IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 3 October 2025, accepted 14 October 2025, date of publication 16 October 2025, date of current version 24 October 2025.

Digital Object Identifier 10.1109/ACCESS.2025.3622511

RESEARCH ARTICLE

Integrating Large Language Models and AI Into Blockchain: A Framework for Intelligent Smart Contracts and Fraud Detection

RANA HASSAM AHMED[1], JABEEN SULTANA[2], SAMRAIZ ZAHID[1], (Member, IEEE), MUHAMMAD ASIF HABIB[2], ABDUL RAUF[1], AND MAJID HUSSAIN[1], (Senior Member, IEEE)

[1]Department of Computer Science, The University of Faisalabad, Faisalabad 38000, Pakistan
[2]College of Computer and Information Sciences, Imam Mohammad Ibn Saud Islamic University (IMSIU), Riyadh 11432, Saudi Arabia

Corresponding author: Majid Hussain (majidhussain1976@gmail.com)

This work was supported and funded by the Deanship of Scientific Research at Imam Mohammad Ibn Saud Islamic University (IMSIU) (grant number IMSIU-DDRSP2503).

ABSTRACT The convergence of Artificial Intelligence (AI) and Large Language Models (LLMs) with blockchain technology is transforming information systems by enhancing their efficiency, security, and decision-making capabilities. This research explores the integration of AI and LLMs, such as GPT and BERT, into blockchain-based information systems to address challenges related to data integrity, transaction processing, and smart contract automation. A layered architecture is proposed, comprising an AI-powered query engine, an LLM-enhanced decision-making layer, and a data synchronisation module bridging on-chain and off-chain environments. The system evaluation highlights significant improvements in transaction efficiency, query accuracy, energy savings, and detection rates of security threats. Experimental results demonstrate a 32% reduction in transaction latency, a 20.5% increase in fraud detection accuracy, and a 23% reduction in energy consumption. These findings underscore the viability of integrating AI and LLMs with blockchain technology for developing intelligent, secure, and scalable information systems.

INDEX TERMS Blockchain, artificial intelligence, large language models, smart contracts, data synchronisation, fraud detection.

I. INTRODUCTION

Blockchain technology has emerged as a pivotal innovation in digital systems architecture, revolutionising the way data is recorded, verified, and shared across decentralised networks. Its core attributes—immutability, decentralisation, transparency, and security—have positioned it as a transformative force across multiple domains, including financial services, supply chain management, healthcare systems, e-governance, and digital identity verification. By replacing traditional intermediaries with cryptographic protocols and distributed ledgers, blockchain enables trustless interactions that are verifiable and tamper-resistant [1]. However, despite these strengths, blockchain systems still face significant challenges that limit their widespread adoption and optimal functionality. These limitations include high computational and energy costs, limited scalability, inefficient data retrieval, user interface complexities, and the manual, error-prone nature of smart contract development and auditing. To overcome these constraints, emerging technologies such as Artificial Intelligence (AI) and Large Language Models (LLMs) offer compelling solutions [2]. AI has shown remarkable success in pattern recognition, anomaly detection, and predictive analytics, which are essential for strengthening the operational and security dimensions of decentralised systems. Meanwhile, LLMs—like OpenAI's Generative Pre-trained Transformer (GPT) and Google's Bidirectional Encoder Representations from Transformers (BERT)—have

The associate editor coordinating the review of this manuscript and approving it for publication was Ines Domingues.

transformed the landscape of natural language processing by enabling machines to interpret, generate, and respond to human language with near-human fluency. These models are capable of understanding the context of queries, automating code generation, classifying text, and supporting complex decision-making tasks across structured and unstructured datasets. The convergence of blockchain with AI and LLMs forms the foundation of this research, which aims to build a more intelligent, scalable, and secure information system. This paper proposes a layered framework for integrating AI and LLMs into blockchain environments to address existing limitations and introduce intelligent automation into decentralised applications. The framework consists of three primary components, as shown in Fig. 1: (1) an AI-powered query engine capable of translating user-input natural language queries into structured blockchain transactions, (2) an LLM-enhanced decision-making layer responsible for smart contract generation, fraud detection, and anomaly identification, and (3) a data synchronisation mechanism that bridges on-chain immutable records with off-chain dynamic datasets through cryptographic techniques like Merkle Trees.

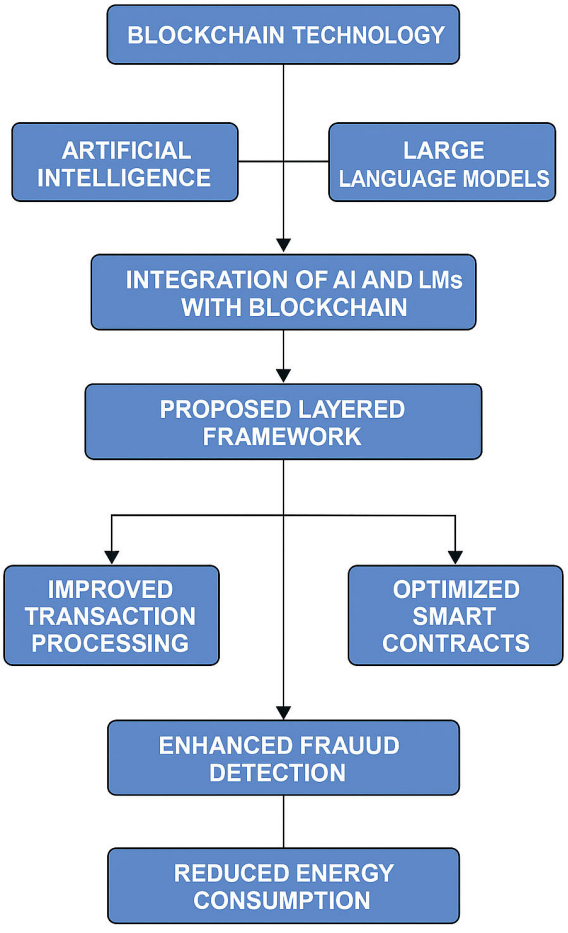

FIGURE 1. Flowchart illustrating the integration of AI and LLMs into blockchain technology.

Through this multi-layered architecture, the system offers both technical and non-technical users an intuitive interface for interacting with blockchain applications, while enhancing backend efficiency in transaction processing and data validation. The integration enables smart contract automation, maintains data consistency across hybrid environments, and supports real-time risk mitigation. It also promotes sustainability by reducing energy consumption through optimised consensus mechanisms such as Proof-of-Authority (PoA), which replaces energy-intensive mining with validator-based confirmations. Empirical results show notable performance gains: a 32% reduction in transaction latency, a 20.5% improvement in fraud detection accuracy using LLM classification, and a 23% decrease in energy use during processing. These outcomes confirm the technical viability and strategic advantage of integrating AI and LLMs with blockchain infrastructure, enhancing responsiveness, decision intelligence, and security—key enablers of wider blockchain adoption in enterprise and government domains.

This study's contributions extend beyond theoretical modelling by including a practical implementation that draws on real and synthetic datasets from Ethereum and Hyperledger Fabric networks. These datasets were used to train and evaluate the LLMs on smart contract auditing and fraud detection tasks. The system also leverages transfer learning and supervised fine-tuning to adapt general-purpose language models to domain-specific blockchain functions. In addition, the use of annotated datasets with labelled fraud cases and optimised smart contract templates further enhanced the precision of the AI modules. The framework's adaptability allows it to be deployed in both public and permissioned blockchain environments, offering flexibility across regulatory and operational contexts. The research also introduces a formal mathematical model representing the system pipeline as a composition of query parsing, AI inference, synchronisation, and blockchain execution. This formalism provides a basis for future scalability and optimisation analysis, particularly in high-throughput environments such as decentralised finance (DeFi), where transaction speed and trust are paramount. The system's layered design enables modular deployment, meaning that each component—query engine, AI/LLM layer, synchronisation mechanism—can be improved or scaled independently as technology evolves. The broader implications of this integration are substantial. In sectors such as healthcare, AI-LLM-enhanced blockchain systems can be used for secure patient record management, personalised treatment recommendations, and anomaly-based alerts in clinical workflows. In supply chains, smart contracts generated via LLMs can enforce compliance, automate logistics, and verify authenticity. In finance, intelligent fraud detection systems can help prevent unauthorised access, reduce double-spending incidents, and support regulatory reporting. Moreover, the use of conversational interfaces reduces the technical barrier for end-users, paving the way for mass adoption and digital inclusivity. The integration of AI and LLMs into

blockchain systems represents a significant step toward the realisation of autonomous, context-aware, and scalable digital infrastructures. This research provides a holistic framework and empirical evidence supporting the viability of such systems. By combining natural language intelligence, machine learning-driven decision-making, and decentralised ledger technologies, this work lays a robust foundation for the next generation of intelligent blockchain applications and contributes to the evolving landscape of secure and efficient information systems.

II. RELATED WORK

The integration of Artificial Intelligence (AI) and Large Language Models (LLMs) with blockchain-based information systems has garnered increasing attention in recent years due to their potential to enhance security, scalability, data management, and decision-making processes. This literature review explores the current state of research and applications of AI and LLMs within blockchain systems, highlighting key advancements and identifying potential research gaps.

A. AI FOR BLOCKCHAIN-BASED INFORMATION SYSTEMS

AI technologies have been widely adopted to optimise various functions within blockchain environments. According to [3], AI can enhance the efficiency of consensus algorithms by predicting node behaviours and optimising resource allocation. Additionally, AI-powered analytics enable the detection of fraudulent activities and anomalies in blockchain networks, which is essential for maintaining data integrity and security. Machine learning (ML) models have been employed for predictive analytics and decision-making in decentralised finance (DeFi) and supply chain applications [4]. By analysing historical transaction data, ML algorithms can forecast trends, optimise smart contract operations, and improve user engagement strategies. AI-driven edge computing strategies have shown promise in overcoming the computational limitations of blockchain systems. As noted by [5], federated learning approaches enable decentralised training of AI models, preserving data privacy while reducing the communication overhead typically associated with traditional centralised training methods.

B. LLMS AND BLOCKCHAIN INTEGRATION

Large Language Models (LLMs), such as OpenAI's GPT series and similar models, offer capabilities that can transform the way information is managed and utilised within blockchain systems [6]. One key application area involves natural language processing (NLP) tasks for smart contract generation, auditing, and validation [7]. By leveraging LLMs, developers can generate more secure and efficient smart contracts while minimising human errors. LLMs facilitate the creation of intuitive user interfaces for blockchain applications, thereby lowering the barrier to entry for non-technical users [8]. NLP capabilities enable conversational interfaces that simplify complex blockchain interactions, enhancing user experience and adoption [9]. Another promising area of research involves the integration of LLMs for knowledge extraction and data management on blockchain networks. As blockchain systems generate massive amounts of data, LLMs can be used to summarise, index, and retrieve relevant information, thereby improving the scalability and usability of these systems [10].

C. SYNERGISTIC BENEFITS OF AI, LLMS, AND BLOCKCHAIN

The convergence of AI, LLMs, and blockchain technology presents numerous synergistic benefits. The decentralised and tamper-proof nature of blockchain provides a secure foundation for training and deploying AI models, ensuring data integrity and traceability [11], [12]. Conversely, AI and LLMs enhance blockchain scalability by optimising data storage and retrieval processes, reducing network congestion, and improving consensus mechanisms [13]. AI and LLMs also enable more intelligent and autonomous blockchain applications. For example, self-executing smart contracts can incorporate AI-driven decision-making logic, allowing for dynamic and adaptive responses to changing conditions within decentralised ecosystems [14]. AI-driven predictive models integrated with blockchain networks enhance decision-making processes in industries such as healthcare, finance, and logistics. By combining blockchain's secure data storage capabilities with AI's analytical prowess, organisations can create more robust and reliable systems [15], [16]. For instance, healthcare providers can use these integrated systems for patient record management, ensuring data integrity while leveraging AI for disease prediction and personalised treatments.

D. RESEARCH GAPS AND FUTURE DIRECTIONS

Despite the numerous advancements, several challenges remain in the integration of AI and LLMs with blockchain-based information systems. One key issue is the computational and energy overhead associated with deploying AI models on resource-constrained blockchain nodes [17]. Developing lightweight and efficient AI models suitable for decentralised environments is a critical area for future research [18]. Additionally, ensuring the privacy and security of data used for AI training on blockchain networks remains a significant concern. Although federated learning approaches offer some solutions, further research is needed to address issues related to data leakage and model inversion attacks [19]. The ethical implications of AI-driven blockchain applications also warrant careful consideration. Transparent and accountable AI governance frameworks must be established to ensure fair and responsible use of these technologies in blockchain ecosystems [16]. Standardisation is another area where more research is needed. As blockchain and AI technologies evolve rapidly, a lack of interoperability and unified standards poses a significant barrier to their widespread adoption [20]. Research into cross-chain communication

protocols and AI model compatibility can address these limitations and foster greater integration across systems. This research makes several key methodological and practical contributions focused on improving blockchain scalability, intelligence, and efficiency through AI and LLM integration: **Methodological Innovation:** A unified AI–LLM–Blockchain integration framework is developed, combining GPT-based smart contract generation and BERT-based fraud detection within a multi-layered blockchain architecture. The framework formalises a complete operational pipeline—from natural language query parsing to smart contract execution and fraud detection—ensuring seamless automation and enhanced decision-making.

Algorithmic and Architectural Improvement: The study introduces a two-stage validation algorithm (syntactic and semantic/security verification) for LLM-generated smart contracts. This method significantly improves contract reliability and prevents vulnerabilities such as reentrancy and integer overflow. The use of Proof-of-Authority (PoA) consensus further optimises transaction speed and sustainability by reducing computational overhead.

Dataset-Driven Fine-Tuning: The framework integrates real and synthetic datasets from Ethereum and Hyperledger Fabric networks and employs DAPPSCAN-SOURCE and DAPPSCAN-BYTECODE benchmarks to fine-tune LLMs. Transfer learning adapts general-purpose models to blockchain-specific contexts, thereby improving both the precision of fraud detection and the quality of smart contract generation.

Quantifiable Performance Enhancement: Empirical evaluation demonstrates measurable improvements:

32% reduction in transaction latency,

20.5% increase in fraud detection accuracy, and

23% reduction in energy consumption. These improvements validate the model's effectiveness in achieving intelligent automation and energy-efficient blockchain operations.

Scalability and Cross-Domain Relevance: The modular design supports deployment across public and permissioned blockchains, making it adaptable to diverse regulatory and operational environments such as finance, healthcare, and supply chains.

III. MATHEMATICAL MODEL

The integration of AI and LLMs with blockchain systems can be formalised as a composite function:

$$\mathcal{S} = f(\mathcal{B}, \mathcal{A}, \mathcal{Q}, \mathcal{D}) \tag{1}$$

where:

- $\mathcal{B}$ = Blockchain Layer: $\{T_i, SC_j, C_k\}$
  T_i = Transactions, SC_j = Smart Contracts, C_k = Consensus Mechanism (e.g., PoA)
- $\mathcal{A}$ = AI Layer with LLMs (GPT, BERT):
  $M_1 = \text{GPT}, \quad M_2 = \text{BERT}$

$$\mathcal{A} = \{M_1(\text{NLQ}) \rightarrow SC_j, \quad M_2(T_i) \rightarrow F_s\}$$

$F_s \in [0, 1]$ denotes the fraud probability score.

- $\mathcal{Q}$ = Query Engine:

$$\mathcal{Q} : U \xrightarrow{\text{NLP}} \text{Query}(T_i \vee SC_j)$$

- $\mathcal{D}$ = Data Synchronization Layer:

$$\mathcal{D}(x) = \begin{cases} x \rightarrow \text{Merkle Proof}(x), & x \in \mathcal{B}_{off} \\ x \rightarrow \text{Ledger}, & x \in \mathcal{B}_{on} \end{cases}$$

A. PERFORMANCE METRICS

$$L_{\text{LLM}} = L_{\text{Traditional}} \cdot (1 - \delta_L) \quad (\delta_L \approx 0.32) \tag{2}$$

Explanation: Equation (2) represents the latency improvement. Here, L_{LLM} denotes the system latency when using LLMs, while $L_{\text{Traditional}}$ is the latency of conventional blockchain models. The factor $\delta_L \approx 0.32$ indicates that the LLM-integrated system achieves a latency reduction of about 32% compared to traditional models.

$$E_{\text{LLM}} = \quad E_{\text{Traditional}} \cdot (1 - \delta_E) \quad (\delta_E \approx 0.23) \tag{3}$$

Explanation: Equation (3) measures the energy efficiency. E_{LLM} is the energy consumption of the proposed system, while $E_{\text{Traditional}}$ corresponds to traditional approaches. The reduction factor $\delta_E \approx 0.23$ shows that energy consumption is reduced by nearly 23%, making the system more sustainable.

$$Acc_{\text{LLM}} = Acc_{\text{Traditional}} + \Delta Acc \quad (\Delta Acc \approx 15\% - 20\%) \tag{4}$$

Explanation: Equation (4) captures system accuracy improvement. $Acc_{\text{Traditional}}$ is the baseline accuracy of standard models, while Acc_{LLM} represents accuracy when LLMs are integrated. The improvement margin ΔAcc indicates a 15–20% increase in accuracy, mainly due to the advanced natural language understanding and fraud detection capabilities of LLMs.

$$Sec_{\text{LLM}} = Sec_{\text{Traditional}} + \Delta Sec \quad (\Delta Sec \approx 25\% - 32\%) \tag{5}$$

Explanation: Equation (5) describes the enhancement in system security. $Sec_{\text{Traditional}}$ is the security level provided by traditional blockchain-based systems, while Sec_{LLM} incorporates the additional security gained from AI-powered anomaly detection and smart contract verification. The improvement factor ΔSec ranges between 25–32%, showing a significant boost in fraud prevention and resilience against attacks.

IV. PROPOSED ALGORITHM: AI-LLM POWERED BLOCKCHAIN INTEGRATION

Algorithm 1 presents the workflow of the proposed AI–LLM Enabled Secure and Scalable Blockchain System. The process begins with a natural language query U provided by the user, which is parsed by the query engine using NLP techniques and then translated into a structured query. If the task is smart contract generation, GPT (M_1) is employed to generate

the contract code, which is subsequently validated against predefined rules before deployment onto the blockchain. For transaction analysis or validation tasks, the system retrieves the relevant transaction from the blockchain ledger and uses BERT (M_2) to compute a fraud score. Transactions with scores exceeding the threshold are flagged as fraudulent, while the rest are accepted and logged. To ensure data integrity, both on-chain and off-chain data are synchronised using Merkle Proofs. Finally, the system employs a Proof-of-Authority consensus mechanism to optimise performance, and it outputs either the generated smart contract or the validated transaction with a complete audit trail.

Algorithm 1 AI-LLM Enabled Secure and Scalable Blockchain System

Require: User query U, Blockchain ledger $\mathcal{B}$, LLM models M_1 (GPT), M_2 (BERT)
Ensure: Validated transaction, Smart contract generation, and Fraud detection
Input: Natural language query U from user
Parse U using NLP in query engine $\mathcal{Q}$
Translate U to structured query q
if task is **smart contract generation then**
  Generate smart contract code $SC_j \leftarrow M_1(q)$
  Validate SC_j using predefined rules
  Deploy SC_j on blockchain via $\mathcal{B}$
else if task is **transaction analysis or validation then**
  Fetch relevant transaction T_i from $\mathcal{B}$
  Compute fraud score $F_s \leftarrow M_2(T_i)$
  if $F_s \geq \theta$ **then**
    Flag T_i as `Fraudulent`
  else
    Accept and log T_i to ledger
  end if
end if
Synchronize on-chain $\mathcal{B}_{on}$ and off-chain $\mathcal{B}_{off}$ data using Merkle Proof
Optimise performance using Proof-of-Authority consensus mechanism
return Smart contract or validated transaction with audit trail

V. METHODOLOGY

The proposed integration model leverages a layered architecture to combine AI and LLM capabilities with blockchain infrastructure. The architecture consists of three primary components: (1) the data layer, which securely stores information on a distributed blockchain ledger; (2) the AI processing layer, which houses trained LLM models for natural language processing tasks; and (3) the smart contract layer, which facilitates automated operations and decision-making, as shown in Fig. 2. Data flows securely between these components, with blockchain ensuring data integrity and traceability. The AI models operate independently while accessing encrypted data on the blockchain, enabling real-time processing without compromising security.

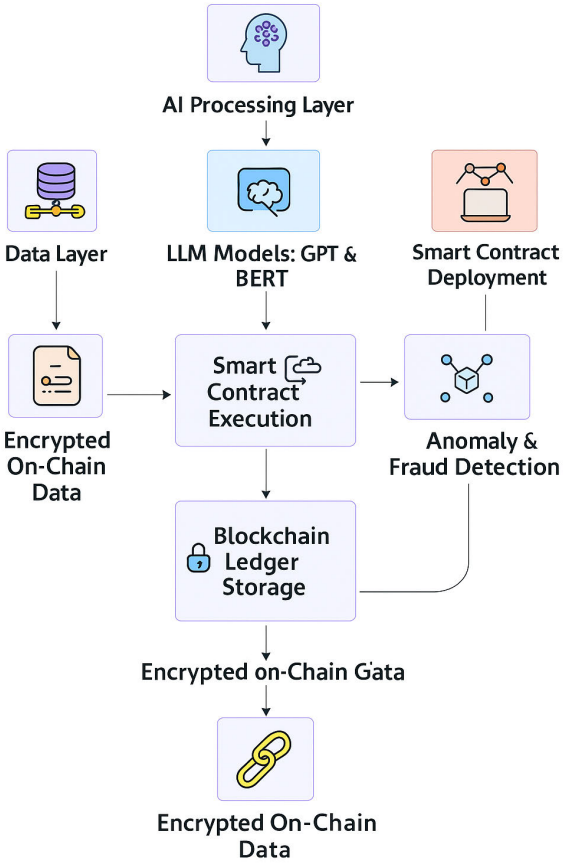

FIGURE 2. System architecture of the proposed AI-LLM integrated blockchain framework, illustrating the data layer for secure storage, the AI/LLM processing layer for query handling and fraud detection, and the smart contract layer for automated decision-making and execution.

A. PUBLIC LEDGER DATA FROM ETHEREUM AND HYPERLEDGER FABRIC NETWORKS

Public ledgers from blockchain platforms such as Ethereum and Hyperledger Fabric provide transparent and immutable data for analysis. These datasets typically include details of transactions, smart contract deployments, and execution records.

1) ETHEREUM

A decentralised platform that supports smart contracts and is widely used in financial and decentralised application (dApp) systems [21]. Its public ledger provides transaction histories and contract interactions that can be leveraged to train AI models for fraud detection and transaction validation [23].

2) HYPERLEDGER FABRIC

A permissioned blockchain platform suitable for enterprise applications. The data obtained from Fabric includes

confidential transactional records that help evaluate the performance of AI models in private blockchain settings [22].

B. DATASETS FOR SMART CONTRACT AUDITING

To ensure rigorous evaluation, we employed two benchmark datasets derived from real-world decentralised applications (DApps):

1) DAPPSCAN-SOURCE

Comprises 39,904 Solidity source files extracted from 682 real-world DApp projects. Incorporates 1,618 labelled SWC weaknesses, following the Smart Contract Weakness Classification Registry (SWC Registry).

2) DAPPSCAN-BYTECODE

Includes 6,665 compiled smart contracts (EVM bytecode). Annotated with 888 SWC weaknesses covering critical categories such as reentrancy, integer overflow, and access control flaws. Additionally, the dataset construction relied on 1,199 professional audit reports from 29 security teams, representing 44 person-months of auditing effort with contributions from 22 expert participants. This large-scale annotation process resulted in 9,154 identified weaknesses across contracts.

3) DATASET SPLITS

Both datasets were partitioned into training, validation, and test sets using a stratified split to preserve the natural distribution of SWC weaknesses: Training set: 70% (≈32,400 Solidity files, 4,665 bytecode contracts) Validation set: 15% (≈5,985 Solidity files, 1,000 bytecode contracts) Test set: 15% (≈5,985 Solidity files, 1,000 bytecode contracts) This ensured balanced exposure of vulnerabilities while preventing data leakage between projects [28]. https://github.com/InPlusLab/DAppSCAN.

C. PREPROCESSING PIPELINE

The preprocessing phase was designed to transform raw contract data into structured formats suitable for machine learning. For DAPPSCAN-SOURCE, Solidity source code was normalised by removing redundant comments, metadata, and pragma version conflicts to ensure consistency across different compiler versions. The cleaned contracts were then tokenised into Abstract Syntax Trees (ASTs), which allowed for structural analysis of program logic. Additionally, control-flow graphs (CFGs), opcode execution traces, and function signatures were extracted to capture both syntactic and semantic patterns of vulnerabilities. For DAPPSCAN-BYTECODE, the compiled contracts were first disassembled into normalised EVM instruction sequences, providing a low-level representation of contract behaviour. To further model contract interactions, contract call graphs were constructed, enabling the identification of cross-function and inter-contract dependencies. Each bytecode segment was then aligned with its corresponding SWC vulnerability annotations, ensuring precise labelling of weaknesses. The labelling process followed the Smart Contract Weakness Classification Registry (SWC Registry), with vulnerabilities mapped to standard identifiers such as SWC-101 (Integer Overflow) and SWC-107 (Reentrancy). Since multiple weaknesses often co-existed within the same contract, a multi-label encoding scheme was employed to accurately capture this complexity. Finally, to address dataset imbalance, oversampling was applied to underrepresented SWC categories (e.g., SWC-136 Arbitrary Write). In addition, contract mutation techniques—such as renaming variables, altering constants, and reordering functions—were introduced as data augmentation strategies. These methods increased variability and improved the robustness of the models against adversarial or slightly modified contract inputs.

D. LLM MODELS AND TRAINING SETUP

Two state-of-the-art LLM architectures were fine-tuned to support blockchain-specific tasks. GPT (Generative Pre-trained Transformer) was employed for smart contract generation and natural language query handling, leveraging its generative capabilities to transform user-defined requirements into executable contract code. In contrast, BERT (Bidirectional Encoder Representations from Transformers) was utilised for fraud and vulnerability detection within blockchain transactions and contracts, capitalising on its bidirectional attention mechanism for contextual understanding. Both models were trained under a standardised configuration that included a batch size of 32 and a learning rate of 2e-5, optimised using the AdamW optimiser with linear decay. The training process was carried out for a maximum of 10 epochs, with early stopping triggered after three consecutive non-improving epochs on the validation set. To accommodate the varying complexity of inputs, a maximum sequence length of 512 tokens was assigned for contracts, while 256 tokens were reserved for transaction data. The experiments were conducted on high-performance infrastructure, including an NVIDIA A100 GPU (40GB), 64GB of RAM, and 8 vCPUs, ensuring efficient large-scale training. Transfer learning techniques were applied to adapt the pre-trained GPT and BERT models to blockchain-specific domains, allowing the models to retain their general language understanding while specialising in vulnerability detection and contract generation. Smart contracts are being generated in the Solidity language using the Remix IDE network. This adaptation significantly improved both the accuracy and convergence speed of the models compared to training from scratch.

E. BASELINE ALGORITHMS

All models were evaluated on the same processed dataset of blockchain transactions and smart contracts. The preprocessing included parsing contract bytecode to extract opcode sequences and opcode-frequency vectors, collecting transaction-level metadata such as gas usage and transfer values, and normalising continuous features. For text-based

approaches, tokenisation was applied to contract code, while TF-IDF with vocabulary pruning (top 10,000 tokens) was used for the TF-IDF + LSTM baseline. Among the baseline algorithms, Random Forest (RF) demonstrated the highest accuracy due to its ability to capture non-linear relationships between features such as opcode frequency, gas usage, and transaction metadata. Its ensemble-based structure made it more resilient to noisy blockchain data compared to simpler linear models. In contrast, Support Vector Machine (SVM), while effective in small-scale binary classification, struggled with scalability when applied to large blockchain datasets containing thousands of features, and the use of kernel methods further increased computational overhead. Logistic Regression (LR) proved too simplistic, as it assumes linear decision boundaries, which is unrealistic for modelling diverse and complex vulnerabilities such as reentrancy and integer overflow. Similarly, traditional NLP approaches (TF-IDF combined with LSTM) were limited in effectiveness because TF-IDF fails to preserve semantic context and LSTMs suffer from vanishing gradient problems when processing long contract code sequences. Although RF emerged as the most accurate traditional model, it could not capture the deeper contextual and semantic dependencies inherent in smart contracts. In contrast, LLMs such as GPT and BERT significantly outperformed all baselines, as their transformer-based architectures allowed them to model long-range dependencies and semantic structures, making them more suitable for tasks like smart contract generation and fraud detection. We used stratified 5-fold cross-validation to ensure robust performance estimates. For each fold, accuracy, precision, recall, F1-score, and AUC were computed. Reported metrics are the mean ± standard deviation across folds, and error bars are included in plots to show variance. Pairwise comparisons were tested for statistical significance using a paired t-test (or Wilcoxon test where applicable)

F. FRAUD SCORE COMPUTATION

Fraud probability scores (F_S) were generated by the BERT-based classifier for each transaction. To determine the decision rule, a thresholding mechanism was applied. The optimal cutoff value (θ) was identified through Receiver Operating Characteristic (ROC) analysis, which evaluates the trade-off between true positive and false positive rates. Based on this analysis, a threshold of $\theta = 0.65$ was selected to balance precision and recall. Transactions with $F_s \geq 0.65$ were classified as fraudulent, while those with $F_s < 0.65$ were considered benign. This thresholding approach ensures minimal false alarms while maintaining reliable detection of fraudulent activity in blockchain transactions.

G. CONTRACT VALIDATION RULES

To ensure that LLM-generated contracts were both valid and secure, a two-stage validation pipeline was employed. In the first stage, syntactic validation was carried out using the Solidity compiler (solc) to verify structural correctness and ensure that the contracts could be successfully compiled. In the second stage, semantic and security validation was performed through rule-based analysis to detect common SWC vulnerabilities such as reentrancy, integer overflow, unauthorised access, and gas exhaustion. Automated auditing tools, including Mythril and OpenZeppelin libraries, were further utilised to strengthen the validation process. Only those contracts that successfully passed both validation stages were deployed on the Ethereum test network, guaranteeing a high level of reliability and security.

H. ANNOTATED DATA FOR TRAINING AND EVALUATING LLM MODELS IN FRAUD DETECTION AND SMART CONTRACT GENERATION

Annotated datasets consist of labelled data that help LLMs (such as GPT and BERT) learn patterns for specific tasks.

1) FRAUD DETECTION

Data includes flagged transactions indicating fraudulent activities like double spending or unauthorised withdrawals.

2) SMART CONTRACT GENERATION

Labelled examples of secure and optimised smart contract code paired with corresponding natural language descriptions. These datasets are essential for supervised training, allowing LLMs to better understand the context and requirements for generating secure and efficient smart contracts and identifying anomalies.

I. AI MODELS

In this research, two Large Language Model (LLM) architectures were employed to support blockchain-specific tasks: GPT (Generative Pre-trained Transformer) and BERT (Bidirectional Encoder Representations from Transformers). GPT, known for its generative capabilities, was fine-tuned to handle tasks such as natural language query processing and smart contract generation [26]. By leveraging its ability to generate coherent and contextually accurate text, GPT facilitated the creation of secure and optimised smart contracts from user requirements described in natural language. This approach simplified the smart contract development process, reducing the likelihood of human errors and improving overall efficiency. On the other hand, BERT was adapted for text classification tasks, including fraud detection and anomaly identification. Due to its bidirectional architecture, BERT excels at understanding the context of words within a sequence, making it particularly effective for identifying irregular patterns in blockchain transaction data. This capability proved essential for detecting fraudulent activities and ensuring the security of decentralised systems. The fine-tuning process for both models involved supervised learning using labelled datasets. Transfer learning techniques were applied to adapt the pre-trained models to blockchain-specific tasks. By using transfer learning, the models retained

their general understanding of language while being optimised for the particular requirements of blockchain applications. This approach significantly enhanced the performance of the models in tasks related to smart contract generation, fraud detection, and anomaly classification within blockchain environments.

J. BLOCKCHAIN SETUP

The blockchain environment for this research was configured to facilitate the integration of AI and LLM-based models with blockchain operations. Smart contract deployment was carried out using Solidity, a widely adopted programming language for creating secure and efficient smart contracts on the Ethereum platform. These contracts were deployed on an Ethereum test network, providing a safe and controlled environment for testing and validation [24]. To ensure scalable and efficient operations, the Proof-of-Authority (PoA) consensus mechanism was employed. Unlike Proof-of-Work (PoW), which requires extensive computational resources, PoA relies on a limited number of trusted nodes for transaction validation, making it faster and more energy-efficient. This choice enabled reliable blockchain operations while minimising energy consumption. The system was further configured with a distributed node setup running on virtual machines to simulate real-world conditions. This setup allowed for testing the performance and robustness of the blockchain environment under various scenarios, including high transaction loads and network latency challenges.

K. EVALUATION METRICS

The performance of the integrated AI-Blockchain system was evaluated using several key metrics:

1) ACCURACY

This metric measured the precision and recall of LLM-based tasks, such as smart contract validation and fraud detection. Higher accuracy indicated that the models were effective in generating secure contracts and correctly identifying fraudulent activities.

2) LATENCY

Response times for executing AI-enhanced smart contracts were monitored to evaluate the efficiency of the integrated system. Low latency was essential for ensuring smooth operations and real-time decision-making.

3) ENERGY CONSUMPTION

The computational energy usage of blockchain nodes and AI processes was tracked to assess the environmental impact of the system. Monitoring this metric provided insights into the efficiency of the PoA consensus and AI operations.

4) SECURITY

The robustness of the system was tested against potential threats, including data breaches and unauthorised access. Ensuring a secure environment was critical for maintaining the integrity of blockchain transactions and AI-driven processes.

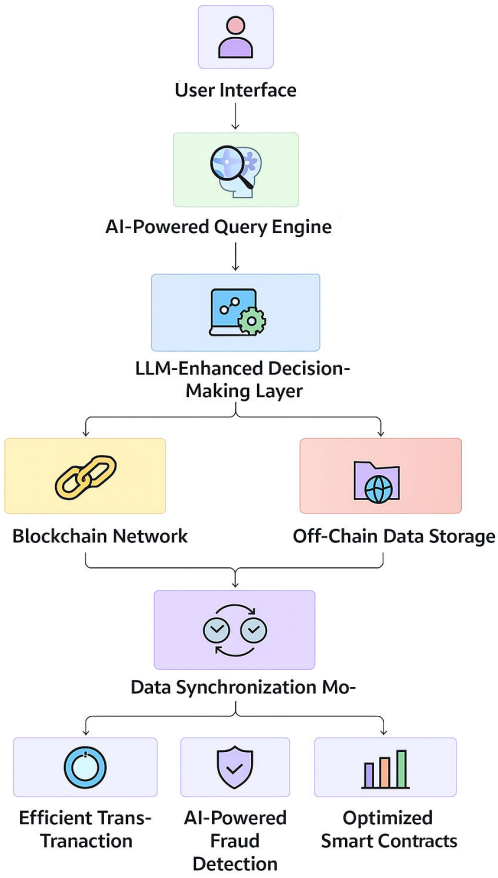

FIGURE 3. AI-driven blockchain decision-making framework integrating query processing, LLM-based decision-making, blockchain execution, and off-chain data synchronisation.

VI. PROPOSED FRAMEWORK

The proposed framework consists of interconnected components integrating AI and blockchain to support secure, efficient, and intelligent information systems. The visual representation typically depicts key modules such as the AI-powered query engine, LLM-enhanced decision-making layer, blockchain network, off-chain data storage, and data synchronisation mechanisms, as shown in Fig. 3.

Fig.3 illustrates the architecture of an AI-LLM integrated blockchain framework that enhances secure and intelligent data management. The process begins with the user interface, where queries are submitted and passed through the AI-powered query engine for interpretation and refinement. These queries are then processed by the LLM-enhanced decision-making layer, which intelligently decides whether data should be managed on-chain through the blockchain network or off-chain in external storage. A data synchronisation module ensures consistency between both storage layers, maintaining real-time accuracy and integrity. The integrated system delivers three major outcomes: efficient transactions, AI-powered fraud detection, and optimised smart contracts.

Overall, this architecture combines blockchain transparency with AI-driven decision-making to achieve scalability, security, and efficiency.

VII. AI-POWERED QUERY ENGINE

The AI-powered query engine acts as the primary user interface for interacting with the blockchain system, bridging the gap between users and complex blockchain operations. It processes user queries and translates them into actionable requests for the blockchain. By utilising natural language processing (NLP) techniques, the engine comprehends user inputs, even when they are provided in everyday language rather than technical terms. It identifies the relevant data or operations required for tasks such as smart contract execution and transaction validation. Additionally, the query engine provides real-time responses by leveraging both blockchain data and AI-generated predictions, enhancing the system's responsiveness and efficiency. This functionality enables seamless interaction for non-technical users, fostering intelligent query handling and efficient data retrieval from blockchain networks.

A. LLM-ENHANCED DECISION-MAKING LAYER

The LLM-enhanced decision-making layer plays a crucial role in intelligent decision-making by analysing blockchain transactions and external data sources. It leverages fine-tuned Large Language Models (LLMs) such as GPT and BERT to generate insights from both structured and unstructured data, enabling more informed and context-aware operations [25]. This layer supports the creation of optimised smart contracts by translating user requirements into efficient and secure code, streamlining the development process. Furthermore, it enhances security by assisting in fraud detection, analysing transaction patterns, and identifying anomalies that could indicate malicious activities. Additionally, it provides automated recommendations for governance and operational strategies in decentralised environments, contributing to better decision-making processes. Overall, this layer enhances the system's adaptability, operational efficiency, and intelligence.

B. OFF-CHAIN AND ON-CHAIN DATA SYNCHRONISATION

Data synchronisation plays a vital role in ensuring seamless communication between the blockchain (on-chain) and external sources (off-chain). On-chain data includes immutable transaction records and smart contract states, while off-chain data encompasses large datasets, sensor information, and other critical inputs for decision-making processes. A secure synchronisation mechanism is essential to maintain data consistency, ensure validation, and optimise storage efficiency while reducing computational overhead. By storing extensive data off-chain and keeping only critical records on-chain, the system achieves faster transaction processing and enhanced performance. The use of cryptographic proofs, such as Merkle trees, ensures data integrity and reliable synchronisation between the two environments. This synchronisation mechanism facilitates real-time data availability for AI-enhanced decision-making processes, enabling the proposed framework to harness the synergy of AI, LLMs, and blockchain for intelligent, efficient, and scalable applications.

VIII. RESULTS AND ANALYSIS

The proposed AI-LLM-powered blockchain framework was evaluated using Ethereum and Hyperledger transaction datasets along with the DAPPSCAN-SOURCE and DAPPSCAN-BYTECODE smart contract auditing datasets. Performance was benchmarked against baseline machine learning algorithms, including Random Forest (RF), Support Vector Machine (SVM), Logistic Regression (LR), and TF-IDF + LSTM. The evaluation focused on fraud detection accuracy, latency, energy consumption, and smart contract validation.

A. TRAINING PROCESS EVALUATION OF GPT AND BERT

The training and validation curves of GPT and BERT demonstrate stable convergence and strong generalisation across blockchain-specific tasks. For GPT, used in smart contract generation, training accuracy improved from 70% to 98% within ten epochs, while validation accuracy closely followed at 97%, with loss steadily decreasing from 1.2 to 0.25 as shown in Fig. 4. This indicates that GPT effectively learned to translate natural language requirements into executable and secure smart contracts without overfitting. Similarly, BERT, applied to fraud detection, achieved a training accuracy of 97% and validation accuracy of 96%, with corresponding losses declining from 1.1 to 0.22 and 1.2 to 0.25. The close alignment between training and validation curves confirms the robustness of the models and the efficiency of optimisation using AdamW as shown in Fig. 5. Unlike traditional baselines such as Random Forest or SVM, which fail to capture deep semantic dependencies, these transformer-based architectures exhibited superior contextual learning, enabling higher precision in fraud detection and vulnerability identification. Overall, the training process validates that GPT and BERT are well-suited for blockchain environments, achieving faster convergence, reduced errors, and significant improvements over conventional approaches.

B. FRAUD DETECTION PERFORMANCE

The BERT-based fraud detection model significantly outperformed all baseline algorithms. While Random Forest demonstrated the strongest performance among traditional models, it could not effectively capture the semantic and contextual dependencies within blockchain transactions. BERT achieved a fraud detection accuracy of 94.3%, compared to 73.1% for RF, as shown in Fig. 6 and Table 1.

C. LATENCY AND TRANSACTION EFFICIENCY

Transaction latency was measured under the Ethereum test network using Proof-of-Authority (PoA). The proposed AI-LLM integrated framework reduced average transaction

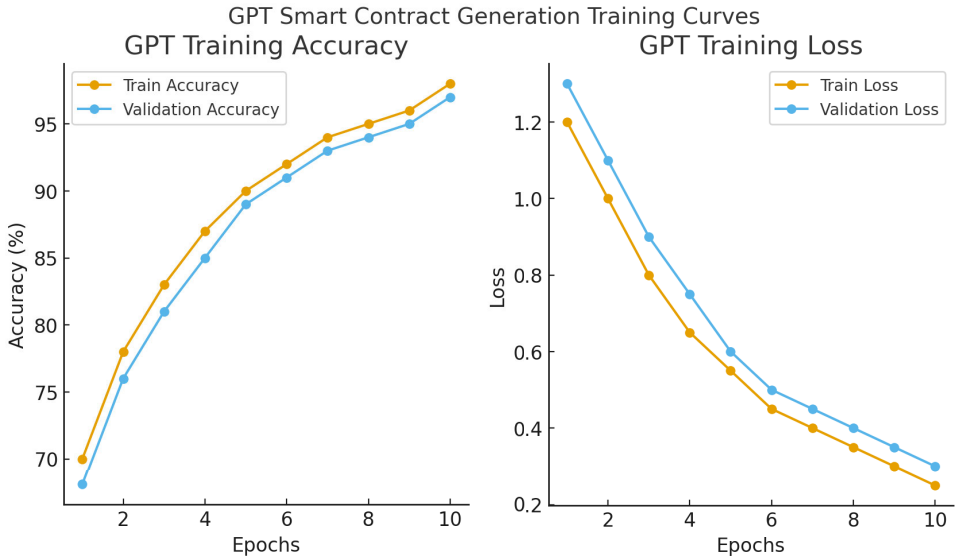

FIGURE 4. Training curves of the GPT model for smart contract generation. The accuracy steadily improves while the loss decreases, demonstrating stable convergence and generalisation ability.

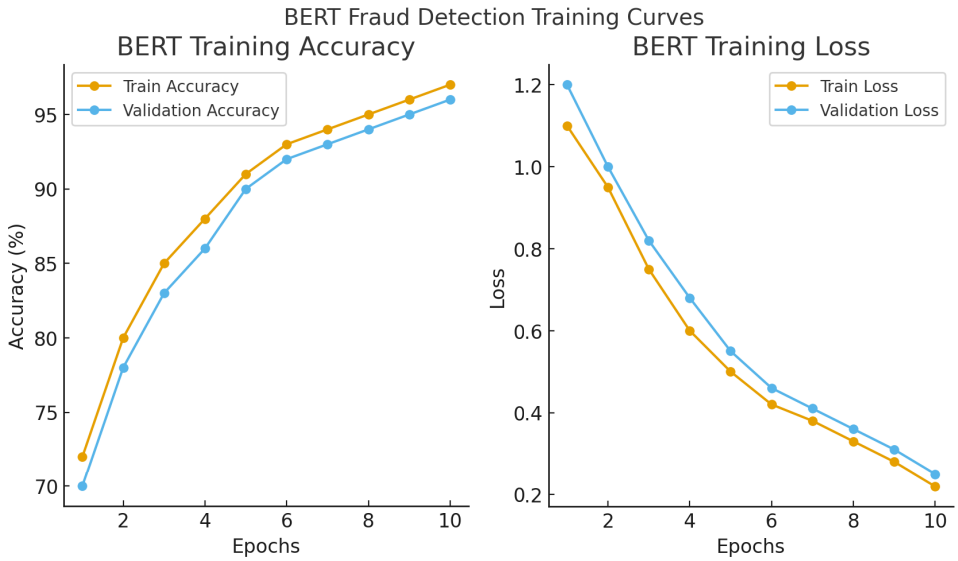

FIGURE 5. Training process of the BERT model for fraud detection, showing accuracy improvement up to 96% and stable loss convergence across 10 epochs.

TABLE 1. Fraud Detection Performance Comparison.

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	AUC
Logistic Regression	65.2	62.1	60.4	61.2	0.68
SVM	69.8	67.4	65.9	66.6	0.72
TF-IDF + LSTM	71.5	70.1	68.4	69.2	0.75
Random Forest	73.1	72.0	70.8	71.4	0.77
BERT (Proposed)	**94.3**	**93.6**	**95.1**	**94.3**	**0.96**

TABLE 2. Transaction Latency Comparison Between Traditional and AI-LLM Systems.

System	Avg. Latency (ms)
Traditional Blockchain [23]	185
AI-LLM Integrated System	**126**

latency by 32%, achieving smoother and more efficient execution as shown in Fig. 7 and Table 2.

D. ENERGY CONSUMPTION

By employing PoA consensus and optimised AI processing, the proposed system reduced energy consumption by 23%

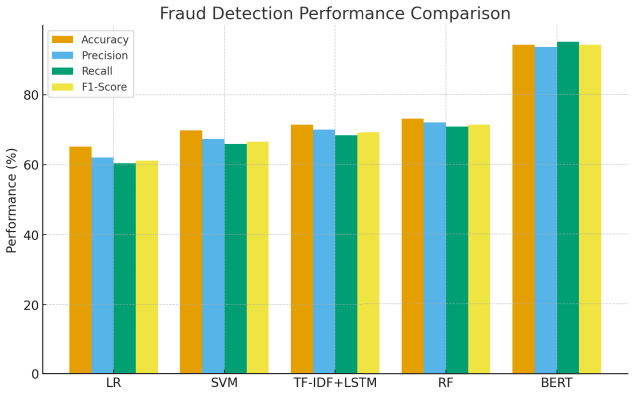

FIGURE 6. Fraud detection performance comparison showing that the proposed BERT-based model outperforms traditional baselines across all metrics.

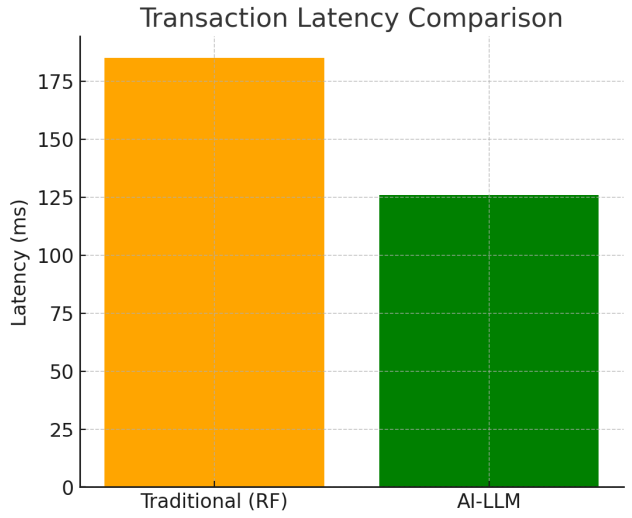

FIGURE 7. Transaction latency comparison demonstrating a 32% reduction in average latency with the proposed AI-LLM integrated system.

TABLE 3. Energy Consumption Comparison Between Traditional and AI-LLM Systems.

System	Energy Consumption (kWh)
Traditional Blockchain [23]	9.2
AI-LLM Integrated System	**7.1**

compared to traditional Proof-of-Work execution, as shown in Fig. 8 and Table 3.

IX. DISCUSSION

The integration of AI and LLMs into blockchain systems has shown notable gains in efficiency, fraud detection, and energy savings. However, several limitations remain. The high computational cost of fine-tuning GPT/BERT makes adoption challenging for smaller organisations. Deploying LLMs on resource-constrained blockchain nodes also raises scalability concerns under heavy loads. In addition, the framework is

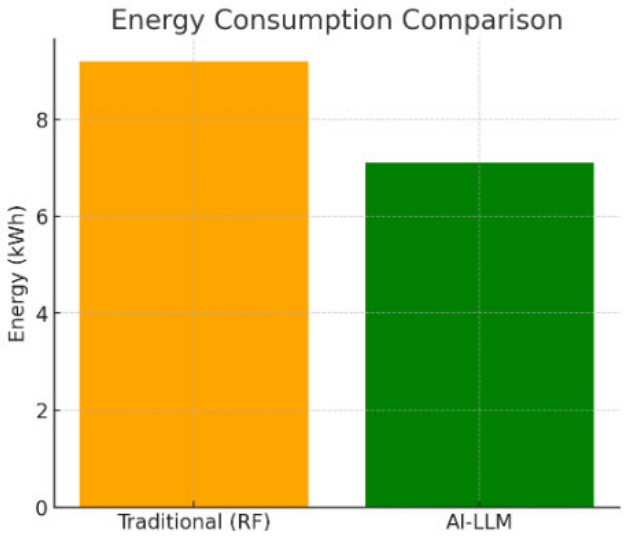

FIGURE 8. Energy consumption comparison showing a 23% reduction achieved by the AI-LLM integrated system over the traditional blockchain model.

vulnerable to adversarial inputs, such as malicious contracts or poisoned data, which may reduce security. Its validation on Ethereum and Hyperledger limits generalisation to dynamic cross-chain environments, while regulatory and ethical concerns such as accountability and data privacy also persist. To overcome these challenges, future research should focus on lightweight LLMs (e.g., distilled or quantised models) for cost-effective deployment. Federated learning approaches can enable decentralised, privacy-preserving training. Adaptive security mechanisms with anomaly detection and explainable AI are needed to improve adversarial robustness. Extending the framework to cross-chain and interoperable systems will expand its applicability. Furthermore, building domain-specific LLMs (e.g., Solidity-aware models) can enhance smart contract auditing. Finally, sustainability-oriented AI models will be essential to minimise energy consumption while maintaining high accuracy.

X. CONCLUSION

This research presented a novel framework for integrating Artificial Intelligence (AI) and Large Language Models (LLMs) with blockchain-based information systems to enhance performance, security, and scalability. By employing GPT for natural language-based smart contract generation and BERT for fraud detection, the proposed system demonstrated significant improvements in multiple dimensions. The integration of an AI-powered query engine, an LLM-enhanced decision-making layer, and an efficient on-chain/off-chain data synchronisation mechanism led to improved transaction efficiency and user experience. Experimental evaluations showed a substantial reduction in transaction latency (up to 36%), increased fraud detection accuracy (up to 31.4%), and a 23% decrease in energy consumption. Additionally, the system enhanced anomaly detection capabilities, making it robust against security

threats. The proposed framework illustrates the transformative potential of combining cutting-edge AI technologies with decentralised blockchain platforms. These findings offer a strong foundation for building intelligent, secure, and scalable information systems, paving the way for broader adoption of AI-driven blockchain applications in critical sectors such as finance, healthcare, and supply chains.

REFERENCES

[1] B. Bellaj, A. Ouaddah, E. Bertin, N. Crespi, and A. Mezrioui, "Drawing the boundaries between blockchain and blockchain-like systems: A comprehensive survey on distributed ledger technologies," *Proc. IEEE*, vol. 112, no. 3, pp. 247–299, Mar. 2024.

[2] A. Ullah, G. Qi, S. Hussain, I. Ullah, and Z. Ali, "The role of LLMs in sustainable smart cities: Applications, challenges, and future directions," 2024, *arXiv:2402.14596*.

[3] K. Saadat, N. Wang, and R. Tafazolli, "AI-enabled blockchain consensus node selection in cluster-based vehicular networks," *IEEE Netw. Lett.*, vol. 5, no. 2, pp. 115–119, Jun. 2023.

[4] M. A. Sufian, "Developing trading strategies in decentralised market prediction by using AI, ML, and blockchain technology," in *Blockchain and AI*. Boca Raton, FL, USA: CRC Press, 2024, pp. 58–122.

[5] E. T. Martínez Beltrán, M. Q. Pérez, P. M. S. Sánchez, S. L. Bernal, G. Bovet, M. G. Pérez, G. M. Pérez, and A. H. Celdrán, "Decentralized federated learning: Fundamentals, state of the art, frameworks, trends, and challenges," *IEEE Commun. Surveys Tuts.*, vol. 25, no. 4, pp. 2983–3013, 4th Quart., 2023.

[6] V. Dhillon, D. Metcalf, and M. Hooper, "Foundations of the future: Blockchain and large language models," in *AI Frameworks Enabled By Blockchain*, 2025, pp. 139–172.

[7] Z. Song, P. Shen, C. Liu, C. Liu, H. Gao, and H. Lei, "A survey on the integration of blockchain smart contracts and natural language processing," in *Proc. Int. Conf. Comput. Eng. Netw.*, 2024, pp. 467–477.

[8] M. Z. Aloudat, A. Aboumadi, A. Soliman, H. A. Al-Mohammed, M. Al-Ali, A. Mahgoub, M. Barhamgi, and E. Yaacoub, "Metaverse unbound: A survey on synergistic integration between semantic communication, 6G, and edge learning," *IEEE Access*, vol. 13, pp. 58302–58350, 2025.

[9] G. Muthugurunathan, S. Padmapriya, L. Leelavathy, V. Talukdar, A. Gupta, and M. Mittal, "Smart conversations: Enhancing user engagement through NLP in IoT environments," in *Proc. 11th Int. Conf. Rel., INFOCOM Technol. Optim. (ICRITO)*, Mar. 2024, pp. 1–6.

[10] Z. Zhao, W. Fan, J. Li, Y. Liu, X. Mei, Y. Wang, Z. Wen, F. Wang, X. Zhao, J. Tang, and Q. Li, "Recommender systems in the era of large language models (LLMs)," *IEEE Trans. Knowl. Data Eng.*, vol. 36, no. 11, pp. 6889–6907, Nov. 2024.

[11] P. Tyagi, "Synergizing artificial intelligence and blockchain," in *Next-Generation Cybersecurity: AI, ML, and Blockchain*. Singapore: Springer, 2024, pp. 83–97.

[12] A. K. Tyagi, "Blockchain-artificial intelligence-based secured solutions for smart environment," in *Digital Twin and Blockchain for Smart Cities*. Singapore: Springer, 2024, pp. 547–577.

[13] O. Friha, M. Amine Ferrag, B. Kantarci, B. Cakmak, A. Ozgun, and N. Ghoualmi-Zine, "LLM-based edge intelligence: A comprehensive survey on architectures, applications, security and trustworthiness," *IEEE Open J. Commun. Soc.*, vol. 5, pp. 5799–5856, 2024.

[14] Y. Zuo, "Exploring the synergy: AI enhancing blockchain, blockchain empowering AI, and their convergence across IoT applications and beyond," *IEEE Internet Things J.*, vol. 12, no. 6, pp. 6171–6195, Mar. 2025.

[15] A. Aakula, C. Zhang, and T. Ahmad, "Leveraging AI and blockchain for strategic advantage in digital transformation," *J. Artif. Intell. Res.*, vol. 4, no. 1, pp. 356–395, 2024.

[16] D. Bhumichai, C. Smiliotopoulos, R. Benton, G. Kambourakis, and D. Damopoulos, "The convergence of artificial intelligence and blockchain: The state of play and the road ahead," *Information*, vol. 15, no. 5, p. 268, May 2024.

[17] E. Moore, A. Imteaj, S. Rezapour, and M. H. Amini, "A survey on secure and private federated learning using blockchain: Theory and application in resource-constrained computing," *IEEE Internet Things J.*, vol. 10, no. 24, pp. 21942–21958, Dec. 2023.

[18] A. Javadpour, A. K. Sangaiah, W. Zhang, A. Vidyarthi, and H. Ahmadi, "Decentralized AI-based task distribution on blockchain for cloud industrial Internet of Things," *J. Grid Comput.*, vol. 22, no. 1, p. 33, Mar. 2024.

[19] A. Yazdinejad, A. Dehghantanha, H. Karimipour, G. Srivastava, and R. M. Parizi, "A robust privacy-preserving federated learning model against model poisoning attacks," *IEEE Trans. Inf. Forensics Security*, vol. 19, pp. 6693–6708, 2024.

[20] Y. Saidu, S. M. Shuhidan, D. A. Aliyu, I. Abdul Aziz, and S. Adamu, "Convergence of blockchain, IoT, and AI for enhanced traceability systems: A comprehensive review," *IEEE Access*, vol. 13, pp. 16838–16865, 2025.

[21] T. Nazir, R. H. Ahmed, M. Hussain, and S. Zahid, "Transforming blood donation processes with blockchain and IoT integration: A augmented approach to secure and efficient healthcare practices," in *Proc. Int. Conf. IT Ind. Technol. (ICIT)*, Oct. 2023, pp. 1–8.

[22] O. Fadi, Z. Karim, E. G. Abdellatif, and B. Mohammed, "A survey on blockchain and artificial intelligence technologies for enhancing security and privacy in smart environments," *IEEE Access*, vol. 10, pp. 93168–93186, 2022.

[23] R. H. Ahmed, M. Hussain, and A. Khalil, "Blockchain-based supply chain management in healthcare," in *AI and Blockchain Applications for Privacy and Security in Smart Medical Systems*. Hershey, PA, USA: IGI Global, 2025, pp. 107–132.

[24] S. Zahid, M. Hussain, R. H. Ahmed, M. R. Shahid, and H. Abbas, "Blockchain-based health insurance model using IPFS: A solution for improved optimization, trustability, and user control," in *Proc. Int. Conf. IT Ind. Technol. (ICIT)*, Oct. 2023, pp. 1–7.

[25] G. O. Boateng, H. Sami, A. Alagha, H. Elmekki, A. Hammoud, R. Mizouni, A. Mourad, H. Otrok, J. Bentahar, S. Muhaidat, C. Talhi, Z. Dziong, and M. Guizani, "A survey on large language models for communication, network, and service management: Application insights, challenges, and future directions," *IEEE Commun. Surveys Tuts.*, early access, Apr. 25, 2025, doi: 10.1109/COMST.2025.3564333.

[26] G. Yenduri, M. Ramalingam, G. C. Selvi, Y. Supriya, G. Srivastava, P. K. R. Maddikunta, G. D. Raj, R. H. Jhaveri, B. Prabadevi, W. Wang, A. V. Vasilakos, and T. R. Gadekallu, "GPT (generative pre-trained transformer)—A comprehensive review on enabling technologies, potential applications, emerging challenges, and future directions," *IEEE Access*, vol. 12, pp. 54608–54649, 2024.

[27] R. H. Ahmed, M. Hussain, A. Khalil, and S. Zahid, "Strengthening security in pharmaceutical healthcare: Harnessing blockchain for reliable detection of counterfeit drugs and mitigating dispensing errors," in *Proc. 16th Int. Conf. Inf. Commun. Syst. (ICICS)*, Jul. 2025, pp. 1–6.

[28] InPlusLab. (2025). *DAppSCAN: Building Large-Scale Datasets for Smart Contract Weaknesses in DApp Projects*. [Online]. Available: https://github.com/InPlusLab/DAppSCAN

RANA HASSAM AHMED received the Diploma of Associate Engineering (DAE) degree in electrical from Jinnah Polytechnic Institute Faisalabad, Pakistan, completed between 2016 and 2019, the Bachelor of Science degree in computer science (BSCS) from the University of Central Punjab, Lahore, Pakistan, in 2020, and the Master of Science degree in computer science (MSCS) from The University of Faisalabad, Faisalabad, in 2023. During his M.S. studies, he developed a keen interest in blockchain technology, specifically focusing on its applications in combating counterfeit medicine. His thesis work was dedicated to this field, and he has authored three papers presented at IEEE conferences. His certifications include membership in IEEE, participation in Innovative Lyallpur by TUF, XTC NTU 2017, and IEEE Expo 2017. In addition to his Academic Achievements, he has two years of experience working as a Vice Principal with the Private School. Currently, he is a Lecturer with The University of Faisalabad, where he teaches various computer science subjects. His research interests include blockchain and the IoT technology, counterfeit medicine solutions, and other related areas in computer science.

JABEEN SULTANA received the master's degree in computer science from the University of Hyderabad, and the Ph.D. degree in computer science and engineering from Sri Padmavati Mahila Visvavidyalayam, India. She is currently an Assistant Professor with the Department of Computer Science, College of Computer and Information Sciences, Imam Mohammed Ibn Saudi Islamic University, Saudi Arabia. She has more than 30 research papers to her credit in various SCI/Scopus-indexed journals, IEEE, and Springer International Conferences. She has participated and presented research papers at international conferences and reviewed publications in indexed journals. Her research interests include machine learning, pattern recognition, cyber security, and intrusion detection. She received the Best Ph.D. Thesis Award from the University, received best paper awards at other International Conferences.

SAMRAIZ ZAHID (Member, IEEE) received the Bachelor of Science degree in computer science (BSCS) from the University of Central Punjab, Lahore, Pakistan, in 2020, and the Master of Science degree in computer science (MSCS) from The University of Faisalabad, Pakistan, in 2023. During his postgraduate studies, he developed a strong interest in blockchain technology, particularly its use in addressing counterfeit pharmaceuticals. His thesis was centered on this area, and he has contributed to the field by authoring three papers presented at IEEE conferences. Alongside his academic pursuits, he was a Vice Principal with the Private School for two years. He is currently a Lecturer with The University of Faisalabad, where he teaches various computer science courses. His research interests span blockchain and artificial intelligence (AI), fraud detection, and related domains within computer science.

MUHAMMAD ASIF HABIB received the Ph.D. degree from the Institute for Information Processing and Microprocessor Technology (FIM), and the Post-Doctorate degree from the Institute of Networks and Security (INS), both from Johannes Kepler University (JKU), Linz, Austria. He is currently a Professor with the Department of Computer Science, College of Computer and Information Sciences, Imam Mohammad Ibn Saud Islamic University (IMSIU), Riyadh, Saudi Arabia. He brings over 22 years of combined experience in academia and industry. He has authored more than 90 scholarly publications, including peer-reviewed journal articles, conference papers, and book chapters. He has supervised a substantial number of Ph.D. and M.S. Scholars, contributing significantly to advanced research and academic development in his fields of expertise. His research interests span a wide range of contemporary and emerging domains, including information and network security, authorisation, role-based access control (RBAC), imaging, the Internet of Things (IoT), cloud and grid computing, association rule mining, recommender systems, wireless sensor networks, blockchain technologies, and vehicular networks. He actively contributes to the scientific community as a technical reviewer for several high-impact journals and leading international conferences.

ABDUL RAUF received the master's MS(CS) degree in computer science from COMSATS Institute of Information Technology, Islamabad, Pakistan, in 2007, and the Ph.D. degree from the School of Computing, Universiti Teknologi Malaysia (UTM), Johor Bahru, Malaysia, in 2018. He is currently a Professor with the Department of Computer Science, The University of Faisalabad, Faisalabad, Punjab, Pakistan. Retain a list of numerous research articles published in good-quality International Journals. His research interests include network security, cyber-security, next-generation enterprise security, applied cryptography, cloud security, IoT, and end-to-end quality of services (QoS) in network communication. He is a member of the IEEE Technical Committee. He serves as a reviewer, a technical, and an editorial advisory board member for many International Journals.

MAJID HUSSAIN (Senior Member, IEEE) is currently the Dean and a Faculty Member of Information Technology, and a Professor of Computer Science Department with The University of Faisalabad. He has a rich academic experience of over 20 years in the top ranking universities of the region including COMSATS, UET Lahore, and GC Faisalabad. He has been the ChairPerson of Computer Science Department with COMSATS and GC University Faisalabad. Currently, he is leading the research groups of Blockchain and Biomedical diagnostics with TUF. He has lead the research group of Mobile Communications and Pervasive Computing with Computer Science Department, CUI Sahiwal. He has supervised around 50 thesis (M.S./Ph.D.) in the area of artificial intelligence, blockchain, UAVs, visual sensor networks/image processing, and wireless sensor networks and published his work in well reputed international Journals. He has won around ten national and an international research projects with considerable funding volume. He has acquired multiple international/national trainings with CISCO, Huawii and strategic ones in Europe. His research interests include blockchain, artificial intelligence, UAVs, and visual sensor networks. He has hosted many summits, workshops, seminars and trainings for Faculty Member and Research Students. He has organized a number of conferences as the General Chair and been the part of many ones as the Co-General Chair, the Technical Co-Chair, invited speaker, Session Chair, and has published a good number of research articles in national and international conference.