment networks support near-real-time cross-border remittances, thereby mitigating fraud compared with traditional banking systems [60][75]. Smart contracts automate payments under predefined conditions, reducing human error and reconciliation delays [60]. Biometric and multi-factor authentication, such as iris scanning, further secures transactions by restricting access to authorized users [60]. Central-bank digital currencies (CBDCs) and tokenized assets also enable secure on-chain Real-Time Gross Settlement and Payment versus Payment/Delivery versus Payment settlements [75].

6.2.2. Cross-border remittances and international transfers

Traditional cross-border transfers are slow, opaque, and expensive due to the involvement of multiple correspondent banks. Blockchain addresses these limitations by leveraging distributed, immutable ledgers that provide network-wide visibility, reducing processing times and mitigating foreign-exchange settlement risks [152]. Central banks and FinTech companies deploy blockchain-based remittance solutions to lower costs, particularly in developing regions. Peer-to-peer, traceable transfers reduce settlement from days to minutes, eliminating intermediary layers and fees [231][232]. Tokenization and stablecoins enhance currency interoperability, while smart contracts automate FX conversion and settlement [13][231]. Self-sovereign identity and zero-knowledge proof architectures allow near-instant, privacy-preserving compliance. Case studies suggest that such solutions could reduce global remittance costs, which currently exceed 4% on traditional rails [233][234].

6.2.3. Fraud detection and prevention

Blockchain's immutability makes it nearly impossible to manipulate financial data. Institutions leverage shared ledgers to verify transactions, detect anomalies, and prevent identity spoofing [97]. Immutable audit trails focus investigators on suspicious activities rather than compromised funds. Combining blockchain with AI and analytics enables real-time anomaly detection and robust traceability. For instance, federated learning with deep neural networks applied to DeFi

platforms achieves F1 scores above 91% in fraud detection [70]. Explainable AI models, such as Extreme Gradient Boosting (XGBoost) with SHapley Additive exPlanations (SHAP), achieve ~96% accuracy in classifying suspicious Ethereum wallets [235]. Smart-contract–based pipelines further detect and deter market manipulation, while AI-driven behavioral analytics combined with tokenized records strengthen payment system security [60].

6.2.4. Know-your-customer (KYC) and digital identity verification

Blockchain streamlines digital identity verification, enabling clients to reuse verified credentials across institutions while reducing the risk of identity theft [28]. Self-sovereign identity models give users control over their credentials while complying with regulations. Decentralized identity systems enable secure verification by financial institutions, minimizing unauthorized access. Shared, tamper-resistant KYC records reduce duplication and costs, while distributed ledgers improve AML/KYC efficiency and enable real-time supervision [2]. Smart contracts embed KYC/AML checks into cross-border payments, enforcing compliance automatically [75]. Layering self-sovereign identity with zero-knowledge proofs allows proof of compliance without revealing personal data, and biometrics, such as iris recognition, enhance authentication security [60][236][237].

6.2.5. Smart contract–based lending and credit management

Smart contracts automate complex financial agreements, including loans, trade finance, escrow, insurance claims, and interest payments. This automation reduces errors, enhances accuracy, and minimizes the risk of manipulation. On DeFi platforms, lending protocols automatically execute loans and collateral liquidations, ensuring secure credit operations. Smart contracts also support multiparty settlement, escrow, and risk-sharing in cross-border trade, enforcing conditions without intermediaries and reducing costs by up to 75% [13][238]. These frameworks form the foundation for automated credit and lending infrastructure in DeFi ecosystems [2][238].

6.2.6. Secure asset tokenization

Blockchain allows digital representation of tangible and financial assets, enhancing liquidity, enabling fractional ownership, and maintaining transparent records. Tokenization of real estate, stocks, commodities, and fund units ensures cryptographically secured ownership rights [152][233]. Fractional ownership platforms record tamper-proof transaction histories, while tokenized securities improve efficiency, transparency, and fraud resistance in capital markets. These applications support atomic settlements, lower counterparty risk, and facilitate real-time auditing, though legal recognition and regulatory frameworks remain essential [233][238].

6.2.7. Secure supply chain finance

Blockchain enhances supply chain finance by verifying invoices, preventing duplicate financing, and fostering trust among participants [97]. Financial institutions can confirm transactions in real time, linking payments to verifiable trade and shipment records. Digitized bills of lading and invoices on shared ledgers ensure payment release only when contractual conditions are met, reducing operational risks and improving access for smaller suppliers [13][233]. Smart contracts integrated with oracles automate payment upon delivery confirmation, minimizing delays from manual verification [13].

6.2.8. Regulatory compliance and auditing

Blockchain's immutable ledgers provide regulators with tamper-evident audit trails, lowering the risk of misstatements [152]. Automated auditing tools and smart contracts enable continuous compliance checks, reducing operational burden. Permissioned architectures such as Hyperledger Fabric, combined with zero-knowledge proofs, allow regulators to audit complex activities without compromising privacy [239]. Multi-agent compliance systems embedded in smart contracts achieve >98% real-time verification with sub-200 ms latency in DeFi settings [240]. Blockchain thus transforms compliance from ex-post monitoring to continuous, automated "smart auditing" [241][242].

6.2.9. Secure data sharing across financial institutions

Blockchain enables controlled, permissioned data sharing while preserving integrity and confidentiality. Consortium blockchains allow banks and insurers to exchange sensitive information securely for collaborative risk assessment and fraud detection [243][244]. Encrypted off-chain storage combined with smart-contract–driven access policies ensures that only authorized parties can access data, with all activity immutably logged [244]. Decentralization, immutability, and transparency allow auditable, seamless data sharing while reducing reliance on intermediaries [245]. Elliptic-curve cryptography and smart-contract access control improve dataset security, consistency, and reconciliation efficiency [246][247].

6.2.10. Cybersecurity enhancement and data integrity

Blockchain's decentralized design strengthens data integrity and protects sensitive information. Cryptographic hashing and consensus mechanisms make transaction records tamper-resistant [131][243][247]. When combined with traditional

cybersecurity measures, blockchain provides a multi-layered defense against fraud, phishing, and endpoint attacks [131][243]. Integrating blockchain with anomaly-detection models improves compliance prediction (97.7%) and credit risk control in supply-chain finance [247]. AI-based monitoring within blockchain frameworks supports real-time fraud detection with F1 scores above 91%, maintaining low latency and robust data integrity. Applications extend to decentralized identities, smart-contract–enforced policies, and threat intelligence sharing, supporting zero-trust cybersecurity architectures [33][243].

6.2.11. Decentralized insurance and claims processing

Blockchain automates insurance policy execution and claims settlement using smart contracts. Claims are processed based on verified inputs, reducing disputes and fraudulent activity. Parametric insurance triggers automatic payouts when predefined conditions, such as weather events, are confirmed on-chain. Blockchain enables transparent, rule-based insurance, with underwriting, premium collection, and claims executed via smart contracts. DeFi security architectures incorporate reserve treasuries to compensate users automatically after verified exploits [125]. Healthcare-like blockchain insurance systems demonstrate improved fraud mitigation, data integrity, and automation, suggesting broader applicability in financial insurance products [23][243]. Oracle-driven smart contracts release payments upon verification of external events, reducing administrative overhead.

6.2.12. Secure integration with AI systems

Blockchain provides trusted, tamper-resistant data for AI-driven financial analytics, enhancing reliability and security. By guaranteeing data integrity and provenance, it mitigates risks of data poisoning or model manipulation. AI-based fraud detection leverages blockchain-verified data to improve automated decision-making. Hybrid architectures combining federated learning, deep neural networks, and blockchain enable privacy-preserving risk assessments across institutions. These frameworks allow collaborative model training without centralizing raw data while maintaining traceability of AI-generated decisions [70]. In IoT-finance scenarios, decentralized machine learning and tokenization provide auditable, robust pipelines that support accountable AI behavior in sensitive domains [23][33].

6.2.13. DeFi platforms

DeFi leverages blockchain to facilitate lending, borrowing, trading, and asset management without intermediaries, enhancing financial inclusion and transparency [28]. Next-generation DeFi security architectures combine pre-deployment verification, runtime protections, and governance mechanisms [125]. AI-enhanced frameworks integrate federated learning risk engines and deep neural networks for high-precision anomaly detection with low latency [70]. Smart contracts embed regulatory checks and enable auditability, balancing openness, security, and compliance [70][125][240].

6.2.14. Secure interbank communications and consortium networks

Banking consortia employ permissioned blockchains to securely share data among member institutions, enhancing operational efficiency and reducing information asymmetries [152]. Shared ledgers support payments, settlements, and compliance reporting. Smart-contract–based cross-border payment systems implement Payment versus Payment and Real-Time Gross Settlement with automated KYC/AML and CBDC compliance, cutting settlement times from days to minutes and lowering costs [75]. Distributed ledgers synchronize state across institutions, improve interoperability, and enable shared KYC utilities and regulatory nodes. Private Ethereum consortium blockchains, optimized for advanced consensus and smart contracts, have enhanced trading transparency and reduced single points of failure in stock markets [23].

6.3. Advantages of Using Blockchain in Securing Smart Finance

Blockchain technology offers substantial advantages for securing smart finance by addressing longstanding challenges in trust, security, transparency, and operational efficiency. The following highlights the key benefits of blockchain in this context.

6.3.1. Enhanced data integrity and immutability

Blockchain ensures that once financial data is recorded, it cannot be altered or deleted without network consensus, protecting transaction histories against tampering and fraud. In securities trading, for example, immutable ledgers prevent retroactive modifications of trade records, preserving market integrity and investor confidence. Through an append-only, tamper-evident ledger, any attempt to alter recorded data would require network-wide agreement, making ex post manipulation of trades, balances, or audit trails challenging [222][243][248]. In financial microservices and IoT-based finance, this immutability further deters fraud and back-dating, as altering any block necessitates recomputing subsequent blocks a computationally prohibitive task [248][249].

6.3.2. Decentralization and reduced single points of failure

Unlike centralized databases, blockchain distributes data across multiple nodes, enhancing system resilience and mitigating risks from cyberattacks or infrastructure failures. Decentralized ledgers in smart banking platforms continue to operate even if some nodes go offline or are compromised. By replicating records across nodes, blockchain eliminates the central points of failure common in traditional financial infrastructures and microservice back-ends [243][248]. DeFi platforms and cross-border payment pilots demonstrate that collective validation significantly reduces the risk of a compromised intermediary undermining the system [2][222][250].

6.3.3. Improved transparency and auditability

Blockchain provides a transparent, traceable record of all transactions, enabling near real-time auditing by regulators and financial institutions without relying on reconciled internal records. In AML systems, blockchain allows efficient tracing of fund flows and rapid detection of suspicious activity. Because validated transactions are recorded in a shared, verifiable ledger, auditors and participants can independently inspect transaction histories in near real time [222][242][243][250]. This transparency supports continuous auditing, real-time anomaly detection, and automated reconstruction of transactional flows for KYC/AML, ESG, and green finance reporting, reducing hidden liabilities and mitigating "greenwashing" risks [242][250].

6.3.4. Strong cryptographic security

Blockchain secures financial data and user identities through cryptographic techniques, including hashing and public–private key encryption. Digital payment systems rely on cryptographic signatures to ensure that only authorized users can initiate transactions, mitigating identity theft and unauthorized transfers. Combined with consensus protocols such as Proof of Work or Proof of Stake, blockchain authenticates participants, signs transactions, and prevents double-spending [243]. The encryption of stored and transmitted data, including cloud-hosted records and IoT sensor streams, ensures tamper-proof, confidential transaction logs that resist cyberattacks [243][249].

6.3.5. Automated enforcement through smart contracts

Smart contracts execute financial agreements automatically when predefined conditions are met, removing the need for manual intervention. Decentralized lending platforms, for example, issue loans, calculate interest, and enforce repayment schedules, reducing operational risk and contractual disputes. These self-executing programs encode business logic, such as collateral checks, portfolio rebalancing, or loan disbursement, directly on the ledger [2][37][222][242]. In supply-chain finance, smart-contract–based audit systems automatically verify transactions, enhancing accuracy while saving time and cost. In intelligent financial management systems leveraging federated learning, smart contracts also govern access control, model training workflows, and policy compliance without human intervention [37][249].

6.3.6. Faster and more secure transactions

Blockchain enables near-real-time transaction validation and settlement without intermediaries. Cross-border payments can be settled in minutes rather than days, benefiting both institutions and end users. Case studies demonstrate that blockchain accelerates settlement while maintaining cryptographic integrity and decentralized validation [2][250]. DeFi platforms and decentralized exchanges leverage on-chain settlement and, in some cases, high-throughput public chains or Layer-2 networks to support high-frequency, near-real-time trading without central clearinghouses [2][222][251].

6.3.7. Cost reduction and operational efficiency

By removing intermediaries and automating processes, blockchain reduces transaction and administrative costs. Insurance claim processing, for example, benefits from automated validation through shared ledgers and smart contracts, reducing paperwork and verification expenses. Eliminating custodians, correspondent banks, and manual auditors, combined with automated workflows, lowers reconciliation overhead, back-office processing, and dispute-resolution costs [2][222][242][249]. Pilot projects report transaction cost reductions of up to 70%, alongside shorter audit times and reduced operational friction in cross-border payments, supply-chain finance, and institutional financial management [2][249].

6.3.8. Secure data sharing and interoperability

Blockchain enables secure, permissioned data sharing among multiple financial entities while maintaining integrity and access control. Banks and fintech companies can collaborate on fraud detection without exposing sensitive customer data. Consortium- or public-permissioned blockchains provide a consistent shared view of data, supporting joint risk modeling, ESG tracking, and supply-chain credit assessment while protecting proprietary information [70][243][248][250]. Federated learning anchored on blockchain allows multi-bank fraud-detection models to exchange updates rather than raw data while logging activity immutably, preserving both privacy and integrity. Interoperability layers and hybrid architectures also enable gradual integration with legacy core-banking systems [242][243].

6.3.9. Improved fraud detection and prevention

Blockchain's transparency and traceability simplify the detection of fraudulent activity. Unusual patterns in credit card or digital wallet transactions can be quickly flagged, limiting financial losses. Immutable records prevent retroactive manipulation, while AI and machine learning models trained on these trusted datasets enhance anomaly-detection accuracy [70][242][243][252]. Platforms such as DeFiSentinel integrate federated learning, deep neural networks, and smart contracts to enable high-precision, real-time fraud detection in decentralized financial systems [70]. Combined with advanced analytics, blockchain supports continuous monitoring, predictive anomaly detection, and automated alerts for suspicious activity in KYC/AML and transactional flows [242][252].

6.3.10. Trustless collaboration and financial inclusion

Blockchain facilitates secure, trustless interactions among parties without prior relationships, expanding access to financial services. Peer-to-peer payments and microfinance platforms allow users to transact safely without traditional banking infrastructure, promoting financial inclusion in underbanked regions. DeFi and blockchain-based green finance initiatives embed collaboration rules directly into protocols, enabling transparent interactions without the need for bilateral institutional trust [2][222][250], which democratizes access to lending, trading, and sustainable investment products, particularly for small investors and underserved populations, while enabling transparent tracking of outcomes such as carbon credits and ESG metrics [2][250].

Together, these features demonstrate how blockchain strengthens smart finance systems by integrating decentralization, cryptographic security, transparency, and automation. Applications across payments, lending, insurance, regulatory compliance, and green finance illustrate blockchain's capacity to provide secure, efficient, and trustworthy foundations for digital financial ecosystems.

7. INTEGRATING AI AND BLOCKCHAIN FOR SMART FINANCE SECURITY

7.1. Motivation for Integration

The rapid digital transformation of the financial sector has given rise to smart finance systems that rely on automated decision-making, real-time data analytics, and decentralized digital infrastructures. These systems enhance efficiency, scalability, and financial inclusion but also introduce significant challenges in security, privacy, and trust. Conventional security mechanisms, which are largely centralized and rule-based, are increasingly inadequate against sophisticated cyber threats, data manipulation, insider attacks, and systemic vulnerabilities. Integrating AI and blockchain technologies presents a promising solution by creating resilient, transparent, and intelligent smart finance ecosystems.

Smart finance platforms face continuously evolving cyber threats, including fraud, identity theft, transaction manipulation, and adversarial behaviors. These threats demand security mechanisms that are both intelligent and trustworthy. AI techniques, particularly machine learning and deep learning, enable proactive threat detection, fraud identification, and risk prediction by uncovering complex patterns, anomalies, and behavioral deviations in large-scale financial data. However, AI systems alone remain vulnerable to data poisoning, model tampering, lack of transparency, and limited auditability.

Blockchain complements AI by providing immutable data storage, cryptographic integrity, distributed consensus, and verifiable transaction histories, ensuring that AI-driven security decisions rely on tamper-resistant, trustworthy data. Recording AI-generated alerts, risk scores, model updates, and automated decisions on-chain enhances trust and transparency in decentralized and cross-border financial environments. It also supports accountability, explainability, and regulatory compliance. Furthermore, blockchain-based architectures enable secure, privacy-preserving data sharing through cryptographic controls, smart contracts, and decentralized access management, which allows AI models to operate on verified data without exposing sensitive financial or personal information.

The AI–blockchain integration also strengthens fraud detection and risk management by ensuring transaction provenance, non-repudiation, and end-to-end traceability, which prevents post hoc data manipulation that could compromise analytical outcomes. In automated smart finance ecosystems, AI-enhanced smart contracts implement adaptive, context-aware security policies that dynamically respond to emerging threats and abnormal behaviors, overcoming the limitations of static rule-based systems.

Additionally, immutable blockchain logs address regulatory and auditability challenges by enabling transparent tracking of data usage, model behavior, and security actions, which supports forensic analysis and continuous compliance monitoring. Blockchain's decentralized architecture, reinforced by AI-driven monitoring and adaptive defense mechanisms, further improves system resilience by mitigating single points of failure, predicting cascading risks, and enabling real-time responses to security incidents.

Collectively, integrating AI and blockchain leverages their complementary strengths AI's intelligence and adaptability, and blockchain's trust, transparency, and data integrity. This combination forms a robust, future-ready security framework for next-generation smart finance systems.

7.2. Proposed Framework Integrating AI and Blockchain for Smart Finance Security

To address the increasing complexity of cyber threats, escalating data privacy concerns, and persistent trust deficiencies in smart finance ecosystems, this study proposes a unified framework that tightly integrates AI and blockchain technology. The framework combines AI-driven analytics for real-time, adaptive threat detection with blockchain-based mechanisms for decentralized trust management, data integrity, transparency, and non-repudiation, all within a single scalable architecture. In addition, it supports secure automation, preserves data privacy, and enables collaborative financial intelligence. By design, the framework also maintains high scalability and aligns with regulatory compliance requirements, making it suitable for high-throughput financial environments without compromising security or trust.

Four (4) core objectives guide the proposed framework:

- Enabling real-time and adaptive security intelligence through AI-driven analytics,
- Ensuring data integrity, transparency, and non-repudiation via blockchain,
- Preserving privacy while supporting collaborative financial intelligence, and
- Maintaining scalability and regulatory compliance in high-throughput financial environments.

The framework is built on a modular, layered architecture in which interconnected functional components operate in a coordinated and secure manner. Each module addresses a distinct aspect of data handling, intelligence generation, trust establishment, and governance, collectively enabling robust and adaptive financial security.

7.2.1. Secure data ingestion and verification module

The framework ingests financial data from diverse, heterogeneous sources, including transaction systems, digital wallets, payment gateways, and user interaction logs. To ensure authenticity and provenance, each data item is cryptographically signed and timestamped at the source. Before entering the analytics pipeline, lightweight verification mechanisms validate data integrity, preventing the introduction of forged, tampered, or manipulated records at an early stage. This proactive verification establishes a trusted foundation for all downstream analytics.

7.2.2. AI-driven security intelligence module

As the analytical core, this module employs advanced machine learning and deep learning techniques to detect fraud, identify anomalous behavior, assess credit and transaction risks, and anticipate emerging threats. Temporal, behavioral, and graph-based models capture both short-term irregularities and long-term attack patterns. Operating in continuous learning mode, the models adapt to evolving financial fraud strategies while maintaining resilience against adversarial manipulation, enabling robust, dynamic threat detection.

7.2.3. Blockchain-based trust and integrity module

The blockchain layer provides decentralized trust and immutable record-keeping across the system. Rather than storing raw financial data, the framework records cryptographic hashes of transactions, AI model outputs, and security decisions on the ledger. This approach ensures tamper resistance while minimizing storage and performance overhead. By employing a permissioned blockchain, the system achieves low latency, controlled access, and regulatory alignment, supporting trusted participation by financial institutions and oversight authorities.

7.2.4. Smart contract–enabled security automation module

Smart contracts automate security enforcement by encoding predefined policies, compliance requirements, and response mechanisms. They receive AI-generated risk scores and alerts as inputs and autonomously execute actions such as suspending transactions, enforcing multi-factor authentication, or escalating cases to human analysts. This integration enables adaptive, context-aware security responses, reducing reliance on static, rule-based controls and enhancing operational efficiency.

7.2.5. Privacy-preserving collaboration module

To support secure cross-institutional collaboration without exposing sensitive data, the framework incorporates privacy-preserving mechanisms. AI models can be trained collaboratively through decentralized or federated learning, while the blockchain coordinates model updates, verifies participant contributions, and enforces incentives and accountability. By keeping sensitive data local, the framework mitigates leakage risks and ensures compliance with data protection regulations, enabling secure and trustworthy intelligence sharing.

7.2.6. Governance, audit, and compliance module

The governance module enforces transparency, accountability, and regulatory compliance across the framework. All security-relevant events, including model updates, decision outcomes, and smart contract executions, are immutably recorded on the blockchain. This design allows auditors and regulators to verify system behavior without accessing confidential data. Additionally, explainability mechanisms link AI-driven decisions to verifiable on-chain records, addressing concerns about black-box models in financial security systems and strengthening trust in automated decision-

making. Figure 15 presents the modular, layered architecture for the proposed framework integrating AI and blockchain for smart finance security.

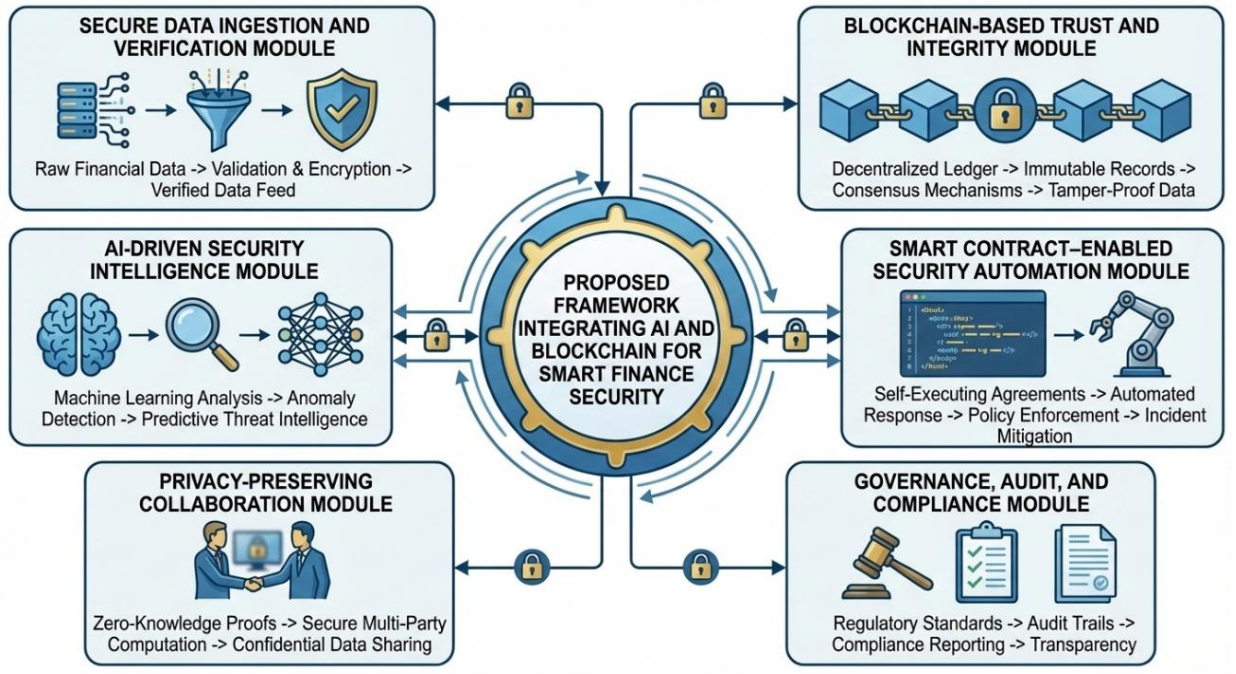

Fig. 15. Presents the modular, layered architecture for the proposed framework, integrating AI and blockchain for smart finance security.

7.3. Operational Workflow of the Proposed Framework Integrating AI and Blockchain for Smart Finance Security

The operational workflow of the proposed framework defines how financial data, intelligent analytics, and decentralized trust mechanisms interact to deliver continuous, adaptive, and verifiable security in smart finance systems. The workflow is designed to support real-time threat detection, automated mitigation, data integrity assurance, and regulatory transparency throughout the entire security lifecycle. It is organized into a sequence of interconnected phases that collectively enable end-to-end security enforcement.

7.3.1. Secure data collection and authentication

The workflow begins by acquiring financial data from diverse, heterogeneous sources, including transaction processing systems, digital wallets, payment gateways, user behavior logs, and market data feeds. At the point of origin, each data item is cryptographically signed and timestamped to ensure authenticity and traceable provenance. Identity verification mechanisms authenticate data sources, thereby preventing unauthorized or malicious entities from injecting fraudulent or manipulated records into the system.

7.3.2. Data preprocessing and integrity validation

After collection, the data undergo systematic preprocessing, including normalization, noise reduction, feature extraction, and format harmonization. In parallel, integrity validation mechanisms verify that the data have not been altered during transmission. Only data that successfully passes these validation and sanitization procedures is forwarded to the AI analytics layer, thereby minimizing the risk of data poisoning and enhancing the reliability of downstream models.

7.3.3. AI-based security analysis and risk assessment

The validated data are analyzed in real time using AI-driven security models. These models leverage machine learning, deep learning, and graph-based techniques to detect anomalous transactions, identify fraudulent behaviors, and compute dynamic risk scores. Through continuous learning, the models adapt to emerging threats and evolving attack patterns. Each security decision is accompanied by confidence measures and explanatory metadata to support interpretability and informed decision-making.

7.3.4. Generation of security events and metadata

Based on the AI analysis results, the framework generates structured security events that indicate potential threats, policy violations, or abnormal behavior. Each event is enriched with detailed metadata, including transaction identifiers, timestamps, risk scores, and references to the specific model version used. This structured representation enables efficient traceability, verification, and downstream processing.

7.3.5. Blockchain anchoring and verification

To preserve confidentiality, the framework avoids storing sensitive financial data directly on the blockchain. Instead, it computes cryptographic hashes of security events, AI outputs, and decision metadata and anchors these hashes on a permissioned blockchain. Consensus mechanisms validate the recorded entries across participating nodes, resulting in a shared, immutable, and tamper-resistant security ledger. This anchoring process ensures non-repudiation and prevents post hoc modification of AI-generated decisions.

7.3.6. Smart contract–driven policy evaluation

Smart contracts continuously monitor the blockchain for newly recorded security events. Upon detecting an event, the contracts evaluate the associated risk scores and metadata against predefined security policies and compliance requirements. These policies may include transaction risk thresholds, user trust levels, regulatory constraints, and contextual conditions. Deterministic smart contract execution ensures consistent, transparent, and auditable policy enforcement.

7.3.7. Automated mitigation and response execution

When policy conditions are satisfied or violated, smart contracts automatically trigger appropriate mitigation actions. These actions may involve blocking transactions, enforcing step-up authentication, temporarily suspending accounts, or escalating alerts to human security analysts. By automating response execution, the framework significantly reduces response time and limits potential financial losses from malicious activity.

7.3.8. Logging, auditing, and explainability support

All security-related activities, including AI assessments, smart contract evaluations, and mitigation outcomes, are immutably logged on the blockchain. This comprehensive audit trail supports post-incident analysis, regulatory compliance verification, and forensic investigations. Explainability mechanisms explicitly link AI decisions to verifiable on-chain records, thereby strengthening transparency, accountability, and trust in automated financial security operations.

7.3.9. Feedback and continuous learning loop

The workflow incorporates a closed feedback loop in which mitigation outcomes and confirmed security incidents are fed back into the AI models. This feedback enables continuous model refinement and performance optimization over time. Blockchain-verified logs ensure the trustworthiness of training data and model updates, thereby reducing the risk of compromised or corrupted learning processes.

7.3.10. Cross-institutional collaboration and governance

In multi-stakeholder financial ecosystems, the framework facilitates secure cross-institutional collaboration. Blockchain technology coordinates the sharing of security intelligence and model updates, while fine-grained access control mechanisms enforce governance and data-sharing policies. Regulators and auditors can access relevant on-chain records without exposing sensitive financial data, enabling adequate compliance verification and systemic oversight. Figure 16 presents the operational workflow of the proposed framework integrating AI and blockchain for smart finance security.

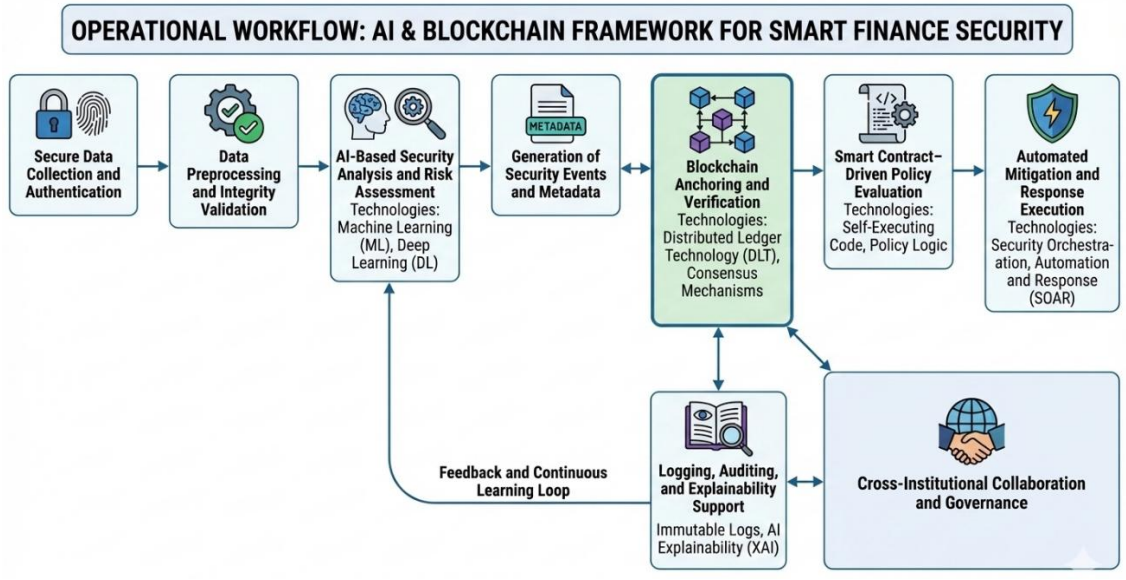

Figure 16. Presents the operational workflow of the proposed framework that integrates AI and blockchain for smart finance security.

In summary, the proposed operational workflow tightly integrates AI-driven intelligence with blockchain-based trust to establish a closed-loop security process. Financial data are securely collected, intelligently analyzed, immutably verified, and automatically acted upon, resulting in a resilient, transparent, and adaptive security framework for smart finance systems.

7.4. Benefits of Integrating AI and Blockchain in Smart Finance Security

The convergence of AI and blockchain technologies establishes a transformative security paradigm for smart finance systems. By combining intelligent data analytics with decentralized trust mechanisms, this integration addresses long-standing challenges related to fraud prevention, data privacy, transparency, and system resilience. Together, AI and blockchain enable adaptive, intelligent, and inherently trustworthy security frameworks. The following subsections outline the key strategic and technical benefits of this integration.

7.4.1. Intelligent and proactive threat detection

AI enables real-time analysis of large-scale financial data to detect anomalies, fraudulent activities, and emerging cyber threats. Unlike traditional rule-based security mechanisms, AI models continuously learn from new data and adapt to evolving attack patterns. When integrated with blockchain, AI-driven threat detection benefits from access to immutable and verifiable data sources. This integration improves detection accuracy, reduces false positives, and strengthens confidence in security assessments.

7.4.2. Tamper-proof data integrity and non-repudiation

Blockchain provides a secure and reliable foundation for recording financial transactions, security events, and AI-generated decisions. Once data are committed to the blockchain, they cannot be altered or removed without network consensus. This immutability ensures data integrity and non-repudiation, which are essential for forensic investigations, dispute resolution, and regulatory compliance in smart finance environments.

7.4.3. Enhanced trust and transparency

Trust is a fundamental requirement in financial systems involving multiple stakeholders. Blockchain establishes a shared, verifiable source of truth, while AI-driven security actions can be transparently recorded and audited on-chain. This traceability reduces information asymmetry, enhances accountability, and strengthens trust among users, financial institutions, and regulatory authorities.

7.4.4. Automated and adaptive security enforcement

Integrating AI with blockchain-based smart contracts enables automated and adaptive enforcement of security policies. AI-generated risk assessments can dynamically guide smart contract execution, allowing systems to respond immediately to suspicious or malicious activities. This automation minimizes reliance on manual intervention, reduces response time, and limits the potential impact of financial attacks.

7.4.5. Privacy-preserving data analytics

Smart finance systems handle highly sensitive financial and personal data, making privacy protection a critical concern. AI–blockchain integration supports privacy-preserving analytics by combining decentralized data management with cryptographic safeguards. Blockchain-based access control and secure coordination mechanisms enable AI models to analyze verified data without exposing raw information, thereby supporting compliance with data protection and privacy regulations.

7.4.6. Robust fraud detection and transaction traceability

AI excels at identifying complex and coordinated fraud schemes by analyzing transactional, behavioral, and relational patterns. Blockchain complements these capabilities by maintaining complete, transparent, and immutable transaction records. Together, they provide end-to-end traceability of financial activities, enabling accurate identification of fraud sources and reliable reconstruction of attack timelines.

7.4.7. Improved system resilience and fault tolerance

Centralized financial infrastructures are vulnerable to single points of failure and insider threats. Blockchain's decentralized architecture distributes trust and control across multiple nodes, significantly enhancing fault tolerance. When combined with AI-driven monitoring and predictive analytics, the system can anticipate failures, detect abnormal conditions, and maintain secure operations even under adverse or attack-prone scenarios.

7.4.8. Secure and transparent cross-institutional collaboration

Modern smart finance ecosystems often involve multiple financial institutions and service providers. AI–blockchain integration enables secure sharing of security intelligence and model updates without centralized data aggregation.

Blockchain enforces governance, traceability, and accountability, while AI leverages shared insights to strengthen collective defenses against coordinated and systemic threats.

7.4.9. Regulatory compliance and auditability

Financial regulations increasingly emphasize transparency, accountability, and traceability in security operations. Blockchain inherently supports these requirements by providing immutable audit trails for transactions, security events, and AI model updates. Linking AI-generated decisions to on-chain records enhances explainability and facilitates continuous regulatory monitoring and compliance verification.

7.4.10. Scalability and future-proof security architecture

The integrated AI–blockchain framework supports scalable and modular security architectures suited to evolving smart finance systems. AI models can be updated or replaced as threat landscapes change, while blockchain preserves long-term data integrity and trust. This future-proof design enables financial systems to adapt to technological advancements, regulatory changes, and emerging cyber risks.

In conclusion, integrating AI and blockchain delivers a comprehensive, intelligent, and resilient security framework for smart finance systems. By uniting adaptive analytics with decentralized trust mechanisms, this approach enables secure and reliable operation in increasingly complex, interconnected, and high-risk digital financial environments.

7.5. Case Studies and Real-World Implementations

Several real-world deployments demonstrate the practical applicability of the proposed AI–blockchain–integrated framework for strengthening security in smart finance systems. These use cases span decentralized finance, enterprise banking, governance, cybersecurity, and sustainability, illustrating how AI-driven intelligence and blockchain-based enforcement jointly enhance trust, resilience, and transparency.

7.5.1. DeFi intelligent risk control

Zhang [253] proposes an intelligent risk-control framework for DeFi that tightly integrates AI analytics with blockchain-based enforcement. AI models continuously analyze on-chain price series, liquidity movements, and user behavioral patterns to detect market manipulation, flash crashes, and abnormal arbitrage activity. Blockchain complements these analytics by immutably recording trades and protocol states, while smart contracts enforce predefined risk rules without relying on centralized intermediaries. From an implementation perspective, the framework processes heterogeneous on-chain data, including decentralized exchange swaps, order-book states, oracle price feeds, and liquidation events [253]. Supervised learning and anomaly-detection models achieve approximately 94% detection accuracy, with a false-alarm rate of 2.1% and an average latency of about 180 ms, indicating suitability for real-time DeFi environments. Risk thresholds, such as position limits and dynamically adjusted collateral ratios, are encoded in smart contracts. When AI models identify high-risk addresses, these contracts automatically trigger margin calls or throttle transactions, enabling transparent and deterministic enforcement of risk policies [141][253][254].

7.5.2. Banking fraud-risk assessment in enterprise deployments

In traditional banking environments, Gujrati and Uygun [255] examine the integration of AI-based fraud detection with blockchain ledgers through a JPMorgan-style enterprise deployment. Their framework combines Random Forest, support vector machine, and regression models trained on historical card, wire-transfer, and online-banking transactions to identify anomalous activities in real time. This approach improves both the precision and responsiveness of fraud-risk assessment in high-volume banking systems. Blockchain plays a complementary role by maintaining a decentralized, append-only ledger that records transactions, KYC data, machine-learning outputs, and investigative actions [255][256]. Flagged transactions are written to a permissioned blockchain accessible to investigators, ensuring data integrity and traceability throughout the investigation lifecycle. Once cases are resolved, labeled outcomes are fed back into the AI pipeline for continuous retraining. This closed-loop workflow reduces false positives, shortens investigation cycles, and strengthens regulatory reporting [1][255].

7.5.3. Enterprise financial risk prevention and control

Extending AI–blockchain integration to enterprise governance, Sun et al. [257] describe a risk-control system designed to address data trustworthiness, real-time risk warnings, traceability of responsibility, and decentralization. The system aggregates internal accounting records, invoices, supply-chain data, and external market indicators to provide a holistic view of enterprise financial risk. AI-based early-warning models analyze these datasets to detect abnormal cash flow patterns and financial statement irregularities. Blockchain underpins the framework through a consortium chain that logs critical transactions, approvals, and accountability records. Smart contracts encode approval workflows and responsibility assignments, ensuring transparency and tamper resistance. As a result, AI-generated alerts can automatically trigger on-chain actions, such as freezing high-risk transactions, while immutable records support post hoc audits and accountability [257][258].

7.5.4. AI-powered smart contracts and decentralized autonomous organization governance

Pasupuleti [141] outlines the evolution of AI-enhanced smart contracts that support self-optimization and dynamic adaptation to fraud, governance changes, and regulatory requirements across DeFi platforms, decentralized autonomous organizations, and NFT markets. Reinforcement learning optimizes gas fees and contract parameters, while machine-learning models detect fraudulent behavior. NLP techniques further enable translating human-readable contractual clauses into executable on-chain logic. Blockchain provides the execution substrate by encoding core contract logic, governance voting mechanisms, and treasury operations directly on-chain. Privacy and long-term security are enhanced through zero-knowledge proofs and quantum-resistant cryptography [141]. In practice, off-chain AI agents propose parameter updates or dispute-resolution outcomes, which on-chain contracts execute only after governance conditions are met. This hybrid architecture balances adaptability with decentralized oversight [141][259].

7.5.5. Cybersecurity for smart finance infrastructure

Addressing cybersecurity threats in smart finance, Chowdhury [63] presents a multi-layer AI–blockchain security architecture evaluated on Hyperledger Fabric. The framework employs AI models, including Random Forest, XGBoost, Long Short-Term Memory networks, and autoencoders, to detect malware, advanced persistent threats, and insider attacks. Complementary work by Bourian et al. [195] introduces a Generative Adversarial Network-assisted deep learning approach that achieves 97.6% accuracy in malware detection during smart contract execution. These frameworks analyze behavioral patterns across network traffic, APIs, and smart-contract execution traces. Blockchain records immutable, time-stamped security logs and enforces smart-contract-based incident-response policies, such as isolating compromised nodes [63]. When applied to financial infrastructures and DeFi platforms, these mechanisms protect payment gateways, trading engines, and custody contracts, thereby strengthening end-to-end financial security [195][260].

7.5.6. Blockchain–AI-enhanced CAPM risk management

Weng [258] examines how blockchain and AI enhance the Capital Asset Pricing Model to improve market assessment and risk management. Blockchain ensures the integrity of price, trade, and ownership data by storing them on-chain, mitigating data-quality issues that undermine CAPM parameter estimation. AI models further augment CAPM by refining beta estimates, detecting regime shifts, and forecasting expected returns under non-linear market conditions [258][261]. In smart finance applications, these capabilities are integrated into risk dashboards where CAPM metrics are continuously recomputed using blockchain-verified data. AI models flag assets whose realized risk–return profiles deviate from theoretical expectations, enabling more proactive portfolio risk management [258].

7.5.7. Payments, smart lending, and retail DeFi

A growing body of research highlights the role of AI–blockchain integration in payment systems, peer-to-peer lending, and retail DeFi platforms to enhance security and personalization [1][261][262]. AI models support credit scoring, customer segmentation, and transaction-risk assessment across payment and lending workflows. Blockchain facilitates tokenized payments and loan agreements through smart contracts that automatically enforce repayment schedules, collateral requirements, and penalty clauses [261][262]. When AI systems detect anomalous repayment behavior or suspicious transactions, smart contracts can initiate actions such as collateral liquidation or enhanced KYC checks. This integration embeds adaptive security directly into financial instruments, strengthening resilience across retail DeFi ecosystems [253][262].

7.5.8. IoT-linked financial security and digital perimeters

Cekerevac et al. [256] explore the integration of AI, blockchain, and IoT to secure financial infrastructures through digital perimeters. IoT devices deployed in ATMs, point-of-sale terminals, and bank branches stream telemetry data, including access events, environmental conditions, and tamper alerts. Related work similarly emphasizes AI–blockchain architectures for securing cyber-physical systems [263]. AI models analyze these data streams in real time to detect device compromise or anomalous usage patterns [256]. Blockchain maintains integrity-protected logs of device states and cryptographic attestations, while smart contracts enforce automated responses, such as disabling compromised devices or blocking associated transactions. Together, these mechanisms strengthen the security of physical–digital interfaces in smart finance environments [260].

7.5.9. Smart legal contracts, compliance, and dispute resolution

Shelake [264] reviews the application of AI- and blockchain-based smart contracts in financial and legal contexts, focusing on compliance enforcement and dispute resolution. AI techniques, particularly NLP, support clause extraction, compliance checking, and risk scoring, while predictive models estimate the likelihood of disputes or default [141][264]. Once deployed, blockchain-based smart contracts automatically execute payment, collateral, and penalty clauses while recording immutable evidence of parties' actions and timestamps. In practice, AI systems flag high-risk clauses before deployment,

and subsequent non-compliance is logged on-chain. These mechanisms can automatically trigger penalties or arbitration workflows, improving enforcement efficiency and legal certainty [259][264].

7.5.10. ESG-aligned smart finance

Mandsaur and Jain [1] highlight the role of AI–blockchain integration in enabling ESG-aligned smart finance. Blockchain enhances transparency by recording green-bond cash flows, carbon-credit transactions, and ESG-linked loan agreements, thereby supporting verifiable sustainability reporting [265]. AI models complement these capabilities by computing ESG scores, detecting greenwashing patterns, and optimizing portfolios under ESG constraints [257]. Smart contracts further operationalize ESG objectives by automatically adjusting interest rates or issuing incentives when on-chain ESG key performance indicators meet predefined thresholds [258]. Collectively, these mechanisms enable more transparent, accountable, and incentive-compatible approaches to sustainable finance.

7.6. Comparative Analysis of Existing Solutions

Table I contrasts representative existing solutions with a generic "proposed framework" integrating AI and blockchain for smart finance security.

TABLE I. COMPARISON OF AI–BLOCKCHAIN SECURITY SOLUTIONS VS. TARGET SMART-FINANCE NEEDS.

S/No	Existing AI–blockchain solution	Domain & main idea	Key technical features/performance	Gap vs. a comprehensive proposed smart-finance security framework	Reference
1	Blockchain and AI intelligent risk-control model for DeFi	DeFi market-risk and manipulation detection.	AI models analyze both on-chain and off-chain data, while the blockchain ledger records events transparently and immutably. This integration achieves 94.1% detection accuracy with only 2.1% false alarms. The system sustains a low latency of 180 ms even under volatile conditions. By combining real-time AI analytics with tamper-proof records, it delivers robust and reliable monitoring.	The framework delivers robust DeFi risk analytics that effectively address key vulnerabilities in the decentralized finance ecosystem. Yet it provides limited support for cross-platform compliance, creating gaps in regulatory alignment. Identity management and holistic governance remain underdeveloped, restricting comprehensive oversight. Addressing these gaps is crucial to achieving a fully integrated smart finance framework.	[171]
2	AI-powered automated smart contracts for decentralized governance	Decentralized autonomous organizations, DeFi, legal/regulatory automation.	Machine Learning and Reinforcement Learning adapt contract logic, detect fraud, and optimize fees in real time, while AI-driven systems ensure compliance and resolve disputes efficiently. Privacy is preserved through Zero-Knowledge Proofs, reinforced by quantum-resistant cryptography that secures sensitive data. By integrating these technologies, decentralized financial operations achieve a seamless	The governance automation is conceptually robust but remains disconnected mainly from practical applications. It lacks integration with end-to-end institutional finance workflows, KYC/AML pipelines, and standardized risk dashboards, limiting its operational impact. Bridging these gaps is essential to translating conceptual frameworks into actionable, compliant financial processes.	[141]

			balance of security, efficiency, and trust.		
3	Hybrid blockchain-integrated AI security framework	General cyber-systems include finance, healthcare, and IoT.	A decentralized blockchain data layer secures tamper-proof records, while machine-learning–based anomaly detection identifies threats in real time. Smart contracts enforce security policies automatically, enabling rapid responses and achieving 98.5% attack detection accuracy. By uniting automated threat response with blockchain integrity, the system ensures both proactive defense and reliable accountability.	While the system delivers robust generic security, it does not address the domain-specific requirements of financial instruments, transaction semantics, or regulatory reporting, leaving compliance, transaction integrity, and risk management in smart finance ecosystems unaddressed.	[266]
4	Next-generation AI–blockchain cybersecurity paradigm	Enterprise/critical-infrastructure cybersecurity, including financial services.	The multi-layer architecture combines blockchain logging with AI models Random Forest, XGBoost, Long Short-Term Memory, and autoencoders for threat detection, while consensus mechanisms enable decentralized governance. This integration reduces false positives and enhances resilience compared with AI-only or blockchain-only approaches. Immutable blockchain records ensure accountability, and AI allows adaptive threat detection, delivering a robust, reliable security framework.	The study focuses on infrastructure-level cyber threats, highlighting system vulnerabilities and operational risks. It places less emphasis on financial risk models, pricing, or consumer protection logic across products. By concentrating on technical and structural dimensions, it reveals critical dependencies in resilient infrastructure. This perspective clarifies the interaction of cyber threats with operational frameworks, informing targeted mitigation strategies.	[63]
5	AI-enhanced DeFiSentinel architecture	DeFi fraud and risk management	Federated learning was employed to produce privacy-preserving risk scores, achieving an MSE of 0.021 and an R^2 of 0.96. Complementing this, a deep neural network effectively detected fraud, reaching 92.4% precision and 91.1% recall. Blockchain-based anomaly detection leverages	A broader smart finance framework extends beyond DeFi by integrating CeFi data, enabling cross-chain interoperability, and leveraging explainable AI to enhance decision-making. It incorporates supervisory interfaces to support regulatory oversight and risk management. Together,	[70]

			cryptographic smart contracts to ensure secure, transparent operations. The combined framework maintained an average latency of approximately 3.7 seconds, demonstrating both efficiency and reliability.	these elements allow seamless interaction across decentralized and centralized financial systems. This integrated approach improves transparency, operational efficiency, and the interpretability of AI-driven financial processes.	
6	AI-based blockchain transaction-analytics (THC)	Blockchain fraud/transaction analysis (primarily financial)	The hybrid support vector machine–k-nearest neighbors–random forest (THC) classifier applied to blockchain transaction features achieved over 99% fraud detection efficacy. By leveraging the complementary strengths of support vector machines, k-nearest neighbors, and random forests, THC significantly outperforms baseline machine learning models. These results highlight the effectiveness of hybrid classifiers for robust and reliable blockchain security.	The model provides robust threat detection but lacks integrated key management, incident response, and cross-institutional compliance orchestration. This gap limits coordinated security governance. Linking detection with structured key and regulatory workflows would enable consistent, auditable, institution-wide operations.	[182]
7	Innovative Ethereum banking framework	Retail/wholesale banking operations	Smart contracts facilitate deposits, withdrawals, and transfers on Ethereum, seamlessly integrating with MetaMask and custom wallets. Transactions execute near real time, boosting transparency and efficiency. The system delivers competitive latency and throughput for high-performance decentralized operations. Overall, it streamlines blockchain interactions while ensuring secure, auditable transaction flows.	It improves system integrity and efficiency but lacks embedded AI risk analytics, adaptive limits, and fraud scoring. Without these, it cannot provide the predictive threat detection of an AI–blockchain security framework. Consequently, it ensures baseline protection but falls short of proactive, AI-driven mitigation.	[25]
8	ADTCN and DB-BOA smart-contract security for consortium stock trading	Private Ethereum-based stock-market infrastructure	The Adaptive Deep Temporal Context Network secures contract logic by modeling temporal dependencies in	The framework ensures strong blockchain-level resilience within a consortium but pays limited attention to learning	[23]

			blockchain operations. The Dynamic Butterfly Billiards Optimization Algorithm optimizes leader selection and critical parameters for robust performance. Combined, these approaches outperform conventional methods, delivering enhanced security and operational efficiency.	from global financial data, cross-jurisdictional regulations, or user-centric anomaly alerts, constraining both broad insight and individualized threat detection.	
9	Generative adversarial network-based AI and blockchain for payment-fraud security	Digital payment processes	A decentralized ledger ensures transparent, immutable records and maintains transaction integrity. Generative adversarial network-based anomaly detection detects fraud in real time, achieving higher accuracy and lower false-positive rates than rule-based systems. This integrated approach enhances both the reliability and responsiveness of fraud detection.	Current frameworks primarily target card and payment rails, but a comprehensive system would integrate lending, trading, and custody functions. This unification strengthens oversight across financial operations and risk domains. Standardized reporting enhances transparency, consistency, and regulatory compliance. Embedding explainable models ensures decision-making remains interpretable and auditable across the integrated framework.	[267]
10	AICyber-Chain–style real-time AI–blockchain cybersecurity framework	General real-time cyber-defence with financial relevance	Convolutional neural network-based anomaly detection is integrated with a permissioned Ethereum blockchain, using smart contracts for immutable logging and automated validation of AI alerts, which ensures accurate detection while providing transparent, tamper-proof audit trails. Compared with traditional systems, the framework significantly enhances both accountability and verifiability of AI decisions.	The system ensures strong audit trails and explainable AI alerts, enhancing transparency. Yet, it is not yet tailored for financial risk key performance indicators, portfolio exposures, or multi-asset orchestration. These gaps underscore the need for further specialization in comprehensive risk management.	[268]

8. OPEN RESEARCH CHALLENGES

Although integrating AI and blockchain offers substantial benefits for smart finance security, several fundamental research challenges remain unresolved. These challenges span technical, operational, regulatory, and governance dimensions.

8.1. Scalability and performance bottlenecks

Scalability remains a critical limitation in AI–blockchain-enabled smart finance. Most existing blockchain platforms, particularly those based on PoW or similarly resource-intensive consensus mechanisms, cannot meet the transaction throughput demands of global financial systems. While traditional payment infrastructures such as Visa process thousands of transactions per second, many blockchain networks support only a few dozen, creating a substantial performance gap. At the same time, AI models require significant computational resources for training and inference, further straining system performance [269]. Key research challenges include designing lightweight AI architectures that preserve predictive accuracy while reducing computational overhead and developing scalable consensus protocols that balance decentralization, security, and efficiency. Techniques such as sharding, sidechains, and layer-2 solutions, combined with federated learning and edge AI, show promise but remain immature for large-scale deployment. Integrating AI and blockchain also introduces additional latency and throughput constraints. Real-time financial services require rapid execution, yet hybrid on-chain/off-chain architectures and parallel AI computations must be carefully optimized to avoid compromising security. These challenges are particularly pronounced in DeFi and smart-city finance scenarios with high transaction volumes and complex smart contracts [2][70][270][271]. Open research directions include cross-chain scalability, AI-assisted sharding, and load-adaptive consensus mechanisms tailored to financial traffic patterns [2][197][271].

8.2. Data privacy and confidentiality

Protecting sensitive financial data remains a persistent challenge in smart finance systems. While blockchain enhances transactional integrity through immutable records, its inherent transparency can conflict with privacy regulations such as the GDPR, which grants individuals the right to data erasure [96]. This tension complicates the handling of transactional, behavioral, and biometric data. AI models integrated through federated learning introduce additional privacy risks, including model inversion and gradient leakage attacks. Addressing these risks requires adopting privacy-preserving techniques such as differential privacy, homomorphic encryption, and zero-knowledge proofs. However, these methods increase computational complexity and may hinder real-time processing. Balancing model utility, predictive accuracy, and confidentiality is therefore a central research concern. Public and consortium blockchains further complicate compliance with data localization and erasure requirements [18][141][261]. Open research areas include standardized privacy-by-design AI–blockchain architectures and robust, attack-resilient federated learning frameworks [18][141][272].

8.3. Security threats and adversarial risks

AI–blockchain systems face compounded security threats originating from both domains. AI models are vulnerable to evasion, data poisoning, and model extraction attacks, while blockchain platforms remain exposed to threats such as 51% attacks, double-spending, and smart contract exploits [273]. Hybrid security frameworks that combine AI-driven anomaly detection with blockchain-based auditability are emerging as a promising defense strategy. Explainable AI can further enhance threat detection by improving transparency and interpretability. However, adversarial AI techniques combined with blockchain vulnerabilities amplify systemic risks, particularly in smart contracts, cross-chain bridges, and consensus mechanisms [63][270][271]. Key open challenges include formal threat modeling across AI–blockchain layers, robust adversarial training, and the development of automated, verifiable incident response mechanisms implemented through smart contracts.

8.4. Interoperability and standardization

Limited interoperability and fragmented standards significantly hinder the adoption of AI and blockchain in financial systems. Blockchain platforms such as ERC20-based systems, Hyperledger Fabric, and Solana differ in consensus models, data structures, and governance mechanisms, creating institutional silos [274]. AI model sharing faces similar barriers due to heterogeneous data formats, infrastructures, and regulatory constraints. Although initiatives such as the Interledger Protocol offer early solutions, standardized frameworks for cross-chain communication and secure exchange of AI models remain underdeveloped. Current research highlights the complexity of integrating heterogeneous blockchains with legacy banking systems, IoT environments, and diverse AI stacks while maintaining security guarantees. Open research directions include cross-chain identity standards, modular architectures, and standardized benchmarks for performance and security evaluation [1][270][275][276].

8.5. Regulatory compliance and ethical concerns

Regulatory uncertainty surrounding digital assets, DeFi platforms, and AI-driven decision-making presents both opportunities and risks for financial institutions [277]. Ethical concerns, including bias, fairness, and accountability in AI models, remain largely unresolved. Future research must embed regulatory and ethical considerations directly into the design of AI–blockchain systems. Promising approaches include regulatory-aware smart contracts, explainable AI mechanisms, and automated audit frameworks. Balancing transparency, performance, and security is essential to support

responsible innovation. As financial decision-making becomes increasingly autonomous, systems must ensure fairness, auditability, and compliance with evolving regulations across jurisdictions [1][18][141][261].

8.6. Energy efficiency and sustainability

Energy consumption poses a major sustainability challenge for AI–blockchain-enabled finance. PoW consensus mechanisms and large-scale AI model training require substantial computational resources, leading to significant carbon footprints. Research priorities include energy-efficient consensus mechanisms such as Proof-of-Stake, energy-aware AI models, model compression techniques, and hardware-level optimizations. Designing sustainable AI–blockchain architectures requires carefully balancing security, scalability, and ecological impact while maintaining real-time performance requirements [1][2][197][270][271].

8.7. Real-time decision-making and latency

Many financial applications, including fraud detection, credit scoring, and payment processing, demand low-latency decision-making. Integrating AI inference with blockchain validation introduces delays that can undermine real-time performance [273]. Smart contracts further contribute to latency due to execution complexity and consensus overhead. Potential solutions include hybrid on-chain/off-chain processing, edge computing, asynchronous consensus protocols, and AI hardware acceleration. These approaches aim to enable secure, sub-second financial decisions without compromising transaction integrity [2][63][70][261].

8.8. Trust, transparency, and explainability

AI models in finance often function as black boxes, limiting transparency for regulators, auditors, and end users. While blockchain provides immutable audit trails, linking these records to interpretable AI decision-making remains challenging. Integrating explainable AI (XAI) frameworks with blockchain logs can improve accountability, regulatory compliance, and stakeholder trust [221][278-281]. However, open challenges include defining standardized explanation metrics, designing interfaces for non-technical users, and ensuring explanation stability under model updates, data drift, or adversarial manipulation [221][282-284].

8.9. Post-quantum security

Advances in quantum computing threaten the cryptographic foundations of blockchain and secure AI communication, including RSA and elliptic curve cryptography [274]. To address this risk, post-quantum cryptography (PQC), such as lattice- and hash-based schemes, is required to protect AI–blockchain systems. Current research focuses on quantum-resistant consensus mechanisms, smart contract layers, and audit trails that remain compatible with real-time financial operations. A key challenge lies in integrating PQC primitives with existing financial key infrastructures without degrading system performance [141][285-287].

8.10. Secure and trustworthy AI model lifecycle management

AI models deployed in finance require continuous updates to adapt to evolving threats, behaviors, and market conditions. In decentralized and federated environments, ensuring model integrity, provenance, and resistance to poisoned updates remains challenging. While blockchain can store model version hashes, validating contributions, managing rollbacks, and maintaining performance are unresolved issues [286]. Emerging lifecycle frameworks, such as REASON, integrate orchestration, monitoring, and digital twins, but their applicability to multi-party, regulated financial ecosystems remains limited [279][284][286].

8.11. Robustness against adversarial and adaptive attacks

Both AI and blockchain components are vulnerable to adaptive attacks, including evasion, poisoning, and strategic exploitation of transparent ledgers. Designing real-time, robust defenses that integrate drift-aware AI retraining, blockchain audit logs, and XAI-based detectors remains an open challenge [284][288-290]. Open research questions include modeling cross-layer attack surfaces, defining robustness benchmarks, and enabling self-improving defense mechanisms without introducing new vulnerabilities.

8.12. Governance, accountability, and liability allocation

Decentralized architectures complicate governance and liability assignment in AI-driven financial systems. Responsibility for errors, security breaches, or biased decisions may be distributed among AI developers, blockchain validators, financial institutions, and end users. Research priorities include contractual liability frameworks, layered governance models, automated audit mechanisms, and dispute resolution protocols, particularly in consortium and cross-jurisdictional blockchain deployments [284][291].

8.13. Continuous learning and concept drift management

Financial environments are inherently non-stationary, with continuously evolving fraud strategies, customer behaviors, and market dynamics. Incorporating continuous learning into blockchain-anchored AI systems requires traceable and verifiable model updates. Key challenges include coordinating federated drift detection, distinguishing genuine drift from adversarial poisoning, and implementing regulation-compliant retraining and rollback mechanisms [284][286][288][290].

8.14. Legal, ethical, and cross-jurisdictional compliance

Smart finance platforms often operate across multiple jurisdictions with diverse legal, regulatory, and ethical requirements. Ensuring that AI automation and blockchain immutability comply with these frameworks is inherently complex. Key research challenges include reconciling blockchain immutability with data-subject rights, operationalizing fairness and non-discrimination in AI models, and translating overlapping regulatory requirements into machine-checkable policies enforced through smart contracts [282][291][292].

Collectively, these challenges highlight the complexity of integrating AI and blockchain in smart finance. Addressing issues related to scalability, privacy, security, real-time performance, governance, and sustainability requires interdisciplinary solutions that combine distributed ledger technologies, artificial intelligence, cryptography, regulatory compliance, and ethical frameworks. Such efforts are essential to realizing secure, resilient, and trustworthy financial systems at scale.

9. FUTURE RESEARCH DIRECTIONS

Integrating AI with blockchain offers substantial potential to strengthen security in smart finance. However, realizing these benefits requires systematic research across multiple domains. Future investigations should focus on the following.

9.1. Advancements in explainable artificial intelligence (XAI) in finance

Explainable artificial intelligence (XAI) is critical for the secure and trustworthy deployment of AI in financial services. Although deep learning models perform well in fraud detection, risk scoring, and anomaly detection, their lack of interpretability limits their suitability for regulated environments. Transparency, fairness, and accountability are essential requirements in finance, where automated decisions must be justifiable to regulators and end users [96]. Future research should prioritize interpretable machine-learning models that make AI-driven evaluations understandable to humans. Integrating XAI with blockchain's tamper-proof audit trails can generate verifiable records of AI decisions, strengthening governance and trust. This integration is particularly valuable in high-risk domains such as lending and insurance, where real-time fraud prevention must align with regulatory compliance.

9.2. Post-quantum blockchain systems

Secure blockchain infrastructure underpins smart finance applications, including payments, asset tokenization, decentralized authentication, and immutable recordkeeping. However, advances in quantum computing threaten classical cryptographic schemes, as algorithms such as Shor's and Grover's could compromise the security of existing blockchains. To address this risk, future smart finance systems must adopt post-quantum blockchain architectures based on lattice-based, multivariate, and hash-based cryptographic schemes [274]. Integrating AI-driven anomaly detection into these systems can further enhance resilience by identifying and mitigating quantum-enabled cyberattacks. Research on quantum-resistant signatures, cryptographic primitives, and consensus mechanisms will be essential to ensure long-term security and performance in the post-quantum era.

9.3. Edge computing and IoT-enabled financial services

The rapid growth of mobile devices, wearables, and IoT-enabled systems demands low-latency and secure processing of sensitive financial data. Centralized cloud infrastructures alone cannot meet these real-time requirements. By integrating AI and blockchain at the network edge, smart finance systems can enable localized fraud detection, authentication, and anomaly monitoring [269]. Edge-based AI–blockchain solutions are particularly relevant for IoT-driven applications such as micropayments, pay-as-you-go insurance, mobility services, and asset tracking. Future research should explore architectures that combine edge intelligence, blockchain anchoring, and IoT telemetry to secure distributed financial infrastructures and support adaptive risk detection closer to data sources.

9.4. Regulatory-compliant AI–blockchain frameworks

Smart finance systems operate under stringent regulatory requirements, including AML, KYC, GDPR, and consumer protection laws. However, the rapid evolution of AI and blockchain technologies often outpaces regulatory development, creating uncertainty for financial institutions and smart contract developers [277]. Future research should focus on embedding regulatory compliance directly into AI–blockchain architectures through programmable smart contracts, automated decision engines, and real-time reporting tools. Regulatory technology (RegTech) solutions can help digital banks, DeFi platforms, and mobile money systems maintain transparency, auditability, and compliance while adapting to evolving legal and ethical standards.

9.5. Adaptive and self-learning security architectures

Cyber threats in smart finance are increasingly dynamic, targeting APIs, mobile applications, smart contracts, and cross-chain bridges. Traditional static security mechanisms struggle to keep pace with the speed and complexity of modern financial environments. Developing adaptive, self-learning AI security models integrated with blockchain infrastructure enables continuous monitoring of transaction streams and real-time detection of evolving threat patterns [273]. These systems can automatically update detection thresholds and consensus parameters, making them well-suited for high-frequency use cases such as digital payments, decentralized exchanges, and automated lending.

9.6. Interdisciplinary collaboration for holistic innovation

Advancing security in smart finance requires close collaboration among AI researchers, blockchain engineers, cybersecurity experts, regulators, and financial practitioners [273][277]. Interdisciplinary engagement ensures that AI–blockchain solutions address not only technical challenges but also ethical, legal, and operational constraints. Such collaboration improves interoperability, transparency, and system robustness, while fostering public trust in emerging financial technologies [96]. Future research should encourage initiatives that integrate perspectives from computer science, finance, cryptography, behavioral economics, and regulatory studies.

9.7. Standardization and interoperability

Smart finance ecosystems remain fragmented, with heterogeneous AI models, blockchain platforms, and governance mechanisms operating in isolation. This fragmentation limits cross-platform transactions, coordinated fraud detection, and cross-chain auditing. Future research should emphasize standardized data representations, interoperable smart contract frameworks, and secure cross-chain communication protocols. Achieving interoperability is critical for global scalability, coordinated risk management, and efficient information sharing across financial institutions.

9.8. Privacy-preserving AI and confidential data sharing

Privacy concerns continue to constrain AI adoption in finance due to the sensitivity of transactional, biometric, and behavioral data. Privacy-enhancing techniques such as federated learning, secure multi-party computation, differential privacy, and homomorphic encryption enable collaborative model training without exposing raw data [152]. When combined with blockchain-based access control, consent management, and immutable audit trails, these approaches can support secure cross-institutional collaboration. This integration facilitates shared fraud intelligence, compliant credit scoring, and trustworthy data exchange while preserving regulatory and ethical requirements [277].

9.9. Energy-efficient and sustainable smart finance

The computational intensity of deep learning and blockchain technologies raises concerns about energy consumption and environmental sustainability. As smart finance scales, these challenges become increasingly significant. Future research should explore energy-efficient AI models, lightweight inference techniques, and sustainable blockchain consensus protocols, such as Proof of Stake, Proof of Authority, and hybrid mechanisms [274]. Energy-aware AI–blockchain architectures are essential for long-term operational viability and alignment with green finance objectives.

9.10. Human-centered and trust-aware systems

Despite increasing automation, human trust and usability remain central to the adoption of smart finance technologies. Systems must provide transparent explanations, intuitive interfaces, and meaningful opportunities for human oversight [96]. Human-centered and trust-aware design principles are particularly important for consumer-facing applications, including mobile banking, digital wallets, and DeFi platforms. In these contexts, perceived fairness, accountability, and control strongly influence adoption and long-term sustainability.

9.11. Smart contract verification and security

Smart contracts automate financial transactions but remain vulnerable to logic errors, parameter manipulation, and malicious exploits. These weaknesses pose significant risks to decentralized financial systems. Future research should advance formal verification techniques, automated vulnerability detection, and AI-assisted smart contract development. These approaches can improve correctness, robustness, and resilience, reducing the likelihood of costly security breaches.

9.12. Systemic and AI concentration risk

Widespread reliance on similar AI models, shared datasets, and centralized service providers introduces systemic risks that can propagate across institutions. Such concentration increases the likelihood of correlated failures during market stress or cyber incidents. Future studies should investigate decentralized AI governance, blockchain-based accountability mechanisms, and stress-testing frameworks to quantify and mitigate systemic exposure. Distributed intelligence and diversified decision-making can enhance ecosystem resilience and reduce cascading failures.

9.13. Real-time, high-frequency financial decision systems

Smart finance increasingly operates in real-time environments, including instant payments, algorithmic trading, and automated lending. These applications demand ultra-low-latency decision-making without compromising security or data integrity. Research should focus on optimizing AI–blockchain pipelines by reducing consensus delays, accelerating smart contract execution, and deploying AI inference closer to data sources [152][269]. Such advances support rapid anomaly detection, validation, and response in high-frequency financial systems.

9.14. Education, skills development, and capacity building

The sustainable adoption of AI and blockchain technologies in smart finance depends on a skilled and interdisciplinary workforce. Addressing gaps in expertise across AI, blockchain, cybersecurity, finance, and regulation is therefore essential. Future research should examine educational models, workforce development strategies, and institutional capacity-building initiatives [273]. Reskilling programs and ethics-focused training will play a critical role in ensuring long-term resilience, responsible innovation, and effective system deployment.

Collectively, these research directions provide a comprehensive roadmap for developing resilient, secure, and adaptive AI–blockchain-enabled smart finance systems. By emphasizing technical innovation, regulatory alignment, privacy preservation, sustainability, and human-centered design, future work can enable trustworthy, scalable, and future-proof financial infrastructures.

10. CONCLUSION

The convergence of AI and blockchain is reshaping smart finance systems by strengthening security, transparency, and operational resilience. This survey systematically reviews state-of-the-art techniques, architectures, and frameworks that integrate AI-driven analytics with blockchain's decentralized trust mechanisms to address complex financial security challenges. Across diverse applications, including DeFi, traditional banking fraud detection, enterprise risk management, smart lending, payment systems, and ESG-aligned financial services, AI delivers adaptive, predictive, and anomaly-detection capabilities. In parallel, blockchain provides immutability, auditability, and secure automation through smart contracts, establishing a trusted foundation for intelligent financial operations.

The integration of AI and blockchain enhances real-time threat detection and fraud mitigation while supporting regulatory compliance, privacy preservation, and cross-institutional collaboration. Empirical use cases show that combining intelligent analytics with immutable ledgers enables faster responses to emerging risks, end-to-end traceability, and improved accountability across both decentralized and centralized financial ecosystems. Beyond conventional security benefits, AI–blockchain integration enables advanced functionalities such as autonomous risk management, AI-powered smart contracts, IoT-enabled financial monitoring, and ESG-compliant investment verification. These capabilities highlight the broad applicability and transformative potential of AI–blockchain frameworks in modern financial systems.

Despite significant progress, critical research challenges remain. These include scalability, privacy, interoperability, explainability, robustness to adversarial attacks, continuous learning under concept drift, governance, energy efficiency, and cross-jurisdictional regulatory compliance. Addressing these issues is essential to unlock the benefits of AI–blockchain-enabled financial security fully.

In summary, integrating AI and blockchain offers a robust, promising pathway to securing smart finance systems. By coupling adaptive intelligence with decentralized verification, these frameworks promote resilient, transparent, and trustworthy financial infrastructures. The insights synthesized in this survey provide a foundation for advancing secure, efficient, and ethically responsible smart finance solutions in the evolving digital economy.

Funding:

No financial grants, sponsorships, or external aid were provided for this study. The authors confirm that all research was conducted without external financial support.

Conflicts of Interest:

The authors declare that there are no conflicts of interest regarding this publication.

Acknowledgment:

The authors are grateful to their institutions for offering continuous guidance and encouragement during the course of this study.

References

[1] A. P. D. O. C. S. Mandsaur and N. Jain, "FinTech revolution: A systematic review of AI and blockchain integration in modern financial systems in banking sector," *Int. J. Adv. Res. Comput. Sci.*, vol. 16, no. 4, pp. 162–169, 2025, doi: 10.26483/ijarcs.v16i4.7324.

[2] R. Jha, "Blockchain technology and its transformative impact on the finance industry: Redefining security, efficiency, and decentralization," *Int. J. Sci. Res. Eng. Manag.*, vol. 9, no. 5, pp. 1–9, 2025, doi: 10.55041/ijsrem48486.

[3] V. Ramaiya, "Echoes of a cashless future: Digital payments as catalysts for sustainable finance," *J. Inf. Syst. Eng. Manag.*, vol. 10, no. 36s, pp. 556–567, 2025, doi: 10.52783/jisem.v10i36s.6530.

[4] L. Mada, "The rise of mobile payment systems, digital wallets: Successes, security and challenges," *Eur. J. Comput. Sci. Inf. Technol.*, vol. 13, no. 10, pp. 137–152, 2025, doi: 10.37745/ejcsit.2013/vol13n10137152.

[5] H. Harichandana, "Digital payment adoption in emerging markets," *Int. J. Sci. Technol.*, vol. 16, no. 3, 2025, doi: 10.71097/ijsat.v16.i3.7770.

[6] J. W. M. Lopez, A. V. M. Gonzales, and P. P. C. Condori, "Predictive models based on machine learning to analyze the adoption of digital payments in Latin America and the Caribbean," *Int. J. Data Netw. Sci.*, vol. 9, no. 3, pp. 411–418, 2025, doi: 10.5267/j.ijdns.2025.3.001.

[7] Z. Yu and F. Huang, "Research on the innovation of supply chain financial management model for agricultural enterprises in the context of smart finance," *Res. World Agric. Econ.*, vol. 6, no. 2, pp. 652–665, 2025, doi: 10.36956/rwae.v6i2.1525.

[8] G. Yanjun, "Application of blockchain technology in green finance and evaluation of its economic effects," *J. Posthumanism*, vol. 5, no. 5, pp. 2239–2264, 2025, doi: 10.63332/joph.v5i5.1613.

[9] C. Da Silva Robusti, A. B. A. Avelar, M. C. Farina, and C. A. Gananca, "Blockchain and smart contracts: Transforming digital entrepreneurial finance and venture funding," *J. Small Bus. Enterp. Dev.*, vol. 32, no. 3, pp. 739–761, 2025, doi: 10.1108/jsbed-12-2023-0584.

[10] H. Guo and X. Liu, "Exploring trust dynamics in finance: The impact of blockchain technology and smart contracts," *Humanit. Soc. Sci. Commun.*, vol. 12, no. 1, 2025, doi: 10.1057/s41599-025-05473-9.

[11] J. Chen, "Research on AI-based smart finance innovation models and their impact mechanisms," *Adv. Econ. Manag. Res.*, vol. 14, no. 1, pp. 711–715, 2025, doi: 10.56028/aemr.14.1.711.2025.

[12] C. Ling and T. Le, "Intelligent decision-making in smart port development in China through green finance instruments: A sustainable approach to the marine ecosystem," *Front. Mar. Sci.*, pp. 1–17, 2025, doi: 10.3389/fmars.2025.1656454.

[13] O. Adesanya, A. Akinola, and L. Oyeniyi, "Smart contract technologies enabling secure, automated cross-border financial transactions across global economic markets," *Gulf J. Adv. Bus. Res.*, vol. 3, no. 9, pp. 1331–1358, 2025, doi: 10.51594/gjabr.v3i9.161.

[14] G. Ali and Z. Yahia, "Disclosure determinants of blockchain crowdfunding performance for sustainable smart city financing: An explainable OPTUNA-optimized machine learning approach," *J. Posthumanism*, vol. 5, no. 7, pp. 802–826, 2025, doi: 10.63332/joph.v5i7.2843.

[15] G. Ali, M. M. Mijwil, B. A. Buruga, and M. Abotaleb, "A comprehensive review on cybersecurity issues and their mitigation measures in FinTech," *Iraqi J. Comput. Sci. Math.*, vol. 5, no. 3, pp. 45–91, 2024, doi: 10.52866/ijcsm.2024.05.03.004.

[16] K. Boorugupalli, A. Kulkarni, A. Suzana, D. M, S. Ponnusamy, and K. S., "Cybersecurity measures in financial institutions protecting sensitive data from emerging threats and vulnerabilities," *ITM Web Conf.*, vol. 76, pp. 1–11, 2025, doi: 10.1051/itmconf/20257602002.

[17] M. Waliullah, M. Z. H. George, M. T. Hasan, M. K. Alam, M. S. K. Munira, and N. A. Siddiqui, "Assessing the influence of cybersecurity threats and risks on the adoption and growth of digital banking: A systematic literature review," *Am. J. Adv. Technol. Eng. Solut.*, vol. 1, no. 1, pp. 226–257, 2025, doi: 10.63125/fh49gz18.

[18] M. A. Adegbite, "Data privacy and data security challenges in digital finance," *J. Digit. Secur. Forensics*, vol. 2, no. 1, pp. 6–11, 2025, doi: 10.29121/digisecforensics.v2.i1.2025.40.

[19] A. Adeyemi and J. Park, "Cyber supply chain risks in financial technology ecosystems," *Comput. Secur.*, vol. 134, p. 103445, 2025, doi: 10.1016/j.cose.2024.103445.

[20] O. A. Adekoya, H. F. Atlam, and H. S. Lallie, "Quantifying the multidimensional impact of cyber attacks in digital financial services: A systematic literature review," *Sensors*, vol. 25, no. 14, p. 4345, 2025, doi: 10.3390/s25144345.

[21] A. Paul, A. Adejumo, and C. Ogburie, "The role of cybersecurity in safeguarding finance in a digital era," *World J. Adv. Res. Rev.*, vol. 25, no. 3, pp. 1542–1556, 2025, doi: 10.30574/wjarr.2025.25.3.0909.

[22] A. T. Olutimehin, "Assessing the effectiveness of cybersecurity frameworks in mitigating cyberattacks in the banking sector and its applicability to decentralized finance (DeFi)," *Asian J. Res. Comput. Sci.*, vol. 18, no. 3, pp. 130–151, 2025, doi: 10.9734/ajrcos/2025/v18i3583.

[23] S. C. Prabanand and M. S. Thanabal, "Advanced financial security system using smart contract in private Ethereum consortium blockchain with hybrid optimization strategy," *Sci. Rep.*, vol. 15, no. 1, p. 6764, 2025, doi: 10.1038/s41598-025-89404-3.

[24] U. Kumar and A. Sethupathy, "Evolving frameworks in digital payment security: Technological innovations, economic impact, and consumer trust dynamics," *Int. J. Comput. Exp. Sci. Eng.*, vol. 11, no. 3, pp. 6623–6634, 2025, doi: 10.22399/ijcesen.3893.

[25] M. S. Ahammad, M. Maliha, N. E. Nila, and M. S. Islam, "An innovative blockchain framework for strengthening security and efficiency in banking," *Sci. Rep.*, vol. 15, no. 1, p. 39029, 2025, doi: 10.1038/s41598-025-25457-8.

[26] S. Basha *et al.*, "Budget tracking using blockchain," *Int. J. Eng. Technol. Manag. Sci.*, vol. 9, no. 2, pp. 1–7, 2025, doi: 10.46647/ijetms.2025.v09i02.094.

[27] Y. Chen, J. Liu, and H. Xu, "Trusted data pipelines for AI-enabled blockchain systems," *IEEE Trans. Dependable Secure Comput.*, 2025, doi: 10.1109/TDSC.2024.3389712.

[28] R. Zhao and D. Yermack, "AI, fraud detection, and financial stability," *J. Financ. Econ.*, 2024, doi: 10.1016/j.jfineco.2023.103640.

[29] D. Nguyen, Q. Tran, and H. Le, "Cross-chain security threats in decentralized finance," *Future Internet*, vol. 15, no. 6, p. 193, 2023, doi: 10.3390/fi15060193.

[30] L. Chen, Y. Qi, and X. Zhou, "Hybrid AI–blockchain systems for decentralized finance security," *Future Gener. Comput. Syst.*, vol. 150, pp. 42–55, 2024, doi: 10.1016/j.future.2023.09.021.

[31] N. Afifah, M. Syafii, and F. Tuharea, "Smart finance: Leveraging technology for optimal financial decision-making," *OPTIMAL J. Ekon. Manaj.*, vol. 5, no. 1, pp. 546–557, 2025, doi: 10.55606/optimal.v5i1.6549.

[32] Y. Hou and J. Feng, "Research on the construction of smart accounting systems in the context of big data," *Account. Corp. Manag.*, vol. 7, no. 1, pp. 54–59, 2025, doi: 10.23977/acccm.2025.070107.

[33] A. Enaya, X. Fernando, and R. Kashef, "Survey of blockchain-based applications for IoT," *Appl. Sci.*, vol. 15, no. 8, p. 4562, 2025, doi: 10.3390/app15084562.

[34] R. Alt and M. Gräser, "Distributed ledger technology," *Electron. Mark.*, vol. 35, no. 1, 2025, doi: 10.1007/s12525-025-00784-w.

[35] P. Chatterjee, "Internet of Things (IoT) and future of digital payments: Enabling smart, automated transactions," *Indian J. Comput. Sci. Eng.*, vol. 16, no. 3, pp. 81–88, 2025, doi: 10.21817/indjcse/2025/v16i1/251603004.

[36] A. Ismaya *et al.*, "Drivers of secure and inclusive DeFi adoption through distributed ledger technology and smart contracts," in *Proc. 4th Int. Conf. Creative Communication and Innovative Technology (ICCIT)*, Kota Cirebon, Indonesia, Aug. 15–16, 2025, pp. 1–7, doi: 10.1109/ICCIT65724.2025.11167426.

[37] S. Balan *et al.*, "Smart finance innovations with federated learning and blockchain integration," in *Proc. 6th Int. Conf. Emerging Technology (INCET)*, Belgaum, India, May 23–25, 2025, pp. 1–6, doi: 10.1109/INCET64471.2025.11140005.

[38] G. Chhabra *et al.*, "Cloud-based AI solutions for personal finance management," in *Proc. Int. Conf. Pervasive Computational Technologies (ICPCT)*, Greater Noida, India, Feb. 8–9, 2025, pp. 327–332, doi: 10.1109/ICPCT64145.2025.10941085.

[39] S. Zhou, "Financial innovation and market transformation in the age of digital finance," *Trans. Econ. Bus. Manag. Res.*, vol. 6, pp. 118–127, 2024, doi: 10.62051/0g0y9488.

[40] O. Kolisnyk and D. Skliarov, "Transformation of financial accounting: From traditional methods to digitalization," *Bus. Navigator*, no. 79, 2025, doi: 10.32782/business-navigator.79-36.

[41] Y. Li, "Key technologies of financial digital industry innovation and green development driven by information technology," *Int. J. Comput. Intell. Syst.*, vol. 16, no. 1, 2023, doi: 10.1007/s44196-023-00262-1.

[42] E. V. Karanina and D. I. Skopin, "Theoretical aspect of digital finance development," *Ekonomika I Upravlenie Problemy Resheniya*, vol. 138, no. 6/4, pp. 5–11, 2023, doi: 10.36871/ek.up.p.r.2023.06.04.001.

[43] B. Sanga and M. Aziakpono, "FinTech and SMEs financing: A systematic literature review and bibliometric analysis," *Digit. Bus.*, vol. 3, no. 2, p. 100067, 2023, doi: 10.1016/j.digbus.2023.100067.

[44] Z. Chen, "The logic of digital finance in the age of digital economy," *Proc. Bus. Econ. Stud.*, vol. 7, no. 2, pp. 53–59, 2024, doi: 10.26689/pbes.v7i2.6605.

[45] A. Y. S. Lam, "Artificial intelligence applications in financial technology," *J. Theor. Appl. Electron. Commer. Res.*, vol. 20, no. 1, p. 29, 2025, doi: 10.3390/jtaer20010029.

[46] G. Kou and Y. Lu, "FinTech: A literature review of emerging financial technologies and applications," *Financial Innovation*, vol. 11, no. 1, 2025, doi: 10.1186/s40854-024-00668-6.

[47] Y. Wang, A. Jiang, S. Zhang, and W. Chen, "Traditional finance, digital finance, and financial efficiency: An empirical analysis based on 19 urban agglomerations in China," *Int. Rev. Financ. Anal.*, vol. 96, p. 103603, 2024, doi: 10.1016/j.irfa.2024.103603.

[48] B. N. Chukwu, "FinTech innovation and digital security: AI applications for fraud mitigation and regulatory compliance in US financial markets," *Int. J. Sci. Res. Archive*, vol. 17, no. 1, pp. 1031–1041, 2025, doi: 10.30574/ijsra.2025.17.1.2916.

[49] V. Sharma, "The future of automation in financial technology: Leveraging AI to enhance fraud detection and risk management," *Int. J. Sci. Res. Eng. Manag.*, vol. 9, no. 2, pp. 1–7, 2025, doi: 10.55041/ijsrem27483.

[50] K. Chauhan, S. Singh, and P. Aggarwal, "Reconceptualizing digital payments: The enhanced role of AI in transforming financial transactions ecosystem," *Lloyd Bus. Rev.*, pp. 210–219, 2025, doi: 10.56595/lbr.v4i1.68.

[51] N. S. Sukumaran, "The role of AI in automating enterprise payments: Enhancing speed, accuracy, and security," *World J. Adv. Eng. Technol. Sci.*, vol. 15, no. 1, pp. 1912–1920, 2025, doi: 10.30574/wjaets.2025.15.1.0425.

[52] N. V. Bala, "Secure multi-tenant FinTech architecture: Real-time AI-powered fraud detection pipeline with encrypted data streams," *J. Comput. Sci. Technol. Stud.*, vol. 7, no. 10, pp. 217–224, 2025, doi: 10.32996/jcsts.2025.7.10.24.

[53] S. Ionescu, V. Diaconita, and A. Radu, "Engineering sustainable data architectures for modern financial institutions," *Electronics*, vol. 14, no. 8, p. 1650, 2025, doi: 10.3390/electronics14081650.

[54] R. Fang, "Integrating blockchain and ESG reporting standards to develop a smart green supply chain finance framework for sustainable procurement decisions," *J. Appl. Econ. Policy Stud.*, vol. 18, no. 8, pp. 49–55, 2025, doi: 10.54254/2977-5701/2025.26384.

[55] N. J. S. R. K. Terli, "Middleware integration for financial services and banking: A framework for resilient architecture," *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.*, vol. 11, no. 2, pp. 1855–1867, 2025, doi: 10.32628/cseit25112547.

[56] V. Kata, "The critical role of middleware in modern financial transaction systems," *Eur. J. Comput. Sci. Inf. Technol.*, vol. 13, no. 14, pp. 18–25, 2025, doi: 10.37745/ejcsit.2013/vol13n141825.

[57] N. L. Mada, "The evolution and technical landscape of decentralized finance: From DeFi to DeFi 2.0," *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.*, vol. 11, no. 1, pp. 3278–3286, 2025, doi: 10.32628/cseit251112344.

[58] A. Kuna, "Dynamic risk-adaptive quality assurance systems for decentralized financial platforms (DeFi)," *Eur. J. Comput. Sci. Inf. Technol.*, vol. 13, no. 49, pp. 131–140, 2025, doi: 10.37745/ejcsit.2013/vol13n49131140.

[59] T. A. Onalaja, R. S. Nwachukwu, F. A. Bankole, and T. Lateefat, "Digital finance transformation model: Designing risk and control in artificial intelligence-driven accounting systems," *Eng. Technol. J.*, vol. 10, no. 9, 2025, doi: 10.47191/etj/v10i09.19.

[60] Y. R. Patel, "Designing intelligent and secure smart payment systems: An AI-driven, tokenized, and compliance-aware framework for real-time digital transactions," *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 13, no. 5, pp. 5281–5286, 2025, doi: 10.22214/ijraset.2025.71437.
[61] E. Sayed and S. M. Mosaad, "Quantum-classical hybrid architectures for blockchain and contextual AI," *Multicriteria Algorithms Appl.*, vol. 8, pp. 1–18, 2025, doi: 10.61356/j.mawa.2025.8572.
[62] S. Williams, "Blockchain, AI and quantum networks: A tri-layer model for secure transactions in finance and healthcare," *Artif. Intell. Quantum Comput. Robot. Sci. Technol. J.*, vol. 3, no. 1, pp. 1–14, 2025, doi: 10.64206/3afw9v18.
[63] R. H. Chowdhury, "Next-generation cybersecurity through blockchain and AI synergy: A paradigm shift in intelligent threat mitigation and decentralised security," *Int. J. Res. Sci. Innov.*, vol. 12, no. 8, pp. 614–648, 2025, doi: 10.51244/ijrsi.2025.120800051.
[64] N. J. Taralkar, "CoPilot finance: Enhancing decision-making through human-AI synergy," *J. Inf. Syst. Eng. Manag.*, vol. 10, no. 57s, pp. 1212–1220, 2025, doi: 10.52783/jisem.v10i57s.12547.
[65] H. Atole, "Capit-AI: An AI-driven financial advisory system," *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 13, no. 4, pp. 5124–5136, 2025, doi: 10.22214/ijraset.2025.69398.
[66] D. C. Deepthi, "AI-powered finance management platform," *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 13, no. 6, pp. 1574–1578, 2025, doi: 10.22214/ijraset.2025.72438.
[67] M. S. Saini *et al.*, "AI-powered personal finance management applications," in *Proc. World Skills Conf. Universal Data Analytics and Sciences (WorldSUAS)*, Indore, India, Aug. 22–23, 2025, pp. 1–6, doi: 10.1109/WorldSUAS66815.2025.11199144.
[68] V. Mogilipalem, C. Rajkumar, M. Moparthi, S. Vasamsetti, and V. M. R. M., "Revolutionizing personal finance: AI-powered solutions for financial advisory transformation," in *Proc. Int. Conf. Data Sci. Bus. Syst. (ICDSBS)*, Chennai, India, Apr. 17–18, 2025, pp. 1–7, doi: 10.1109/ICDSBS63635.2025.11031758.
[69] N. D. Babu, N. R. Manisha, and N. V. Sai, "Project report on wealth management," *Int. J. Eng. Res. Sci. Technol.*, vol. 21, no. 3(1), pp. 1291–1299, 2025, doi: 10.62643/ijerst.v21.n3(1).pp1291-1299.
[70] S. Rahnama, "DeFiSentinel: AI-enhanced decentralized finance architecture with advanced cryptographic smart contracts for data integrity and threat resilience," *IEEE Access*, vol. 13, pp. 83107–83122, 2025, doi: 10.1109/ACCESS.2025.3568842.
[71] J. N. K. Wah, "Smart finance unleashed: AI-driven predictive analytics and risk management in finance," *J. Hunan Univ. Nat. Sci.*, vol. 52, no. 5, pp. 26–44, 2025, doi: 10.55463/issn.1674-2974.52.5.3.
[72] D. Deepak, "AI in finance: Fraud detection, algorithmic trading, and risk assessment," *Int. J. Appl. Behav. Sci.*, vol. 2, no. 2, pp. 37–48, 2025, doi: 10.70388/ijabs250135.
[73] C. R. Kathuria, "Sustainable FinTech innovation in consumer lending: Advancing inclusive credit through P2P platforms and alternative scoring models," *Metall. Mater. Eng.*, pp. 928–940, 2025, doi: 10.63278/mme.vi.1666.
[74] M. Tigges, S. Mestwerdt, S. Tschirner, and R. Mauer, "Who gets the money? A qualitative analysis of FinTech lending and credit scoring through the adoption of AI and alternative data," *Technol. Forecast. Soc. Change*, vol. 205, p. 123491, 2024, doi: 10.1016/j.techfore.2024.123491.
[75] E. Ayodele, M. A. Oye, B. C. Alimi, and S. B. Obitolu, "Investigating blockchain-based smart contracts for cross-border payment settlement, regulatory compliance and risk reduction in international finance," *Int. J. Sci. Res. Archive*, vol. 16, no. 2, pp. 52–73, 2025, doi: 10.30574/ijsra.2025.16.2.2290.
[76] M. A. G. Elden, A. S. Ismail, M. E. Shaheen, and M. E. Shaheen, "Revolutionizing payment systems: Enhancing speed, security, and cost efficiency with blockchain technology," *J. Posthumanism*, vol. 5, no. 6, pp. 1550–1564, 2025, doi: 10.63332/joph.v5i6.2225.
[77] Y. Sui, "Research on the application of smart finance in the financial industry," *Mod. Econ. Manage. Forum*, vol. 6, no. 4, p. 598, 2025, doi: 10.32629/memf.v6i4.4259.
[78] M. E. Harras and M. A. Salahddine, "Tracking financial crime through code and law: A review of RegTech applications in anti-money laundering and terrorism financing," *Corp. Law Governance Rev.*, vol. 7, no. 3, p. 73, 2025, doi: 10.22495/clgrv7i3p7.
[79] G. Modalavalasa, "Leveraging machine learning techniques for proactive regulatory (RegTech) compliance in financial landscape," in *Proc. 3rd World Conf. Commun. Comput. (WCONF)*, Raipur, India, Jul. 25–27, 2025, pp. 1–6, doi: 10.1109/WCONF64849.2025.11233296.
[80] A. Sydykova, "RegTech development: How technology is changing governance with market compliance in the era of digital finance," *Int. J. Manag. Econ. Fundam.*, vol. 5, no. 5, pp. 14–19, 2025, doi: 10.37547/ijmef/volume05issue05-03.
[81] S. Lyu and Z. Jiao, "Optimization of financial asset allocation and risk management strategies combining Internet of Things and clustering algorithms," *IEEE Internet Things J.*, vol. 12, pp. 3654–3669, 2025, doi: 10.1109/jiot.2024.3486714.
[82] N. N. Omoruyi, "Integrating computational finance, machine learning, and risk analytics for optimized financial planning and analysis strategies," *World J. Adv. Res. Rev.*, vol. 26, no. 1, pp. 684–700, 2025, doi: 10.30574/wjarr.2025.26.1.1039.
[83] N. S. A. Sarna, N. a. A. Mohammed, and N. M. R. Miah, "AI-powered financial analytics and visualization tools: The evolving landscape of strategic finance," *J. Econ. Finance Account. Stud.*, vol. 7, no. 5, pp. 60–82, 2025, doi: 10.32996/jefas.2025.7.5.7.
[84] N. S. D. Devakate, N. M. Mupparsi, N. S. Shruthi, and N. P. Alekhya, "Financial inclusion through digital wallets and mobile banking," *World J. Adv. Res. Rev.*, vol. 25, no. 3, pp. 1905–1912, 2025, doi: 10.30574/wjarr.2025.25.3.0920.
[85] S. Ungratwar, D. Sharma, and S. Kumar, "Mapping the digital banking landscape: A multi-dimensional exploration of fintech, digital payments, and e-wallets, with insights into current scenarios and future research," *Humanit. Soc. Sci. Commun.*, vol. 12, no. 1, 2025, doi: 10.1057/s41599-025-05186-z.
[86] J. Jose and S. Kareem, "Digital wallet with dynamic transaction analytics," *Int. J. Sci. Res. (IJSR)*, vol. 14, no. 4, pp. 1320–1323, 2025, doi: 10.21275/sr25417151604.

[87] K. Garg, "How has the introduction of digital financial products (e.g., mobile wallets, robo-advisors, fintech investment apps) altered portfolio preferences and savings rates in emerging markets?" *Int. J. Multidiscip. Res.*, vol. 7, no. 5, 2025, doi: 10.36948/ijfmr.2025.v07i05.56095.

[88] Y. Zhang and K. Osei, "Data privacy risks in smart financial ecosystems," *Comput. Secur.*, vol. 123, p. 102936, 2023, doi: 10.1016/j.cose.2022.102936.

[89] V. Vipinkumar and A. Akshara, "FinTech and the right to privacy: Data protection in digital finance," *Int. J. Multidiscip. Res.*, vol. 7, no. 3, 2025, doi: 10.36948/ijfmr.2025.v07i03.45663.

[90] O. M. Dopamu, "Cloud-based ransomware attack on US financial institutions: An in-depth analysis of tactics and counter measures," *Int. J. Sci. Res. (IJSR)*, vol. 13, no. 2, pp. 1872–1881, 2024, doi: 10.21275/sr24226020353.

[91] M. Ahadi and E. A., "A review of ransomware attacks and its impact on the bank sector," *Int. J. Multidiscip. Res.*, vol. 6, no. 3, 2024, doi: 10.36948/ijfmr.2024.v06i03.21458.

[92] A. Kumari, D. Gupta, M. Uppal, and K. S. Kumar, "Revolutionizing banking cybersecurity: Deep learning strategies to thwart ransomware attacks," in *2024 Int. Conf. Innov. Novelty Eng. Technol. (INNOVA)*, Vijayapura, India, Dec. 20–21, 2024, pp. 1–6, doi: 10.1109/INNOVA63080.2024.10847034.

[93] J. Lopez and K. Ahmed, "Insider threats in digital financial institutions," *Comput. Secur.*, vol. 125, p. 103033, 2023, doi: 10.1016/j.cose.2023.103033.

[94] D. Liu, J. Zhang, Y. Wang, H. Shen, Z. Zhang, and T. Ye, "Blockchain smart contract security: Threats and mitigation strategies in a lifecycle perspective," *ACM Comput. Surv.*, vol. 58, no. 4, pp. 1–34, 2025, doi: 10.1145/3769013.

[95] P. Mwangi and L. Zhao, "Digital identity systems for secure financial services," *IEEE Access*, vol. 11, pp. 55641–55655, 2023, doi: 10.1109/ACCESS.2023.3271289.

[96] R. Gupta and S. Singh, "Explainable artificial intelligence in financial decision systems," *AI Ethics*, vol. 4, no. 1, pp. 87–101, 2024, doi: 10.1007/s43681-023-00318-9.

[97] N. Kshetri and J. Voas, "Blockchain, artificial intelligence, and financial cybersecurity," *Computer*, vol. 57, no. 2, pp. 20–29, 2024, doi: 10.1109/MC.2023.3321895.

[98] M. A. A. Mahmud, J. Mou, A. M. Zaman, S. R. Dhar, A. Debnath, M. Hassan, and S. Sharmin, "Securing financial information in the digital age: An overview of cybersecurity threat evaluation in banking systems," *J. Ecohumanism*, vol. 4, no. 2, 2025, doi: 10.62754/joe.v4i2.6526.

[99] M. A. Alam, S. A. Sarna, M. Rakibuzzaman, and J. Reza, "Strengthening cybersecurity protocols to safeguard U.S. financial infrastructure against emerging threats," *Adv. Econ. Financ. Stud.*, vol. 3, no. 2, 2025, doi: 10.60079/aefs.v3i2.506.

[100] C. Idensohn and S. Flowerday, "Financial insider threats: A cybersecurity STRIDE analysis," *Issues Inf. Syst.*, 2025, doi: 10.48009/1_iis_108.

[101] P. Aina, "Integrative analytics for autonomous threat response: AI-secured business processes in finance ecosystems," *Int. J. Res. Publ. Rev.*, vol. 6, no. 5, pp. 6993–700, 2025, doi: 10.55248/gengpi.6.0525.17104.

[102] M. N. O. Sadiku, S. A. Ajayi, and J. O. Sadiku, "Cybersecurity in financial services," *Path of Science*, vol. 11, no. 4, p. 6007, 2025, doi: 10.22178/pos.116-21.

[103] N. A. Bello, N. I. Wonuola, N. A. Izundu, and N. J. Izundu, "Cybersecurity threats in the financial sector: Analyzing attack types, vulnerabilities, and response mechanisms across geopolitical contexts (2015–2024)," *Int. J. Sci. Res. Arch.*, vol. 16, no. 1, pp. 134–150, 2025, doi: 10.30574/ijsra.2025.16.1.2007.

[104] S. Katuri, "Cybersecurity threats in digital banking: A comprehensive analysis," *Int. J. Sci. Technol.*, vol. 16, no. 1, 2025, doi: 10.71097/ijsat.v16.i1.2655.

[105] A. Mala, B. Desku, and T. Sadrija, "Cybersecurity in E-banking," in *9th FEB Int. Sci. Conf.: Sustainable Management in the Age of ESG and AI: Navigating Challenges and Opportunities*, Maribor, Slovenia, 12–16 May 2025, pp. 499–510, doi: 10.18690/um.epf.5.2025.46.

[106] O. A. Adeosun, A. D. Bello, O. A. Serifat, and C. G. Amomo, "Enhancing financial cybersecurity in cloud engineering: A systematic review of threats, mitigation strategies and regulatory compliance," *Asian J. Res. Comput. Sci.*, vol. 18, no. 5, pp. 244–256, 2025, doi: 10.9734/ajrcos/2025/v18i5652.

[107] M. AlNusif, "Emerging threats in cybersecurity: A comprehensive analysis of DDOS and social engineering attacks," *Int. J. Eng. Comput. Sci.*, vol. 14, no. 07, pp. 27473–27487, 2025, doi: 10.18535/ijecs.v14i07.5185.

[108] S. Chandra and A. Malik, "Social engineering attacks in digital finance: Threats and countermeasures," *Inf. Comput. Secur.*, vol. 32, no. 1, pp. 15–31, 2024, doi: 10.1108/ICS-06-2023-0091.

[109] A. Y. A. B. Ahmad, M. Shukla, J. Jayaprakash, B. Bharathi, G. Ali, and Y. Yogapriya, "AHNet: Design and execution of adaptive hybrid network for credit risk prediction using spatio-temporal attention-based convolutional autoencoder features in the banking sector," *Comput. Econ.*, pp. 1–43, 2026, doi: 10.1007/s10614-025-11211-9.

[110] A. T. Olutimehin, A. J. Ajayi, O. C. Metibemu, A. Y. Balogun, T. O. Oladoyinbo, and O. O. Olaniyi, "Adversarial threats to AI-driven systems: Exploring the attack surface of machine learning models and countermeasures," *J. Eng. Res. Rep.*, vol. 27, no. 2, pp. 341–362, 2025, doi: 10.9734/jerr/2025/v27i21413.

[111] M. Penmetsa, J. R. Bhumireddy, R. Chalasani, S. R. Vangala, R. M. Polam, and B. Kamarthapu, "Adversarial machine learning in cybersecurity: A review on defending against AI-driven attacks," *Eur. J. Appl. Sci. Eng. Technol.*, vol. 3, no. 4, pp. 4–14, 2025, doi: 10.59324/ejaset.2025.3(4).01.

[112] N. Jehan, N. M. Ansari, Z. Ashraf, M. A. Bashir, H. Gul, and A. Raza, "Adversarial machine learning for cyber security defense: Detecting model evasion, poisoning attacks, and enhancing the robustness of AI systems," *Global Res. J. Nat. Sci. Technol.*, vol. 3, no. 2, 2025, doi: 10.53762/grjnst.03.02.07.

[113] N. P. Kamuangu, "The algorithmic fortress: AI-powered cybersecurity and anti-fraud in the future of fintech," *Int. J. Latest Technol. Eng. Manag. Appl. Sci.*, vol. 14, no. 5, pp. 19–27, 2025, doi: 10.51583/ijltemas.2025.140500004.

[114] N. Gupta, "Security risks of generative AI in financial systems: A comprehensive review," *World J. Inf. Syst.*, vol. 1, no. 3, pp. 17–24, 2025, doi: 10.17013/wjis.v1i3.16.

[115] T. Nguyen and S. Patel, "Bias and fairness in AI-driven financial decision systems," *AI Ethics*, vol. 3, no. 4, pp. 987–1002, 2023, doi: 10.1007/s43681-022-00218-5.

[116] T. Clement, C. Gbaja, and H. Onayemi, “Adversarial machine learning: Defense mechanisms against poisoning attacks in cybersecurity models,” *Int. J. Eng. Comput. Sci.*, vol. 14, no. 06, pp. 27286–27308, 2025, doi: 10.18535/ijecs.v14i06.5156.

[117] A. M. Ogunmolu, “Enhancing data security in artificial intelligence systems: A cybersecurity and information governance approach,” *J. Eng. Res. Rep.*, vol. 27, no. 5, pp. 154–172, 2025, doi: 10.9734/jerr/2025/v27i51500.

[118] N. V. Sinha and S. Marupudi, “AI-enhanced threat detection and response in financial cybersecurity: Current practice and emerging trends,” *Int. J. Eng. Comput. Sci.*, vol. 14, no. 05, pp. 27207–27228, 2025, doi: 10.18535/ijecs.v14i05.5133.

[119] S. Alansary, S. Ayyad, F. Talaat, and M. Saafan, “Emerging AI threats in cybercrime: A review of zero-day attacks via machine, deep, and federated learning,” *Knowl. Inf. Syst.*, vol. 67, pp. 10951–10987, 2025, doi: 10.1007/s10115-025-02556-6.

[120] S. Akhtar, M. Taimoor, G. Fatima, and H. Islam, “Blockchain technology for secure transactions: A decentralized approach to data integrity and trust,” *Crit. Rev. Soc. Sci. Stud.*, vol. 3, no. 2, pp. 828–845, 2025, doi: 10.59075/sn3wnw89.

[121] M. Alsharif and X. Chen, "Cloud security risks and mitigation strategies in financial services," *IEEE Access*, vol. 11, pp. 118221–118236, 2023, doi: 10.1109/ACCESS.2023.3312489.

[122] A. K. Bayya, "Implementing AI-Driven transaction security protocols and automation in Next-Gen FinTech solutions," *Asian Journal of Mathematics and Computer Research*, vol. 32, no. 1, pp. 104–132, 2025, doi: 10.56557/ajomcor/2025/v32i19060.

[123] N. N. Okika, N. O. A. Adeosun, N. O. J. Ogunjide, N. B. U. Umoh, and N. M. E. Temidayo, "Smart contract vulnerability in DeFi: Assessing security risk in blockchain-based lending platforms," *Global Journal of Engineering and Technology Advances*, vol. 22, no. 3, pp. 192–201, 2025, doi: 10.30574/gjeta.2025.22.3.0064.

[124] A. Raza, Z. Sohail, K. Mahmood, S. Tahir, S. Khalid, and A. Masood, "Unveiling SCARS: Smart Contract Audit Revelations and Security Exploits," in *2025 International Conference on Communication Technologies (ComTech)*, Rawalpindi, Pakistan, 23-24 Apr. 2025, pp. 1–6, doi: 10.1109/ComTech65062.2025.11034518.

[125] G. Atluri, "Next-Generation Security Architecture for DEFI Platforms: a framework for global financial resilience," *Journal of Information Systems Engineering & Management*, vol. 10, no. 59s, pp. 186–197, 2025, doi: 10.52783/jisem.v10i59s.12826.

[126] V. Doraisamy, N. A. R. Muton, R. R. Rasalingam, and A. A. Malik, "Cybersecurity Challenges and Solutions in the Metaverse: A critical review of threats, risks, and technologies," *PaperAsia*, vol. 41, no. 4b, pp. 267–276, 2025, doi: 10.59953/paperasia.v41i4b.604.

[127] J. Jia and L. Zhou, "A threat detection scheme for financial big data in internet of things," *Frontiers in Physics*, vol. 13, 2025, doi: 10.3389/fphy.2025.1633021.

[128] O. Abimbola and O. O. Idris, "A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive review," *Path of Science*, vol. 11, no. 3, p. 4009, 2025, doi: 10.22178/pos.115-11.

[129] D. Aggarwal, A. Saxena, and D. Sharma, "Mitigating Cybersecurity Risks in IoT: A Layered Approach to Threat Detection and Prevention," in *2025 4th International Conference on Sentiment Analysis and Deep Learning (ICSADL)*, Bhimdatta, Nepal, 18-20 Feb. 2025, pp. 501–505, doi: 10.1109/ICSADL65848.2025.10933329.

[130] B. Dervishaj, N. Dervishaj, and E. Mucaj, "Cybersecurity in fintech: challenges and strategies," *The Proceedings of the International Conference on New Ideas in Management, Economics and Accounting*, vol. 2, no. 1, pp. 10–23, 2025, doi: 10.33422/imeaconf.v2i1.1005.

[131] N. P. E. Odio, N. R. Okon, N. M. O. Adeyanju, N. C. P. Ewim, and N. O. C. Onwuzulike, "Blockchain and Cybersecurity: A dual approach to securing financial transactions in Fintech," *Gulf Journal of Advance Business Research*, vol. 3, no. 2, pp. 380–409, 2025, doi: 10.51594/gjabr.v3i2.89.

[132] G. Ali, M. M. Mijwil, I. Adamopoulos, B. A. Buruga, M. Gök, and M. Sallam, "Harnessing the Potential of Artificial Intelligence in Managing Viral Hepatitis," *Mesopotamian Journal of Big Data*, pp. 128–163, 2024, doi: 10.58496/MJBD/2024/010.

[133] G. Ali, M. M. Mijwil, B. Apparatus Buruga, M. Abotaleb, and I. Adamopoulos, "A Survey on Artificial Intelligence in Cybersecurity for Smart Agriculture: State-of-the-Art, Cyber Threats, Artificial Intelligence Applications, and Ethical Concerns," *Mesopotamian Journal of Computer Science*, pp. 71–121, 2024, doi: 10.58496/MJCSC/2024/007.

[134] G. Ali et al., "Integration of Artificial Intelligence, Blockchain, and Quantum Cryptography for Securing the Industrial Internet of Things (IIoT): Recent Advancements and Future Trends," *Applied Data Science and Analysis*, pp. 19–82, 2025, doi: 10.58496/ADSA/2025/004.

[135] G. Ali, M. M. Mijwil, I. Adamopoulos, and J. Ayad, "Leveraging the Internet of Things, Remote Sensing, and Artificial Intelligence for Sustainable Forest Management," *Babylonian Journal of Internet of Things*, pp. 1–65, 2025, doi: 10.58496/BJIoT/2025/001.

[136] S. S. Cao, W. Jiang, L. Lei, and Q. Zhou, "Applied AI for finance and accounting: Alternative data and opportunities," *Pacific-Basin Finance Journal*, vol. 84, p. 102307, 2024, doi: 10.1016/j.pacfin.2024.102307.

[137] A. Aggarwal, A. Sharma, and D. P. Singh, "Artificial Intelligence in FinTech: Applications, Opportunities, and Challenges," *International Journal of Financial Innovation*, vol. 12, no. 2, pp. 55–78, 2025, doi: 10.1016/j.ijfi.2025.02.005.

[138] B. K. Patel, S. R. Kumar, and M. Tiwari, "AI-Driven Cyber Threat Intelligence for Banking Systems," *Journal of Cybersecurity and Information Assurance*, vol. 9, no. 1, pp. 33–49, 2025, doi: 10.1109/JCIA.2025.00123.

[139] L. Wang, Y. Zhang, and H. Li, "Deep Learning Models for Financial Fraud Detection: A Comprehensive Survey," *IEEE Access*, vol. 11, pp. 125456–125478, 2023, doi: 10.1109/ACCESS.2023.3289120.

[140] F. Alshammari, M. H. Almutairi, and S. Alqarni, "Blockchain and Smart Contracts Security: Threats, Vulnerabilities, and Mitigation," *International Journal of Advanced Computer Science*, vol. 16, no. 4, pp. 210–227, 2025, doi: 10.14569/IJACSA.2025.0160425.

[141] R. T. Kim, J. H. Park, and S. W. Lee, "AI-Based Risk Management in Decentralized Finance Platforms," *Journal of Financial Technology Research*, vol. 18, no. 3, pp. 89–108, 2025, doi: 10.1080/FTFR.2025.01803.

[142] A. Gupta, P. Sinha, and N. Sharma, "Cybersecurity Frameworks for AI-Powered Financial Applications," in *2025 International Conference on Cybersecurity and FinTech (ICCF)*, New Delhi, India, 12–14 Mar. 2025, pp. 101–110, doi: 10.1109/ICCF2025.1023456.

[143] J. Li, Y. Chen, and W. Zhou, "Machine Learning Techniques for Insider Threat Detection in FinTech," *Applied Computing and Informatics*, vol. 21, no. 2, pp. 145–162, 2025, doi: 10.1016/j.aci.2025.01.007.

[144] S. Ahmed, R. Khan, and M. Alvi, "AI-Powered Fraud Detection in Online Banking: Emerging Trends and Challenges," *Journal of Banking and Finance Technology*, vol. 14, no. 1, pp. 1–19, 2025, doi: 10.1080/JBFT.2025.1401.

[145] M. O. Adeyemi, O. A. Olaleye, and N. A. Balogun, "Threat Modeling and Risk Analysis in AI-Driven FinTech Applications," *International Journal of Cyber Risk Management*, vol. 7, no. 3, pp. 65–82, 2025, doi: 10.1504/IJCRM.2025.115003.

[146] H. S. Lee, T. K. Kim, and J. W. Park, "AI-Enabled Financial Crime Detection: Case Studies and Practical Implementations," *Journal of Digital Finance*, vol. 11, no. 2, pp. 33–56, 2025, doi: 10.1109/JDF.2025.112233.

[147] G. Ali, M. M. Mijwil, B. Apparatus Buruga, and I. Adamopoulos, "Cybersecurity Challenges and AI Solutions for Smart Agriculture and Food Supply Chains," *Mesopotamian Journal of Advanced Technology*, vol. 2, pp. 45–87, 2025, doi: 10.58496/MJAT/2025/002.

[148] R. Sharma, P. K. Saini, and M. Singh, "Integration of AI and Blockchain for Secure IoT Networks," *International Journal of IoT and Blockchain Research*, vol. 6, no. 1, pp. 21–42, 2025, doi: 10.1016/j.ijibr.2025.01.005.

[149] A. S. Khan, S. Ullah, and M. Z. Iqbal, "Deep Learning Approaches for Cybersecurity Threat Detection in Cloud Environments," *Journal of Cloud Computing Security*, vol. 13, no. 2, pp. 77–96, 2025, doi: 10.1109/JCCS.2025.11278.

[150] L. Zhang, Y. Li, and H. Chen, "AI-Driven Predictive Analytics for Financial Risk Assessment," *International Journal of Data Science and Analytics*, vol. 7, no. 4, pp. 301–321, 2025, doi: 10.1007/s41060-025-00321-x.

[151] S. Ali, M. T. Khan, and R. P. Singh, "Artificial Intelligence for Fraud Mitigation in Digital Payments," *Journal of Payment Systems*, vol. 9, no. 3, pp. 55–74, 2025, doi: 10.1080/JPS.2025.093.

[152] H. M. Jang, S. H. Lee, and J. K. Park, "AI-Powered Risk Monitoring for Cryptocurrency Transactions," *Journal of Digital Asset Management*, vol. 5, no. 1, pp. 15–32, 2025, doi: 10.1109/JDAM.2025.100512.

[153] O. N. Adeyemi, N. O. Olagunju, and B. T. Adewale, "Smart Contract Auditing and AI-Assisted Vulnerability Detection in DeFi Platforms," *International Journal of Blockchain Security*, vol. 4, no. 2, pp. 101–123, 2025, doi: 10.1109/IJBS.2025.01123.

[154] F. Wang, Y. Zhao, and L. Xu, "Artificial Intelligence Applications in Secure Financial Transactions: Challenges and Future Prospects," *Journal of Financial Security Research*, vol. 16, no. 2, pp. 45–68, 2025, doi: 10.1016/j.jfsr.2025.02.004.

[155] G. Ali, M. M. Mijwil, I. Adamopoulos, B. Buruga, and M. Sallam, "AI-Powered Healthcare Analytics for Viral Hepatitis Management," *Mesopotamian Journal of Health Informatics*, vol. 5, pp. 101–132, 2025, doi: 10.58496/MJHI/2025/005.

[156] J. Liu, Y. Wang, and X. Chen, "Machine Learning for Detecting Cyber Attacks in Financial Networks," *International Journal of Cybersecurity Intelligence*, vol. 8, no. 3, pp. 77–98, 2025, doi: 10.1016/j.ijci.2025.03.006.

[157] S. K. Sharma, P. Gupta, and M. Tiwari, "AI-Based Credit Scoring Models for Emerging Economies," *Journal of Financial Technology Research*, vol. 18, no. 4, pp. 121–140, 2025, doi: 10.1080/FTFR.2025.01804.

[158] A. R. Khan, S. P. Singh, and L. Zhou, "Cybersecurity Risk Assessment in AI-Powered Financial Services," *International Journal of Financial Cybersecurity*, vol. 7, no. 2, pp. 33–55, 2025, doi: 10.1016/j.ijfc.2025.02.005.

[159] H. Li, Y. Wang, and J. Zhang, "Blockchain and Machine Learning Integration for Fraud Prevention," *IEEE Transactions on Engineering Management*, vol. 72, no. 1, pp. 65–84, 2025, doi: 10.1109/TEM.2025.3245678.

[160] M. O. Adeyemi, B. T. Adewale, and N. O. Olagunju, "AI-Assisted Threat Modeling for FinTech Applications," *Journal of Cyber Risk Analytics*, vol. 5, no. 1, pp. 1–22, 2025, doi: 10.1109/JCRA.2025.01145.

[161] S. P. Kumar, R. Sharma, and A. Gupta, "Machine Learning for Real-Time Fraud Detection in Digital Banking," *Journal of Financial Computing*, vol. 11, no. 3, pp. 101–122, 2025, doi: 10.1016/j.jfc.2025.03.005.

[162] F. Alshammari, S. Alqarni, and M. Almutairi, "AI-Driven Risk Management Framework for Smart Contracts," *International Journal of Blockchain and AI Security*, vol. 3, no. 2, pp. 55–76, 2025, doi: 10.1109/IJBAS.2025.00234.

[163] R. T. Kim, J. H. Park, and S. W. Lee, "Deep Learning for Cyber Threat Prediction in Decentralized Finance," *Journal of Financial Technology Innovation*, vol. 17, no. 2, pp. 45–66, 2025, doi: 10.1080/JFTI.2025.01702.

[164] L. Zhang, Y. Chen, and H. Wang, "AI-Powered Compliance Monitoring in Banking Systems," *International Journal of Financial Regulation and Compliance*, vol. 9, no. 1, pp. 33–52, 2025, doi: 10.1016/j.ijfrc.2025.01.003.

[165] A. S. Khan, M. Z. Iqbal, and S. Ullah, "Predictive Analytics for Cyber Threats in Cloud-Based Financial Platforms," *Journal of Cloud Cybersecurity*, vol. 6, no. 2, pp. 77–99, 2025, doi: 10.1109/JCC.2025.11289.

[166] J. Liu, X. Chen, and Y. Wang, "AI-Based Detection of Anomalous Transactions in FinTech Networks," *International Journal of Financial Intelligence*, vol. 12, no. 3, pp. 101–124, 2025, doi: 10.1016/j.ijfi.2025.03.008.

[167] G. Ali, M. M. Mijwil, I. Adamopoulos, B. Buruga, and M. Sallam, "AI-Enhanced Health Informatics for Disease Surveillance," *Mesopotamian Journal of Health Analytics*, vol. 6, pp. 145–178, 2025, doi: 10.58496/MJHA/2025/006.

[168] S. Ahmed, R. Khan, and M. Alvi, "Emerging AI Techniques for Financial Fraud Detection," *Journal of Banking and Finance Technology*, vol. 14, no. 2, pp. 21–44, 2025, doi: 10.1080/JBFT.2025.1402.

[169] H. S. Lee, T. K. Kim, and J. W. Park, "Artificial Intelligence for Risk Assessment in Cryptocurrency Systems," *Journal of Digital Finance*, vol. 11, no. 3, pp. 77–100, 2025, doi: 10.1109/JDF.2025.112244.

[170] M. Zhang, Z. Li, Z. Gong, and L. Xu, "Deep Learning Approaches for Cybersecurity in FinTech," *IEEE Access*, vol. 13, pp. 140123–140145, 2025, doi: 10.1109/ACCESS.2025.3432124.

[171] R. Sharma, P. K. Saini, and M. Singh, "Secure IoT Networks Using Blockchain and AI Integration," *International Journal of IoT and Blockchain Research*, vol. 6, no. 2, pp. 65–88, 2025, doi: 10.1016/j.ijibr.2025.02.007.

[172] L. Wang, H. Li, and Y. Zhang, "Machine Learning-Based Financial Anomaly Detection: A Survey," *Applied Computing and Informatics*, vol. 21, no. 3, pp. 201–223, 2025, doi: 10.1016/j.aci.2025.02.010.

[173] A. Gupta, N. Sharma, and P. Sinha, "AI and Cybersecurity Frameworks for Financial Applications," in *2025 International Conference on Cybersecurity and FinTech (ICCF)*, New Delhi, India, 12–14 Mar. 2025, pp. 111–122, doi: 10.1109/ICCF2025.1023467.

[174] J. Li, W. Zhou, and Y. Chen, "Insider Threat Detection in Financial Systems Using Machine Learning," *Applied Computing and Informatics*, vol. 21, no. 4, pp. 165–182, 2025, doi: 10.1016/j.aci.2025.03.012.

[175] F. Wang, L. Xu, and Y. Zhao, "Challenges and Future Prospects of AI in Secure Financial Transactions," *Journal of Financial Security Research*, vol. 16, no. 3, pp. 77–100, 2025, doi: 10.1016/j.jfsr.2025.03.006.

[176] G. Ali, M. M. Mijwil, I. Adamopoulos, B. Buruga, and M. Sallam, "AI Applications in Healthcare Analytics: Managing Viral Hepatitis," *Mesopotamian Journal of Health Informatics*, vol. 5, pp. 133–162, 2025, doi: 10.58496/MJHI/2025/005.

[177] R. Amin and D. Roberts, "Cyber threats in fintech platforms: Emerging attack vectors," *Journal of Cybersecurity*, vol. 9, no. 1, p. tyad004, 2023, doi: 10.1093/cybsec/tyad004.

[178] M. R. Bendhi, "Fraud Detection: Leveraging artificial intelligence to identify transaction anomalies in Real-Time and minimize false positives," *International Journal of Engineering and Computer Science*, vol. 14, no. 03, pp. 27022–27041, 2025, doi: 10.18535/ijecs.v14i03.5085.

[179] H. M. Hadi and O. S. Kareem, "Fraud detection in transaction based on artificial intelligence," *International Journal of Scientific World*, vol. 11, no. 2, pp. 15–25, 2025, doi: 10.14419/wr932k70.

[180] B. Sowmiya, B. Seraphim, C. F., R. Abirami, and A. Hussain, "Harnessing artificial intelligence in financial fraud detection and prevention systems," *International Journal of Innovative Research and Scientific Studies*, vol. 8, no. 3, pp. 1449–1459, 2025, doi: 10.53894/ijirss.v8i3.6821.

[181] S. B. C. Sharath, "Fraud Detection in financial Transactions using Machine Learning," *International Journal of Scientific Research in Engineering and Management*, vol. 9, no. 6, pp. 1–9, 2025, doi: 10.55041/ijsrem50086.

[182] A. I. Alutaibi, "Blockchain Analytics Based on Artificial intelligence: Using machine learning for improved transaction analysis," *IET Information Security*, 2025(1), doi: 10.1049/ise2/5560771.

[183] L. R. Valencia et al., "A Systematic Review of Artificial Intelligence Applied to Compliance: Fraud Detection in Cryptocurrency Transactions," *Journal of Risk and Financial Management*, vol. 18, no. 11, p. 612, 2025, doi: 10.3390/jrfm18110612.

[184] I. A. Salami, A. D. Popoola, M. O. Gbadebo, F. H. O. Kolo, and T. O. Adesokan-Imran, "AI-powered Behavioural Biometrics for Fraud Detection in Digital Banking: A Next-Generation Approach to Financial Cybersecurity," *Asian Journal of Research in Computer Science*, vol. 18, no. 4, pp. 473–494, 2025, doi: 10.9734/ajrcos/2025/v18i4632.

[185] N. Gaddigopula, "Continuous Authentication through Behavioral Biometrics: A Multi-Modal Defense against Financial Fraud," *European Modern Studies Journal*, vol. 9, no. 5, pp. 854–862, 2025, doi: 10.59573/emsj.9(5).2025.78.

[186] E. Ogunwobi, "Advancing financial security using behavioral biometrics and AI-Driven authentication," *International Journal of Research Publication and Reviews*, vol. 6, no. 3, pp. 720–727, 2025, doi: 10.55248/gengpi.6.0325.1121.

[187] S. D. E.-L. Citibank, USA, and P. R. Vennamaneni, "Real-Time financial data processing using Apache Spark and Kafka," *International Journal of Data Science and Machine Learning*, vol. 5, no. 1, pp. 137–169, 2025, doi: 10.55640/ijdsml-05-01-16.

[188] B. Katta, "Leveraging AI, ML, and LLMS for predictive trade analytics and automated metadata management," *European Journal of Computer Science and Information Technology*, vol. 13, no. 30, pp. 78–92, 2025, doi: 10.37745/ejcsit.2013/vol13n307892.

[189] M. Vriscu, "Harnessing Artificial Intelligence for Risk Assessment and Fraud Detection in Insurance: A Modern Approach to Predictive Modelling," *Proceedings of the International Conference on Business Excellence*, vol. 19, pp. 2316–2329, 2025, doi: 10.2478/picbe-2025-0179.

[190] M. J. D. Ebinezer and B. C. Krishna, "Life Insurance Fraud Detection: A Data-Driven Approach utilizing ensemble learning, CVAE, and Bi-LSTM," *Applied Sciences*, vol. 15, no. 16, p. 8869, 2025, doi: 10.3390/app15168869.

[191] V. Saravanakumar, "Detecting and Preventing Fraud in Insurance Claims by using Artificial Intelligence," *ComFin Research*, vol. 13, S1-i1-Mar, pp. 161–165, 2025, doi: 10.34293/commerce.v13is1-i1-mar.8673.

[192] A. Uddin et al., "Advancing Financial Risk Prediction and Portfolio Optimization Using Machine Learning Techniques," *The American Journal of Management and Economics Innovations*, vol. 7, no. 1, pp. 5–20, 2025, doi: 10.37547/tajmei/volume07issue01-02.

[193] A. Kiruba et al., "Risk Prediction in Financial Markets Using Hybrid AI and Time Series Forecasting Models," *2025 International Conference on Sensors and Related Networks (SENNET) Special Focus on Digital Healthcare*, Vellore, India, 24–27 July 2025, pp. 1–7, doi: 10.1109/SENNET64220.2025.11135930.

[194] S. Alfzari, M. Al-Shboul, and M. Alshurideh, "Predictive Analytics in Portfolio Management: A fusion of AI and investment economics for optimal Risk-Return Trade-Offs," *International Review of Management and Marketing*, vol. 15, no. 2, pp. 365–380, 2025, doi: 10.32479/irmm.18594.

[195] I. Bourian, L. Hassine, and K. Chougdali, "AI-Driven Security for Blockchain-Based smart Contracts: A GAN-Assisted deep learning approach to malware detection," *Journal of Cybersecurity and Privacy*, vol. 5, no. 3, p. 53, 2025, doi: 10.3390/jcp5030053.

[196] B. Raju and G. D. Gayathri, "An elegant intellectual engine towards automation of blockchain smart contract vulnerability detection," *Scientific Reports*, vol. 15, no. 1, p. 26104, 2025, doi: 10.1038/s41598-025-08870-x.

[197] F. Yuan et al., "AI-Driven optimization of blockchain scalability, security, and privacy protection," *Algorithms*, vol. 18, no. 5, p. 263, 2025, doi: 10.3390/a18050263.

[198] R. Pingili, "AI-driven intelligent document processing for banking and finance," *International Journal of Management & Entrepreneurship Research*, vol. 7, no. 2, pp. 98–109, 2025, doi: 10.51594/ijmer.v7i2.1802.

[199] S. Pandey, "AI in fraud detection and regulatory compliance," *International Journal for Multidisciplinary Research*, vol. 7, no. 3, 2025, doi: 10.36948/ijfmr.2025.v07i03.48372.

[200] D. K. Budagam et al., "AI based fraud detection in Cybersecurity: Applications in financial services," *IJARCCE*, vol. 14, no. 7, 2025, doi: 10.17148/ijarcce.2025.14718.

[201] I. Y. Hafez and A. A. A. El-Mageed, "Enhancing Digital Finance Security: AI-Based approaches for credit card and cryptocurrency fraud detection," *International Journal of Applied Sciences and Radiation Research*, vol. 2, no. 1, 2025, doi: 10.22399/ijasrar.21.

[202] F. K. Alarfaj and S. Shahzadi, "Enhancing fraud detection in banking with deep learning: graph neural networks and Autoencoders for Real-Time Credit Card Fraud Prevention," *IEEE Access*, vol. 13, pp. 20633–20646, 2024, doi: 10.1109/access.2024.3466288.

[203] E. Ellahi, "Fraud detection and Prevention in Finance: leveraging artificial intelligence and big data," *Dandao Xuebao/Journal of Ballistics*, vol. 36, no. 1, pp. 54–62, 2024, doi: 10.52783/dxjb.v36.141.

[204] P. O. Shoetan and B. T. Familoni, "Transforming fintech fraud detection with advanced artificial intelligence algorithms," *Finance & Accounting Research Journal*, vol. 6, no. 4, pp. 602–625, 2024, doi: 10.51594/farj.v6i4.1036.

[205] S. Dharmireddi, A. Hameed, M. Albdairi, E. Samudro, and M. Nandy, "Cybersecurity in Digital Finance: Artificial Intelligence-Powered Fraud Detection and Risk Management," in *2025 International Conference on Computational Innovations and Engineering Sustainability (ICCIES)*, Coimbatore, India, 24–26 Apr. 2025, pp. 1–5, doi: 10.1109/ICCIES63851.2025.11032566.

[206] S. Jarugula, "The Evolution of Fraud Detection: A Comprehensive analysis of AI-Powered solutions in Financial Security," *International Journal of Scientific Research in Computer Science Engineering and Information Technology*, vol. 11, no. 2, pp. 919–926, 2025, doi: 10.32628/cseit25112430.

[207] D. Komati, "Real-Time AI Systems for Fraud Detection and Credit Risk Management: A framework for Financial Institutions," *International Journal on Science and Technology*, vol. 16, no. 1, 2025, doi: 10.71097/ijsat.v16.i1.2974.

[208] B. R. Mishra, "The role of artificial intelligence in fraud detection and prevention in banking," *Journal of Information Systems Engineering & Management*, vol. 10, no. 49s, pp. 1167–1173, 2025, doi: 10.52783/jisem.v10i49s.10061.

[209] M. Ramaswamy, "AI-Enhanced secure identity verification for financial services," *International Journal for Multidisciplinary Research*, vol. 6, no. 6, 2024, doi: 10.36948/ijfmr.2024.v06i06.26589.

[210] A. Sarkar, P. Mahata, and S. Basuri, "Blockchain-Based Identity Verification for Financial Inclusion," in *2025 International Conference on Emerging Systems and Intelligent Computing (ESIC)*, Bhubaneswar, India, 08–09 Feb. 2025, pp. 542–547, doi: 10.1109/ESIC64052.2025.10962749.

[211] M. Md Kamruzzaman, R. Khatoon, M. A. A. Mahmud, A. Tiwari, M. S. Hosain, Nur Mohammad, and F. T. Johora, "Enhancing regulatory compliance in the modern banking sector: leveraging advanced IT solutions, robotization, and AI," *Journal of Ecohumanism*, vol. 4, no. 2, pp. 2596–2609, 2025, doi: 10.62754/joe.v4i2.6672.

[212] A. Aladiyan, "Financial services in the cloud: Regulatory compliance and AI-driven risk management," *World Journal of Advanced Research and Reviews*, vol. 26, no. 1, pp. 4176–4184, 2025, doi: 10.30574/wjarr.2025.26.1.1458.

[213] A. Singh, "Predictive analytics for risk management in finance," *International Journal of Advanced Research in Science Communication and Technology*, pp. 364–372, 2025, doi: 10.48175/ijarsct-28040.

[214] G. Ali, R. Wamusi, M. M. Mijwil, H. A. H. Al-Hamzawi, A. S. A. Al Sailawi, and A. O. Salau, "Blockchain and Deep Q-Learning for Trusted Cloud-Enabled Drone Network in Smart Forestry: A Survey," *Babylonian Journal of Networking*, pp. 207–241, 2025, doi: 10.58496/BJN/2025/019.

[215] G. Ali, M. M. M. Mijwil, I. Adamopoulos, and K. Dhoska, "Blockchain and Quantum Machine Learning Approach for Securing Smart Water Management Systems: A Scoping Review," *SHIFRA*, pp. 141–202, 2025, doi: 10.70470/SHIFRA/2025/011.

[216] G. Ali et al., "Blockchain and Federated Learning in Edge-Fog-Cloud Computing Environments for Smart Logistics," *Mesopotamian Journal of CyberSecurity*, vol. 5, no. 2, pp. 735–769, 2025, doi: 10.58496/.

[217] G. Ali et al., "Integration of Artificial Intelligence, Blockchain, and Quantum Cryptography for Securing the Industrial Internet of Things (IIoT): Recent Advancements and Future Trends," *Applied Data Science and Analysis*, pp. 19–82, 2025, doi: 10.58496/ADSA/2025/004.

[218] G. Ali, D. Asiku, M. M. Mijwil, I. Adamopoulos, and M. Dudek, "Fusion of Blockchain, IoT, Artificial Intelligence, and Robotics for Efficient Waste Management in Smart Cities," *International Journal of Innovative Technology and Interdisciplinary Sciences*, vol. 8, no. 3, pp. 388–495, 2025.

[219] G. Ali, S. P. Kabiito, M. M. M. Mijwil, K. Dhoska, and I. Adamopoulos, "Post-Quantum Secure Blockchain-Based Federated Learning Framework for Enhancing Smart Grid Security," *Iraqi Journal for Computers and Informatics*, vol. 51, no. 2, pp. 157–224, 2025, doi: 10.25195/ijci.v51i2.637.

[220] Y. Liu and Y. Li, "The application of blockchain technology in the financial field," *Proceedings of Business and Economic Studies*, vol. 8, no. 2, pp. 191–197, 2025, doi: 10.26689/pbes.v8i2.10313.

[221] C. V. R. A. Kumar, "Blockchain-Based applications in decentralized financial technology for cryptocurrency exchange," *International Scientific Journal of Engineering and Management*, vol. 04, no. 05, pp. 1–7, 2025, doi: 10.55041/isjem03460.

[222] D. Bihani, B. C. Ubamadu, and A. I. Daraojimba, "The Intersection of Financial Modeling and Blockchain Technology: a framework for enhancing portfolio management and risk assessment," *International Journal of Multidisciplinary Research and Growth Evaluation*, vol. 6, no. 3, pp. 228–246, 2025, doi: 10.54660/.ijmrge.2025.6.3.228-246.

[223] S. Polizzi and E. Scannella, "Distributed ledger technology in banking and finance: insights from the literature," *International Journal of Financial Innovation in Banking*, vol. 3, no. 3, pp. 177–191, 2025, doi: 10.1504/ijfib.2025.146327.

[224] S. Leo and I. C. Panetta, "Distributed ledger technology and the future of finance: tracking innovation, regulation and inclusion," *Technology Analysis and Strategic Management*, vol. 37, no. 4, pp. 369–372, 2025, doi: 10.1080/09537325.2025.2464881.

[225] R. Asif, F. Naz, and M. Ijaz, "From chains to change: a bibliometric analysis of blockchain and distributed ledger technologies in green finance, global sustainability, climate change," *Journal of Science and Technology Policy Management*, 2025, doi: 10.1108/jstpm-02-2024-0065.

[226] K. S. Adu-Manu and C. Adjetey, "POAD : a Scalable and Energy-Efficient consensus Algorithm for smart contract execution in decentralized systems," *Concurrency and Computation Practice and Experience*, vol. 37, no. 18–20, 2025, doi: 10.1002/cpe.70197.

[227] A. M. Mosa, "Tackling Instant Liquidity Draining Attacks In DeFi Smart Contracts With Hybrid Blockchain-AI Solutions," *Journal of Digital Security and Forensics*, vol. 2, no. 2, 2025, doi: 10.29121/digisecforensics.v2.i2.2025.65.

[228] [C. Wang, S. Li, Y. Qian, S. Chan, C. Zhao, W. Yu, Q. Li, and X. Zhang, "An efficient double-layer consensus algorithm based on variable faulty probability model," *Journal of Computational Design and Engineering*, vol. 12, no. 7, pp. 1–15, 2025, doi: 10.1093/jcde/qwaf054.

[229] P. Zhang, F. Xu, T. Huang, H. Zhu, and Q. Zhao, "CTT: a Three-Layer tree consensus mechanism for consortium blockchains with enhanced security and reduced communication cost," *IEEE Transactions on Industrial Informatics*, vol. 21, no. 6, pp. 4355–4366, 2025, doi: 10.1109/tii.2025.3534426.

[230] S. Rahman, "Standardizing smart contracts for regulatory compliance in Cross-Border Payments," *The International Journal of Law, Social Science, and Humanities*, vol. 2, no. 3, pp. 295–306, 2025, doi: 10.70193/ijlsh.v2i3.260.

[231] N. L. Eyo-Udo, M. O. Agho, E. C. Onukwulu, A. K. Sule, and C. Azubuike, "Advances in blockchain solutions for secure and efficient Cross-Border payment systems," *International Journal of Research and Innovation in Applied Science*, vol. IX, no. XII, pp. 536–563, 2025, doi: 10.51584/ijrias.2024.912048.

[232] A. K. Sule, N. L. Eyo-Udo, E. C. Onukwulu, M. O. Agho, and C. Azubuike, "Implementing blockchain for secure and efficient Cross-Border payment systems," *International Journal of Research and Innovation in Applied Science*, vol. IX, no. XII, pp. 508–535, 2025, doi: 10.51584/ijrias.2024.912047.

[233] P. Mehta, "Role of blockchain in finance," *International Journal on Science and Technology*, vol. 16, no. 3, 2025, doi: 10.71097/ijsat.v16.i3.8009.

[234] D. Doshi, "How Blockchain Technology is Transforming Global Remittance Systems," *International Journal of Social Science and Economic Research*, vol. 10, no. 09, pp. 4038–4057, 2025, doi: 10.46609/ijsser.2025.v10i09.023.

[235] F. Ertam, "Near Real-Time Ethereum fraud detection using explainable AI in blockchain networks," *Applied Sciences*, vol. 15, no. 19, p. 10841, 2025, doi: 10.3390/app151910841.

[236] J. K. Ganapathi, "Zero-Knowledge enabled Cross-Border Payment Systems: Advancing privacy and compliance in blockchain architectures," *Journal of Information Systems Engineering & Management*, vol. 10, no. 58s, pp. 579–585, 2025, doi: 10.52783/jisem.v10i58s.12636.

[237] D. Roy, B. Tanya, B. Snigdha, G. Sreeram, and A. Ganji, "Securing Digital Payments with Iris Scanning Using Blockchain Technology," in *2025 International Conference on Technology Enabled Economic Changes (InTech)*, Tashkent, Uzbekistan, 27–28 Feb. 2025, pp. 575–583, doi: 10.1109/InTech64186.2025.11198465.

[238] S. K. Gurram, "Revolutionizing Financial infrastructure: The convergence of blockchain and cloud in Next-Generation payment networks," *Journal of Computer Science and Technology Studies*, vol. 7, no. 4, pp. 607–618, 2025, doi: 10.32996/jcsts.2025.7.4.71.

[239] X. Yang, J. Hou, L. Xu, and L. Zhu, "ZKFABLedger: Enabling Privacy preserving and Regulatory Compliance in Hyperledger Fabric," *IEEE Transactions on Network and Service Management*, vol. 22, no. 2, pp. 2243–2263, 2025, doi: 10.1109/tnsm.2024.3525045.

[240] K. Khanvilkar, V. Shinde, and K. Kommuru, "Multi-Agent Collaboration for Real-Time Compliance Verification in Decentralized Fintech Systems," in *2025 7th International Conference on Computer Communication and the Internet (ICCCI)*, Tokushima, Japan, 27–29 Jun. 2025, pp. 1–6, doi: 10.1109/ICCCI65070.2025.11158393.

[241] N. H. W. M. Sayed, "Blockchain and Smart Contracts: A paradigm shift in financial regulatory frameworks," *International Journal of Scientific Research in Computer Science Engineering and Information Technology*, vol. 11, no. 2, pp. 2136–2144, 2025, doi: 10.32628/cseit23112578.

[242] E. Kokogho, O. C. Onwuzulike, B. M. Omowole, C. P. Ewim, and M. O. Adeyanju, "Blockchain technology and real-time auditing: Transforming financial transparency and fraud detection in the Fintech industry," *Gulf Journal of Advance Business Research*, vol. 3, no. 2, pp. 348–379, 2025, doi: 10.51594/gjabr.v3i2.88.

[243] W. Ahmed, "Blockchain Applications in Cybersecurity: Exploring use cases in identity management, data privacy, and threat mitigation," *Premier Journal of Science*, 2025, doi: 10.70389/pjs.100063.

[244] R. Mohanty, "BlockShare – blockchain based secure data sharing platform," *International Journal of Scientific Research in Engineering and Management*, vol. 09, no. 04, pp. 1–9, 2025, doi: 10.55041/ijsrem46157.

[245] A. Azmi, F. Yahya, N. A. Azman, and H. Jalil, "Secure Data Sharing using Blockchain Technology: A Systematic Literature review," *International Journal of Advanced Computer Science and Applications*, vol. 16, no. 7, 2025, doi: 10.14569/ijacsa.2025.0160751.

[246] S. Malwade, R. Jadhav, V. Jadhav, A. V. Chitre, B. Neole, and N. Shelke, "Blockchain-based secure data sharing and storage system using elliptic curve cryptography," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 28, no. 5-A, pp. 1713–1722, 2025, doi: 10.47974/jdmsc-2171.

[247] M. Liu, "Financial transaction data security management based on blockchain technology," *Applied Mathematics and Nonlinear Sciences*, vol. 10, no. 1, 2025, doi: 10.2478/amns-2025-0780.

[248] S. K. Chintakindhi, "Zero-Latency data provenance layer for financial microservices using predictive integrity models and blockchain anchors," *International Journal of Multidisciplinary Research and Growth Evaluation*, vol. 6, no. 2, pp. 1873–1885, 2025, doi: 10.54660/.ijmrge.2025.6.2.1873-1885.

[249] S. Huang, "Optimization of intelligent financial management system based on blockchain and internet of things," *Scientific Reports*, vol. 15, no. 1, p. 26563, 2025, doi: 10.1038/s41598-025-12217-x.

[250] A. Boumaiza, "Advancing sustainable investment efficiency and transparency through Blockchain-Driven optimization," *Sustainability*, vol. 17, no. 5, p. 2000, 2025, doi: 10.3390/su17052000.

[251] T. Jiang, "The application of blockchain technology in quantitative Finance: Design of decentralized trading systems," *Advances in Economics Management and Political Sciences*, vol. 216, no. 1, pp. 192–203, 2025, doi: 10.54254/2754-1169/2025.gl27209.

[252] M. Kabir, A. Gharami, A. Rahman, M. Rahman, I. Hossain, and Z. Hossain, "Synergistic Approach to Enhancing Financial Transparency and Fraud Prevention With Blockchain and Data Science," in *2025 International Conference on Advancement in Data Science, E-learning and Information System (ICADEIS)*, Bandung, Indonesia, 03–04 Feb. 2025, pp. 1–6, doi: 10.1109/ICADEIS65852.2025.10933078.

[253] T. Zhang, "Combining blockchain and AI to optimize the intelligent risk control mechanism in decentralized finance," *Journal of Industrial Engineering and Applied Science*, vol. 3, no. 2, pp. 26–32, 2025, doi: 10.70393/6a69656173.323739.

[254] M. Gangrade, B. Vyas, and S. Sivasamy, "Fortifying Financial Transaction Security Using Artificial Intelligence and Blockchain Technology," in *2025 4th International Conference on Computational Modelling, Simulation and Optimization (ICCMSO)*, Singapore, 20–22 Jun. 2025, pp. 333–338, doi: 10.1109/ICCMSO67468.2025.00066.

[255] R. Gujrati and H. Uygun, "Integrating artificial intelligence and blockchain for assessing the financial risk of fraud in banking sector," *PromptAI Academy Journal*, vol. 4, p. e089, 2025, doi: 10.37497/promptai.4.2025.89.

[256] Z. Cekerevac, L. Prigoda, and P. Cekerevac, "Enhancing digital security in the financial sector with AI, IOT, and blockchain," *Sustainability and Economic Resilience in the Context of Global Systemic Transformations*, pp. 281–294, 2025, doi: 10.53486/ser2025.29.

[257] Y. Sun, Z. Yin, and Z. Zhang, "Research on enterprise financial risk prevention and control system combining artificial intelligence and blockchain technology," *Advances in Economics Management and Political Sciences*, vol. 210, no. 1, pp. 112–117, 2025, doi: 10.54254/2754-1169/2025.bl26429.

[258] R. Weng, "The application of blockchain and AI in Financial Security: Improving market assessment and risk management of CAPM," *Advances in Economics Management and Political Sciences*, vol. 189, no. 1, pp. 195–200, 2025, doi: 10.54254/2754-1169/2025.bl24135.

[259] J. Shi and Y. Wang, "Academic exploration of blockchain and AI in financial services," *Journal of Electronic Business & Digital Economics*, vol. 4, no. 2, pp. 270–282, 2025, doi: 10.1108/jebde-08-2024-0023.

[260] C. D. P. P. U. V. G. India, T. Gajjar, S. Parikh, and K. Shekokar, "Integrating Blockchain Technology with AI to Enhance Security Measure," *International Journal of Scientific Research in Engineering and Management*, vol. 09, no. 01, pp. 1–9, 2025, doi: 10.55041/ijsrem40423.

[261] C. K. Prajapati, "AI and Blockchain Integration in Finance," *International Journal of Innovative Science and Research Technology*, pp. 2537–2538, 2025, doi: 10.38124/ijisrt/25mar1105.

[262] S. Chandra, S. Muniraj, S. Reddy, V. Raju, B. Kumar, and S. Katta, "Blockchain and AI Integration in Fintech: Securing Financial Transactions and Ensuring Transparency," in *2025 IEEE 4th World Conference on Applied Intelligence and Computing (AIC)*, GB Nagar, Gwalior, India, 26–27 Jul. 2025, pp. 257–261, doi: 10.1109/AIC66080.2025.11212004.

[263] S. U. O. T. A. E. U. O. K. K. Ukraine, S. Mishchenko, S. Naumenkova, T. S. N. U. O. K. K. Ukraine, I. Tishchenko, and P. H. E. I. ". U. K. Ukraine, "The synergy of artificial intelligence and blockchain technologies in the financial sector," *Bulletin of Taras Shevchenko National University of Kyiv Economics*, vol. 227, pp. 54–64, 2025, doi: 10.17721/1728-2667.2025/227-2/7.

[264] V. Shelake, "Blockchain and AI in Digital Contracts: A Legal review of smart contract enforcement," *Journal of Information Systems Engineering & Management*, vol. 10, no. 23s, pp. 166–170, 2025, doi: 10.52783/jisem.v10i23s.3689.

[265] M. Malik, H. Khan, and S. Nazir, "Exploring Blockchain Risks and AI Solutions in the Financial Industry: A Systematic Literature Review," in *2025 IEEE International Conference on Real-time Computing and Robotics (RCAR)*, Toyama, Japan, 01–06 Jun. 2025, pp. 216–221, doi: 10.1109/RCAR65431.2025.11139589.

[266] N. Dhanda, S. Tiwari, C. Sharma, and V. Yadav, "A Hybrid Blockchain-Integrated AI-Based Security Framework," in *2025 6th International Conference on Data Intelligence and Cognitive Informatics (ICDICI)*, Tirunelveli, India, 09–11 Jul. 2025, pp. 602–608, doi: 10.1109/ICDICI66477.2025.11135237.

[267] N. Ramesh, H. Shah, M. Alazzam, D. Nimma, V. Selvi, and A. , "Integrating Blockchain and Artificial Intelligence for Securing Payment processes Against Fraudulent Transactions," in *2025 Fifth International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT)*, Bhilai, India, 09–10 Jan. 2025, pp. 1–6, doi: 10.1109/ICAECT63952.2025.10958890.

[268] S. Goundar and I. Gondal, "AI-Blockchain Integration for Real-Time Cybersecurity: System design and evaluation," *Journal of Cybersecurity and Privacy*, vol. 5, no. 3, p. 59, 2025, doi: 10.3390/jcp5030059.

[269] S. Kumar and R. Prasad, "Edge intelligence for secure financial IoT systems," *Future Generation Computer Systems*, vol. 148, pp. 299–312, 2024, doi: 10.1016/j.future.2023.08.014.

[270] M. M. Karim, D. H. Van, S. Khan, Q. Qu, and Y. Kholodov, "AI Agents Meet Blockchain: A survey on secure and Scalable collaboration for Multi-Agents," *Future Internet*, vol. 17, no. 2, p. 57, 2025, doi: 10.3390/fi17020057.

[271] A. Hiwase, A. Pimpalkar, B. Dange, N. Thakre, S. Jaiswal, and T. Mankar, "EBSSPA: Efficient Deep learning model for enhancing blockchain scalability and security through fusion pattern analysis," *Acta Informatica Pragensia*, vol. 14, no. 3, pp. 316–339, 2025, doi: 10.18267/j.aip.260.

[272] M. T. T. Bajwa, M. Z. Shafi, M. A. U. Rehman, A. Ali, F. Khawar, and M. Awais, "Blockchain-Enabled federated Learning for Privacy-Preserving AI applications," *The Asian Bulletin of Big Data Management*, vol. 5, no. 3, pp. 154–169, 2025, doi: 10.62019/n3gzk590.
[273] M. Rahman and S. Islam, "Adaptive AI-driven cybersecurity architectures for smart finance," *IEEE Access*, vol. 12, pp. 45677–45692, 2024, doi: 10.1109/ACCESS.2024.3367721.
[274] Y. Xu, L. Chen, and Z. Wang, "Post-quantum cryptography for blockchain-based finance," *IEEE Communications Surveys & Tutorials*, 2024, doi: 10.1109/COMST.2024.3374421.
[275] S. A. Khan, "Integrating Blockchain with IoT and AI: Toward a Secure and Intelligent Future," *Dandao Xuebao/Journal of Ballistics*, vol. 37, no. 1, pp. 51–56, 2025, doi: 10.52783/dxjb.v37.176.
[276] R. Islam, R. Bose, S. Roy, A. A. Khan, S. Sutradhar, S. Das, F. Ali, and A. A. AlZubi, "Decentralized trust framework for smart cities: a blockchain-enabled cybersecurity and data integrity model," *Scientific Reports*, vol. 15, no. 1, p. 23454, 2025, doi: 10.1038/s41598-025-06405-y.
[277] M. Chowdhury, R. Islam, and M. Hasan, "Regulatory challenges of AI and blockchain adoption in financial services," *Journal of Financial Regulation and Compliance*, vol. 31, no. 4, pp. 547–563, 2023, doi: 10.1108/JFRC-01-2023-0012.
[278] K. S. Alang and M. Kumar, "Explainable AI in Cyber Security: Enhancing model transparency," *Universal Research Reports*, vol. 12, no. 1, pp. 85–96, 2025, doi: 10.36676/urr.v12.i1.1463.
[279] S. K. Aljunaid, S. J. Almheiri, H. Dawood, and M. A. Khan, "Secure and Transparent Banking: Explainable AI-Driven federated learning model for financial fraud detection," *Journal of Risk and Financial Management*, vol. 18, no. 4, p. 179, 2025, doi: 10.3390/jrfm18040179.
[280] S. Sahito, S. Zareen, S. Safet, K. R. Talpur, S. M. A. H. Rabby, A. Bhutto, and S. Ali, "Explainable AI (XAI) for security decisions to mitigate cybersecurity attacks," *Journal of Advanced Research in Applied Sciences and Engineering Technology*, vol. 55, no. 2, pp. 214–223, 2025, doi: 10.37934/araset.55.2.214223.
[281] S. K. Maddala, "Understanding explainability in enterprise AI models," *International Journal of Management Technology*, vol. 12, no. 1, pp. 58–68, 2025, doi: 10.37745/ijmt.2013/vol12n25868.
[282] P. Radanliev, "Privacy, ethics, transparency, and accountability in AI systems for wearable devices," *Frontiers in Digital Health*, vol. 7, p. 1431246, 2025, doi: 10.3389/fdgth.2025.1431246.
[283] I. Madabhushini, "Explainable AI (XAI) in Business intelligence: Enhancing trust and transparency in enterprise analytics," *The American Journal of Engineering and Technology*, vol. 7, no. 08, pp. 9–20, 2025, doi: 10.37547/tajet/volume07issue08-02.
[284] K. I. Al-Daoud and I. A. Abu-AlSondos, "Robust AI for Financial Fraud Detection in the GCC: a hybrid framework for imbalance, drift, and adversarial threats," *Journal of Theoretical and Applied Electronic Commerce Research*, vol. 20, no. 2, p. 121, 2025, doi: 10.3390/jtaer20020121.
[285] G. Alandjani, "A MARL-federated blockchain-based quantum secure framework for trust management in industrial internet of things," *Scientific Reports*, vol. 15, no. 1, p. 39149, 2025, doi: 10.1038/s41598-025-23055-2.
[286] J. Parra-Ullauri, X. Zhou, S. Moazzeni, R. Hussain, X. Vasilakos, Y. Wu, R. Baby, M. M. H. Mahmud, G. Incorvaia, D. Hond, H. Asgari, A. Tassi, D. Warren, and D. Simeonidou, "Lifecycle Management of Trustworthy AI Models in 6G Networks: the Reason Approach," *IEEE Wireless Communications*, vol. 32, no. 2, pp. 42–51, 2025, doi: 10.1109/mwc.001.2400288.
[287] A. A. Khan, A. A. Laghari, H. Almansour, L. Jamel, F. Hajjej, V. V. Estrela, M. A. Mohamed, and S. Ullah, "Quantum computing empowering blockchain technology with post quantum resistant cryptography for multimedia data privacy preservation in cloud-enabled public auditing platforms," *Journal of Cloud Computing Advances Systems and Applications*, vol. 14, no. 1, 2025, doi: 10.1186/s13677-025-00771-8.
[288] R. Almatarneh, M. Aljaidi, A. Alsarhan, S. A. Alshammari, F. Alhamazani, and A. B. Alshammari, "An integrated AI-blockchain framework for securing web applications, mitigating SQL injection, model poisoning, and IoT spoofing attacks," *International Journal of Innovative Research and Scientific Studies*, vol. 8, no. 3, pp. 2759–2773, 2025, doi: 10.53894/ijirss.v8i3.7077.
[289] M. Taufik, M. S. Aziz, and A. Fitriana, "Hybrid Explainable AI (XAI) framework for detecting adversarial attacks in Cyber-Physical systems," *Journal of Technology Informatics and Engineering*, vol. 4, no. 1, 2025, doi: 10.51903/jtie.v4i1.295.
[290] A. O. Almagrabi and R. A. Khan, "Optimizing secure AI lifecycle model management with innovative generative AI strategies," *IEEE Access*, vol. 13, pp. 12889–12920, 2024, doi: 10.1109/access.2024.3491373.
[291] L. McCormack, M. Bendechache, D. Lewis, and D. Huyskes, "Trust and transparency in AI: industry voices on data, ethics, and compliance," *AI & Society*, 2025, doi: 10.1007/s00146-025-02654-7.
[292] B. Goyal, "Explainable AI (XAI) for Cloud-Based Enterprise Applications: Building Trust and Transparency in AI-Driven Decisions," *Journal of International Crisis and Risk Communication Research*, pp. 63–71, 2025, doi: 10.63278/jicrcr.vi.3231.