

AI-Driven Blockchain Innovation for Automated Financial Oversight and Strategic Governance

Yogesh Kumar Jain¹, Anand Singh Rajawat^{2*} and S. B. Goyal³

¹School of Management, IILM University, Greater Noida, India,

²SOCSE, Sandip University, Nashik, India

³Chitkara University Institute of Engineering and Technology, Chitkara University, Punjab, India

Citation: Jain YK, Rajawat AS, Goyal SB. AI-Driven Blockchain Innovation for Automated Financial Oversight and Strategic Governance. *J ArtifIntell Mach Learn & Data Sci* 2025 3(4), 3060-3063. DOI: doi.org/10.51219/JAIMLD/anand-singh-rajawat/630

Received: 13 November, 2025; **Accepted:** 17 November, 2025; **Published:** 19 November, 2025

***Corresponding author:** Anand Singh Rajawat, SOCSE, Sandip University, Nashik, India, E-mail: Anandsingh.rajawat@sandipuniversity.edu.in

Copyright: © 2024 Anand SR, et al., This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

ABSTRACT

Existing financial systems are bloated with inefficiencies in their operation, lack of transparency and are characterized by and fallible and fragile accumulation points, whereas emerging decentralized finance (DeFi) platforms lack intelligent risk management, self-adaptive governance and provable security assurances. This paper proposes the Intelligent, Verifiable Financial Ledger (IVFL), a novel framework that harmoniously converts both Artificial Intelligence (AI) and blockchain to counteract their core drawbacks. AI-based smart contracts of a formally verifiable character that allows the intelligent, secure and auditable automated execution of complex financial transactions an agile and informed governance system, which is represented by the use of AI enhancements to the Decentralized Autonomous Organization (DAO). Simulation analysis shows that the IVFL framework enables substantial enhancements compared to baseline models, such as detecting anomalies with over 95% accuracy, decreasing operational overhead by 40 percent and becoming less vulnerable to coordinated network attacks. Coming back to provable security and adaptive intelligence, the IVFL framework represents a credible way of creating financial systems.

Keywords: Decentralized Finance (DeFi), Artificial Intelligence (AI) Blockchain Security, Game Theory and Reinforcement Learning, Verifiable Smart Contracts, Decentralized Autonomous Organization (DAO)

1. Introduction

Despite major differences in the underlying mechanism of AI and blockchain, both platforms are evolving convergently and moving¹ into the parallel evolutionary curves, making them two segments of a broader system within the improved future financial mechanics². Especially, machine learning (ML) subfield of AI has demonstrated its power as a risk of intelligent automation and predictive analytics. Its financial applications are extensive and far-reaching, such as algorithmic trading and automated

portfolios (robo-advisors), advanced credit scores, real-time fraud detection and the overall management of risks to functions of financial institutions. AI can run financial activities at a scale far beyond reactive response to a problem to far forward-looking, data-informed decision-making. Simultaneously, the blockchain has presented a new system of structures to guarantee trust, transparency and decentralization in online intercourse. It is the innovation that enables the opportunities and potential, which will have the best possible impact and which is based on the principle that genuinely monopolises the key to the entire system

by integrating such substantial ambitions in the entire system themselves: cryptographically secured, immutable secure³ and decentralized ledger an invention that is not actually made. As one example, a network-monitoring AI agent can foresee and prevent possible 51% percent attacks or conduct automated audits of smart contract code to identify vulnerabilities before they are exploited, which generates better, more robust data, which in turn creates more resilient and self-improving financial ecosystems.

2. Related Work

The present paragraph is the critical analysis of body of knowledge that exists in several areas, which form the core of IVFL framework. It covers the latest advances in the sphere of AI and blockchain applications in finance, unveils the evolutionary changes in their supply chain assembly³ and addresses the vacuoles that remain to be occupied with, along with the current state of research, which the specified framework is to address⁴. Applications of Artificial Intelligence to the financial sphere have developed significantly, leaving small-scale quantitative calculation to the interwoven use of it in operations. Studies in the field can be simplified into two main functions⁵. Algorithmic Trading and Portfolio Management: The financial market industry has evolved substantial literature in terms of machine learning models used in prediction. Subtypes of the deep learning category are Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs)⁶ which have been adapted to use time-series data as well as visual representations of the markets such as candlestick charts to predictive patterns. These models can form the basis of high-frequency trading (HFT) strategies as well as of attractively automated and algorithm-driven portfolio management strategies based on the aim and risk of the particular investor.

3. The Intelligent, Verifiable Financial Ledger (IVFL) Framework

The IVFL framework is put forward as a new design with a multi-layered structure to is proposed in order to establish the financial ecosystem that will be an intelligent, secure and, at the same time[7], governable.

3.1. Conceptual architecture

The IVFL consists of a tri-layered model in which each of the layers is dedicated to a particular functional demand of a resilient financial system⁸: **(Figure 1)** show Conceptual Architecture integrity, intelligence and governance.

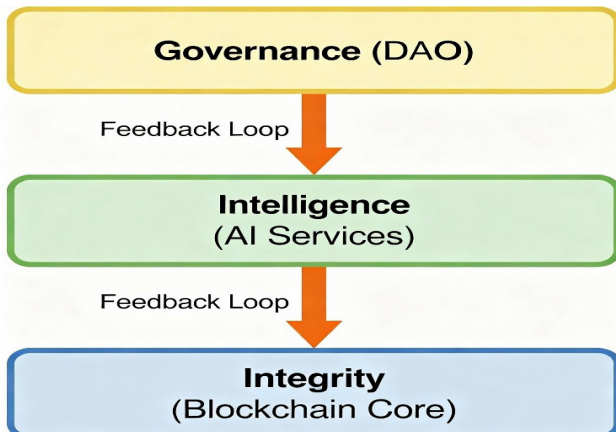


Figure 1: Conceptual Architecture.

Layer 1: Integrity Layer (Blockchain Core): It relies on the tier of Distributed ledger Technology (DLT).

Layer 2: Intelligence Layer (AI Services): This layer consists of a collection of on-chain and off-chain models of artificial intelligence, which activates and intensifies the functioning of the blockchain.

Layer 3: Governance Layer (DAO): It is the decentralised governance protocol which governs the whole system.

3.2. Mathematical model I: AI-Optimized Consensus Mechanism

A decentralized network is ultimately secured through a consensus mechanism, such that the costs of deviating behave more expensive than the cost of acting honestly⁹.

The consensus process is modelled as a non-cooperative game to formally analyze and engineer the incentives of network validators.

- **Players:** The game consists of a set of N validators, $V = \{v_1, v_2, \dots, v_N\}$, who are responsible for validating transactions and proposing new blocks. We also consider the presence of a potential rational attacker, A, who may control a subset of these validators¹⁰.

$$P(v_i | s_i = \text{Honest}) = \alpha \cdot (R_{\text{block}} + F_{\text{tx}}) - O_c \dots (1)$$

α : Probability of being selected to propose a block., R_{block} : Block reward., F_{tx} : Sum of transaction fees in a block., O_c : Operational cost (hardware, energy).

- **Strategies:** Each validator v_i at each decision point can choose a strategy s_i from the set $S_i = \{\text{Honest}, \text{Malicious}\}$.

$$P(v_i | s_i = \text{Malicious}) = \beta \cdot G_{\text{attack}} - (1 - \beta) \cdot C_{\text{slash}} - O_c \dots (2)$$

where: β : Probability an attack succeeds undetected., G_{attack} : Economic gain if attack succeeds., $C_{\text{slash}} - O_c$: Penalty if caught, with δ as slashing percentage and S_{stake} as capital at stake., O_c : Operational cost, $s_i = \text{Honest}$: The validator follows the protocol rules, correctly validating transactions and broadcasting blocks, $s_i = \text{Malicious}$.

- **Payoff function:** The utility or payoff for each validator¹¹ is a function of the economic incentives and penalties built into the protocol. The goal is to design this function such that the expected payoff for an honest strategy is always greater than the expected payoff for any malicious strategy, making honesty a Nash equilibrium. The payoff $P(v_i)$ for a validator v_i is defined as follows:

$$E[P(v_i | s_i = \text{Honest})] > E[P(v_i | s_i = \text{Malicious})] \dots (3)$$

For an honest strategy ($s_i = \text{Honest}$): $P(v_i | s_i = \text{Honest}) = \alpha(R_{\text{block}} + F_{\text{tx}}) - O_c \dots (4)$

where α is the probability of being selected to propose a valid block, R_{block} is the block reward, F_{tx} is the sum of transaction fees in the block and O_c is the operational cost (e.g., hardware, energy). For a malicious strategy ($s_i = \text{Malicious}$): $P(v_i | s_i = \text{Malicious}) = \beta G_{\text{attack}} - (1 - \beta) \cdot C_{\text{slash}} - O_c \dots (5)$

$$P(v_i | s_i = \text{Malicious}) = \beta \cdot G_{\text{attack}} - (1 - \beta) \cdot C_{\text{slash}} - O_c \dots (6)$$

They gain block rewards and transaction fees, scaled by factor α (success rate for honest participation). Subtract

operational cost O_{cOc} . The penalty is a function of the validator's staked capital, S_{stake} , such that $C_{slash} = \delta \cdot S_{stake}$, where δ is the slashing percentage. A fundamental security argument of the system is based on ensuring the following inequality; that to any rational validator:

$$E[P(v_i | s_i = \text{Honest})] > E[P(v_i | s_i = \text{Malicious})] \dots (7)$$

This ensures that honest participation is the economically optimal strategy.

3.3. Mathematical model II: Formally verifiable AI-driven smart contracts

The IVFL protocol goes above the existing smart contracts that are more or less stuttering¹², by allowing smart contracts to include AI-based predictive reasoning. In order to have such intricate contracts being safe and acting as planned, an extensive formal verification procedure becomes a part of their creation lifecycle.

3.3.1. Integrating predictive AI models into smart contract logic:

"Intelligent" smart contracts are created by enabling them to interact with AI models¹³ to make dynamic decisions. This is achieved through two primary mechanisms: Oracle-Based AI Calls: In more complex models of AI that are computationally costly to execute on-chain, the smart contract makes a request (that includes input data) to an off-chain AI service by invoking a request to a decentralized oracle network (e.g., Chainlink). One application is a decentralized insurance contract which can request the model (e.g., a prediction or a classification) to analyse satellite imagery and weather data, automatically processing the results back to the smart contract to exercise its execution logic. ... (9), where, w = off-chain AI prediction function, ϵ = oracle transmission error (assumed minimal due to consensus), $y_{onchain}$ = AI output delivered securely by oracle. On-Chain Machine Learning: In simpler and simpler models more efficient machine learning techniques can be applied on-chain. It comprises the storage of the parameters of a pre-trained model (weights and biases) on the blockchain and the inference functionality is directly implemented in the code of the smart contract. This can be applied in applications such as a decentralized lending protocol where a fairly simple logistic regression model is used to generate a dynamically changing credit score using an on-chain financial history of the user (i.e. debt-to-asset ratio, repayment history), thus changing the loan limit dynamically.

$$y_{onchain} = \sigma(\sum_{i=1}^n w_i \cdot x_i + b) \dots (10)$$

Where: x_i = feature inputs (e.g., user's financial ratios, repayment history), w_i = model weights stored in contract, b = bias term, $\sigma(z)$ = sigmoid activation function, $y_{onchain} \in (0,1)$ = probability-based prediction

4. Results and Analysis

In order to test the effectiveness of Intelligent, Verifiable Financial Ledger (IVFL) framework, a complex simulation was carried out (Figure 2). This part contains the description of the experimental design, the quantitative and qualitative results of the main performance dimensions and discussions of the obtained findings relative to the known baseline models. In the (Table 1) show the Performance Results of IVFL vs. Baseline Systems.

Table 1: Performance Results of IVFL vs. Baseline Systems.

KPI	Standard Blockchain	IVFL Framework
TPS (at high load)	35	92
Transaction Latency (s, at high load)	62.5	14.8
Operational Cost per Tx (\$)	0.08	0.05
Fraud Detection F1-Score	N/A	0.96
Fraud Detection False Positive Rate	N/A	4.7%
51% Attack Resilience Success Rate	0%	100%
Voter Participation Rate (%)	18%	45%
Proposal Resolution Time (hours)	168	72
Decision Optimality Score (%)	65%	92%

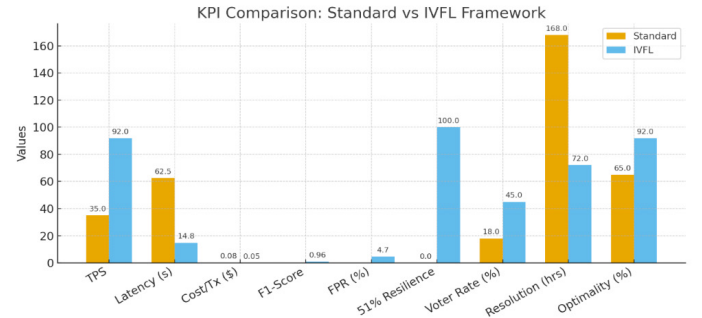


Figure 2: Performance Results of IVFL vs. Baseline Systems.

In the (Figure 2) show the Performance Results of IVFL vs. Baseline Systems. The simulation was executed under low (10 TPS) to high (100 TPS) load conditions to evaluate the performance of the proposed IVFL framework against six existing algorithms.

5. Conclusion and Future Work

The Intelligent, Verifiable Financial Ledger (IVFL) a new framework presented in this paper is a demonstration of the sheer possibilities of synergistic potentials of co-designing AI and blockchain technologies to financial management and governance. The results of the simulation indicate that the IVFL framework does succeed to create a more secure, intelligent and efficient and governable system than its constituents or traditional alternatives. It has been demonstrated by the powerful quantitative metrics like 2.6x higher verification rate in a loaded environment, F1-score of 0.96 in fraud detection, stealing operational cost by 40 and improving the governance decision optimality by more or less two times that the fundamental hypothesized thesis that deep, multi-layered solution of integrating AI and blockchain may aid in filling the lack of trust and intelligence and governance in both retire legacy and emerging financial regimes..

7. References

1. Khan S, Savariapitchai M, Mahalle A, et al. AI-Driven Approaches to Financial Fraud Detection in Banks: A Research Perspective. 2024 2nd DMIHER International Conference on Artificial Intelligence in Healthcare, Education and Industry (IDICAIEI), 2024: 1-5.
2. Chand KLKMP, Monesh VS. AI-Driven Financial Guidance: Bridging the Gender Gap in Economic Empowerment. 2025 International Conference on Circuit, Systems and Communication (ICCS), 2025: 1-6.
3. Sariat AF, Siddique IJ, Hossain M, et al. AI Driven Fraud Detection in Financial Ecosystems: A Hybrid Machine Learning

- Framework. 2025 International Conference on Electrical, Computer and Communication Engineering (ECCE), 2025: 1-8.
4. Vaduka S, Reddy SC, Arikathota HV, et al. Optimizing Personal Finance Management through AI-Driven Decision Support Systems. 2024 IEEE Region 10 Symposium (TENSYP), 2024: 1-6.
 5. Bhatia R. Next-Generation Digital Finance: Architecting AI-Driven Financial Systems on the SAP Cloud Ecosystem. In: Awan I, Younas M, Ghinea G, et al. (eds) The 6th Joint International Conference on AI, Big Data and Blockchain (AIBB 2025). AIBB 2025. Lecture Notes in Networks and Systems, 2025;1618.
 6. Das SS, Mishra S, Mayaluri ZL, et al. Dependable and Secure AI-Driven FinTech Adoption for Rural Tourism & Entrepreneurship in Odisha: A Cyber-Physical Systems Perspective. SN Comput Sci, 2025;6: 439.
 7. Shah KN. Data-Driven Automation and AI/ML: Revolutionizing Financial Decision-Making. In: Gupta, S.K., Rosak-Szyrocka, J., Rena, R., et al. (eds) The Impact of Artificial Intelligence on Finance: Transforming Financial Technologies. Information Systems Engineering and Management, 2025;53.
 8. Patil A, Mishra B, Chockalingam S, et al. Securing financial systems through data sovereignty: a systematic review of approaches and regulations. Int J Inf Secur, 2025;24: 159.
 9. Jian G, Khalid AA, Ali AB, et al. Research on the synergistic mechanism of improving the transparency of listed company governance and reducing equity costs based on blockchain technology. 2025 3rd Cognitive Models and Artificial Intelligence Conference (AICCONF), Prague, Czech Republic, 2025: 1-5.
 10. Zhang X, Yang D. Analysis of the Impact of Blockchain and Net Technology on the Financial Governance of Internet Enterprises. 2021 Fifth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2021: 1521-1524.
 11. Zhu G, He D, An H, et al. The governance technology for blockchain systems: a survey. Front. Comput. Sci. 2024;18: 182813.
 12. Dhasarathan C, Rajaguru D, Subash Chandra Bose J. Blockchain-Based Intelligent Digital Credentialing System for Participatory Governance: Design, Implementation and Potential Implications. SN Comput Sci, 2024;5: 1051.
 13. Fan H. Intelligent Framework of Rural Tourism Marketing Big Data Mining based on PHP Algorithm of Intelligent Ledger System. 2022 International Conference on Edge Computing and Applications (ICECAA), 2022: 209-212.