Environmental Economics & Natural Resources Vol(issue), PP.
.atu.ac.ir
DOI:

AI-Enhanced Smart Contracts for Sustainable Resource Management A Framework for Adaptive Environmental Governance and Economic Efficiency

Ali Sohofi

Computer Engineering Department Shahab Danesh University, Iran
Email: sohofi@shdu.ac.ir

Abstract

Background and Problem Statement:

The digital management of natural resources and environmental governance has increasingly turned toward blockchain technology due to its inherent transparency, decentralization, and tamper-resistant record-keeping. Smart contracts—self-executing agreements coded directly onto the blockchain—have become the cornerstone of this innovation, automating processes in decentralized finance (DeFi), supply chain management, and carbon credit markets without the need for intermediaries. By enforcing obligations automatically when specific conditions are met, smart contracts reduce transaction costs and enhance trust among disparate stakeholders.

However, a fundamental limitation creates a bottleneck for the broader adoption of blockchain in complex environmental scenarios: traditional smart contracts are inherently static and deterministic. Once deployed, their code is immutable, and they function strictly on pre-defined "if/then" logic. This rigidity renders them inefficient when confronting the dynamic, real-world conditions often found in natural resource management, such as fluctuating environmental regulations, variable resource availability, and complex, subjective dispute resolution scenarios. For instance, a standard smart contract cannot inherently interpret ambiguous legal language regarding land conservation rights or adjust execution based on unforeseen weather patterns affecting agricultural yields. Consequently, the current generation of

blockchain governance often requires manual intervention to handle exceptions, negating the efficiency gains of automation.

To address these limitations, Artificial Intelligence (AI) has emerged as a transformative solution, offering capabilities in adaptive decision-making, predictive analytics, and automated risk assessment. This research posits that integrating AI with blockchain infrastructure can evolve decentralized governance from rigid automation to intelligent, context-aware execution.

Research Objectives:

The primary objective of this study is to propose and validate a conceptual framework for AI-enhanced smart contracts designed specifically for sustainable resource management and environmental governance. This framework aims to bridge the gap between on-chain deterministic execution and off-chain intelligence.

Specifically, the research focuses on three critical applications where this integration can yield high economic and governance value:

1. AI-Assisted Dispute Resolution: Utilizing Natural Language Processing (NLP) to interpret contractual ambiguities and automate conflict resolution in Decentralized Autonomous Organizations (DAOs).

2. Adaptive Gas Fee Optimization: Leveraging machine learning (ML) algorithms to predict network congestion and dynamically adjust transaction fees, thereby minimizing the carbon footprint and economic cost of blockchain operations.

3. Automated Risk Assessment: Deploying AI-driven fraud detection models to evaluate the legitimacy of transactions, such as carbon credit verification, ensuring environmental compliance.

Methodology and Proposed Framework:

The study employs a constructive research methodology, developing a comprehensive architectural framework that integrates Solidity-based smart contracts with AI oracles. The proposed framework operates on three layers:

the On-Chain Smart Contract Layer, the AI/Oracle Interface Layer, and the Off-Chain AI Processing Layer.

- The AI-Oracle Bridge: Recognizing that smart contracts cannot directly access external data, the framework utilizes AI-enhanced oracles. These oracles do not merely fetch data but process it using ML models to ensure accuracy and reliability before relaying actionable insights to the blockchain.
- Privacy-Preserving Mechanisms: To address privacy concerns inherent in public blockchains, the methodology incorporates Zero-Knowledge Proofs (ZKPs). This allows the AI models to process sensitive user data off-chain and generate a cryptographic proof of the result (e.g., a risk score) which is then verified on-chain without revealing the underlying private data.
- Technical Implementation: The feasibility of the framework is demonstrated through the development of sample smart contracts written in Solidity.
  - Dispute Resolution: A contract is designed to query an AI oracle that utilizes NLP to analyze text and resolve disputes regarding carbon credit validity, returning a verified outcome to the ledger.
  - Gas Optimization: An "EcoFriendlyGasOptimizer" contract interacts with a predictive ML model to schedule transactions during off-peak times, reducing energy intensity and cost.
  - Risk Compliance: An "EnvironmentalCompliance" contract uses an oracle to assign risk scores to actors based on emission data, flagging anomalies indicative of "greenwashing" or fraud.

Key Findings and Discussion:

The research demonstrates that AI-enhanced smart contracts are technically feasible and offer significant advantages over traditional static models.

- Enhanced Adaptability and Efficiency: The sample implementations confirm that smart contracts can successfully trigger dynamic execution pathways based on AI insights. For example, the gas fee optimization model illustrates how predictive analytics can lower transaction costs and reduce the energy waste associated with high-congestion periods. This is crucial for "Green Blockchain" initiatives, ensuring that the environmental governance tool itself does not become an environmental liability.

- Intelligent Governance: The framework shows that AI can effectively handle subjective tasks previously requiring human intervention. In dispute resolution, NLP models can analyze evidence and legal precedents to suggest or implement fair resolutions, significantly accelerating governance processes in Environmental DAOs.
- Security and Fraud Prevention: The integration of AI-driven risk assessment provides a proactive defense mechanism. Unlike static rules, ML models can learn from historical fraud patterns to identify new anomalies in real-time, such as falsified carbon credit data. The addition of ZKPs ensures that this enhanced security does not come at the cost of user privacy.

However, the study also identifies critical challenges. Oracle vulnerabilities remain a primary risk; if the AI oracle is manipulated, the smart contract will execute flawed decisions. Furthermore, AI model bias poses an ethical risk, where training data flaws could lead to unfair dispute outcomes or discriminatory risk assessments. Finally, the computational overhead of complex AI models necessitates off-chain processing to remain economically viable, as running these models directly on-chain is cost-prohibitive.

Policy Implications and Future Directions:

The integration of AI and blockchain holds profound implications for environmental policy and economic resource management.

- Economic Efficiency in Carbon Markets: The framework offers a pathway for more transparent and efficient carbon trading. By automating compliance verification and fraud detection, the system builds greater trust in decentralized environmental markets, encouraging broader participation.
- Regulatory Frameworks: As decision-making shifts to AI algorithms, regulatory bodies must develop frameworks to recognize AI-arbitrated outcomes as legally binding and ensure that AI models are transparent and auditable. Policies must mandate "Explainable AI" (XAI) and blockchain-based audit trails to mitigate bias and liability issues.
- Sustainability of Digital Infrastructure: The findings highlight the necessity of Layer 2 scaling solutions and off-chain computing to align the energy consumption of digital governance with sustainability goals.

Policymakers should encourage the adoption of "Green AI" principles to minimize the carbon footprint of the governance infrastructure itself.

In conclusion, this research validates that while challenges regarding security and regulation persist, AI-enhanced smart contracts represent a necessary evolution for decentralized environmental governance. Future work must focus on decentralized AI model training (Federated Learning) and robust oracle consensus mechanisms to fully realize the potential of intelligent, autonomous resource management systems.

Keywords: Artificial Intelligence, Digital Environmental Governance, Sustainable Resource Management, Green Blockchain, Carbon Markets, AI in Natural Resources, Economic Efficiency

1. Introduction

Blockchain technology has revolutionized digital transactions by enabling decentralized, transparent, and tamper-resistant record-keeping (Nakamoto, 2008). Smart contracts, self-executing agreements stored on the blockchain, further enhance this innovation by automating processes without intermediaries (Szabo, 1997). However, smart contracts are inherently static and lack adaptability, making them inefficient in handling dynamic real-world conditions such as fluctuating environmental regulations and dynamic resource availability, and complex dispute resolution scenarios (Atzei et al., 2017).

AI has emerged as a potential solution to these limitations, offering adaptive decision-making, predictive analytics, and automated risk assessments (Salah et al., 2019). By integrating AI into smart contracts, blockchain governance can evolve from rigid automation to intelligent, context-aware execution (Hussain & Al-Turjman, 2021). This integration can improve efficiency, security, and fairness in decentralized ecosystems, particularly in Environmental Decentralized Autonomous Organizations (DAOs), Green bond settlements, and legal dispute resolution mechanisms (Casino et al., 2019; Liang et al., 2017).

This paper proposes a conceptual framework for AI-enhanced smart contracts, focusing on three key areas:

- AI-Assisted Dispute Resolution: Leveraging NLP models to interpret contractual terms, resolve ambiguities, and provide automated legal insights.
- Adaptive Gas Fee Optimization: Using machine learning algorithms to predict network congestion and dynamically adjust gas fees for efficient transaction processing.
- Automated Risk Assessment: Deploying AI-driven fraud detection models to evaluate transaction legitimacy, reducing vulnerabilities in blockchain-based financial systems.

To illustrate these concepts, we provide sample Solidity smart contracts that demonstrate the feasibility of integrating AI-generated insights into blockchain applications. Additionally, we discuss the challenges and limitations of AI-enhanced smart contracts, particularly in terms of security, privacy, and computational overhead.

The rest of this paper is structured as follows: Section 2 reviews related works on AI and blockchain integration. Section 3 presents the proposed framework and its key components. Section 4 outlines sample smart contracts demonstrating AI-driven automation. Section 5 discusses security considerations and potential challenges. Finally, Section 6 concludes with future research directions.

2. Theoretical Foundations

2.1 Introduction to Smart Contracts

Smart contracts are self-executing agreements where the terms are written into code (Wu et al., 2022). They operate on a blockchain, a decentralized ledger, automatically enforcing obligations when conditions are met (Kontos et al., 2024). This automation increases transparency and efficiency (Mohanta et al., 2018). Smart contracts use

"if/then" logic: upon condition completion, actions execute automatically. The blockchain provides a secure, immutable infrastructure(Wu et al., 2022). Once deployed, code cannot be altered, ensuring a tamper-proof record. Decentralization means verification by multiple nodes, enhancing security (Wu et al., 2022).

Traditional smart contracts offer deterministic execution, always producing the same output for the same inputs (Alp et al., 2022). This ensures consensus and reliability. Automation is key, enabling self-execution without manual intervention (Ravisankar, 2025), increasing efficiency and reducing disputes. Examples include DeFi, real estate, and supply chain management (Mohanta et al., 2018).

Despite benefits, traditional smart contracts lack adaptability. Immutability makes updates difficult (Zou et al., 2021). They rely on predefined conditions coded at creation (Sirena & Patti, 2021), lacking the ability to interpret context or make decisions based on unforeseen data (Hupe, 2024). This limits their use to simple agreements where all contingencies are known.

2.2 The Role of AI in Smart Contracts

AI enables machines to learn, reason, and make decisions. AI excels at analyzing data, finding patterns, and making predictions, automating decision-making (Patel, 2024). Key AI techniques for smart contracts include machine learning, neural networks, and decision trees, providing a foundation for adaptable and intelligent contracts.

AI can overcome the limitations of traditional smart contracts by adding adaptability and intelligence. Adaptability comes from AI's ability to learn from data, adjust contract terms in real-time, and predict risks, making contracts more responsive (Patel, 2024). Intelligence is added through AI's capacity to analyze complex data and make data-driven decisions without explicit pre-programming, allowing AI-enhanced smart contracts to manage more complex agreements (Patel,

2024). AI uses techniques like neural networks, machine learning algorithms, and natural language processing (Virovets et al., 2024).

2.3 AI-Enhanced Smart Contract Execution

AI has the potential to revolutionize the execution of smart contracts by enabling dynamic adjustments to contract terms based on real-time data. Traditional smart contracts, once deployed, operate according to a fixed set of rules. However, by integrating AI, these contracts can monitor and analyze real-world data streams through mechanisms like oracles, and subsequently modify their terms or trigger different execution pathways based on the insights derived from this data (R. Gupta et al., 2020). For instance, in a supply chain smart contract, AI could analyze real-time weather data or traffic conditions to predict potential perishable agricultural goods. Based on this prediction, the contract could automatically adjust delivery schedules, notify stakeholders, or even trigger penalties as per the agreed terms (Badruddoja et al., 2021). This dynamic adjustment capability makes AI-enhanced smart contracts significantly more flexible and responsive to the complexities of real-world scenarios compared to their static counterparts (Ouyang et al., 2022).

Furthermore, AI can facilitate AI-powered dispute resolution and the development of self-adjusting governance models within smart contract frameworks (Pasupuleti, 2025). When disputes arise in traditional smart contracts, resolving them often requires manual intervention or reliance on external legal systems. By integrating AI, smart contracts can be equipped with the ability to analyze evidence, interpret land use rights for conservation using NLP, and even suggest or automatically implement resolutions based on predefined rules and learned patterns from past disputes (Vijay Shelake, 2025). This can lead to faster, more efficient, and potentially fairer dispute resolution processes within the decentralized environment (Vijay Shelake, 2025). Similarly, for DAOs governed by smart contracts, AI can enable self-adjusting governance models. AI algorithms can analyze the performance of the DAO,

monitor community sentiment, and even propose or automatically implement changes to governance rules or operational parameters to optimize the organization's effectiveness and resilience (Karthikeyan, 2024). This capability for continuous self-improvement and adaptation represents a significant advancement in decentralized governance.

AI-enhanced smart contract execution opens up a wide range of example applications across various industries. In the realm of environmental markets, AI can drive gas fee optimization in blockchain networks like Ethereum (Pasupuleti, 2025). By predicting network congestion, AI helps schedule transactions during off-peak times, optimizing economic costs and reducing the energy intensity per transaction. By using machine learning, AI algorithms can suggest optimal gas fees for transactions, helping users save costs and ensure timely processing (Kowalski, 2024). This dynamic optimization is particularly valuable during periods of high network activity where gas prices can fluctuate significantly (Ferenczi & Bădică, 2024). Another crucial application is AI-based compliance monitoring in carbon trading markets (Pasupuleti, 2025). By analyzing transaction patterns, identifying anomalies, and leveraging machine learning to learn from past instances of fraud, AI can significantly enhance the security of carbon credit transactions executed through smart contracts (Krichen, 2023). This proactive detection capability can help prevent financial losses and build greater trust in decentralized resource management systems (Luo et al., 2025). These examples illustrate the tangible benefits of integrating AI into the execution phase of smart contracts, leading to greater efficiency, cost-effectiveness, and security across different application domains (Pranto et al., 2022).

2.4 AI and Oracles: Bridging Blockchain with Off-Chain Intelligence

Oracles connect blockchains with off-chain data, enabling smart contracts to interact with the real world (Virovets et al., 2024). Smart contracts cannot directly access external data like prices or weather

(Ezzat et al., 2022). Oracles securely fetch and verify this data from sources like APIs and IoT devices, relaying it to smart contracts to trigger execution (T et al., 2025), expanding their applications.

AI can enhance the accuracy and reliability of oracles (Noei Teymoordash et al., 2025). Traditional oracles can be prone to inaccuracies. AI-enhanced oracles use machine learning to analyze data from multiple sources, identify inconsistencies, and provide more accurate information (Kalpinagarajarao, 2025). For example, in prediction markets, AI oracles could analyze news to verify event outcomes, improving the reliability of data used by smart contracts (Armstrong & O'Rorke, 2017).

Security concerns exist with AI-powered oracles, including data manipulation and single points of failure. Manipulated data sources could lead to incorrect information and harmful outcomes (Shaverdian, 2019). Centralized AI oracles could also be single points of failure (Gao et al., 2025). Decentralized oracle networks using consensus mechanisms across multiple oracles help mitigate these risks. Research also focuses on developing AI models to detect manipulated data (Mosa et al., 2024).

2.5 Smart Contract Adaptability with AI

Traditional smart contracts have static logic, fixed at deployment, limiting their ability to adapt (Reshi et al., 2023). AI-driven adaptive contract logic allows smart contracts to dynamically adjust based on real-time data and learned patterns (Badruddoja et al., 2021). Machine learning models analyze data and modify contract execution (Vionis & Kotsilieris, 2023). For example, in a supply chain, an AI contract could monitor shipment sensor data and adjust terms based on temperature deviations, making them more versatile (Ouyang et al., 2022).

Self-improving contracts learn and evolve over time using AI learning models (Pasupuleti, 2025). They analyze past executions and update their code to improve efficiency or fairness (Paul, 2021). For

instance, a decentralized insurance contract could use machine learning to analyze claims data and adjust risk assessment to prevent fraud, allowing continuous improvement without manual updates (Pranto et al., 2022).

An example is smart contracts adjusting insurance premiums based on AI risk predictions. Traditional insurance uses static risk assessments. AI-enhanced smart contracts could dynamically adjust premiums based on real-time data and AI predictions (Sajid, 2025). For example, in agricultural crop insurance, real-time weather and soil moisture data could lead to premium adjustments, creating more personalized and potentially fairer insurance models (S. Gupta et al., 2022).

Traditional smart contracts offer deterministic execution and automation but lack adaptability. AI can introduce adaptability and intelligence through machine learning, NLP, and predictive analytics. AI can enable dynamic adjustments to contract terms, enhance oracles, and facilitate self-improving contracts.

To demonstrate these concepts practically, Section 3 will introduce sample Solidity-based smart contracts with AI functionalities, illustrating the translation of these theoretical principles into working solutions.

3. Proposed Framework: AI-Enhanced Smart Contracts

The integration of AI with blockchain presents new opportunities for enhancing smart contract functionality. This section introduces a conceptual framework for AI-enhanced smart contracts, focusing on three primary applications: AI-assisted dispute resolution, adaptive gas fee optimization, and automated risk assessment. Each component leverages AI techniques to improve the efficiency, adaptability, and security of smart contracts. Figure 1 depicts the proposed framework.

3.1 AI-Assisted Dispute Resolution

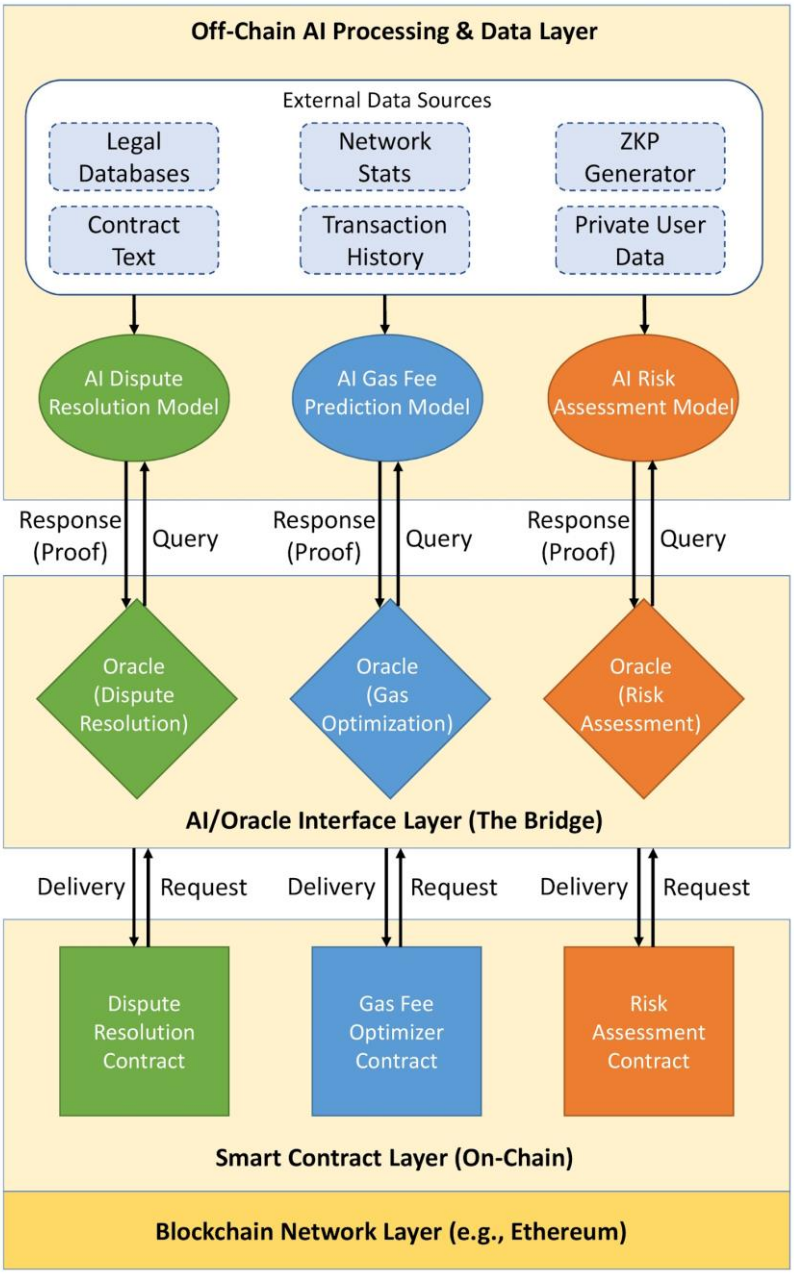

Figure 1- **Proposed Framework for AI-Enhanced Governance (Adaptable for Environmental Resource Management).**

strictly follow pre-programmed logic without the flexibility to interpret ambiguities in contractual agreements. However, real-world contracts often involve complex legal language, unforeseen circumstances, and subjective interpretations. To address these challenges, we propose integrating NLP models with smart contracts to facilitate automated dispute resolution. Key components are:

- *Smart Contract Interpretation Layer:* Uses NLP models to analyze contractual clauses and detect inconsistencies or ambiguities.
- *Decentralized AI Arbitration:* AI-driven dispute resolution mechanisms evaluate evidence and provide recommendations within DAOs.
- *Oracles for Legal Precedents:* AI-powered oracles fetch external legal rulings and case law relevant to disputes.

A Solidity-based dispute resolution contract can interact with an AI oracle to analyze contract terms and provide dispute outcomes based on pre-trained legal models.

```
pragma solidity ^0.8.0;
contract DisputeResolution {
    address public oracle; // AI-powered dispute
resolution oracle
    constructor(address _oracle) {
        oracle = _oracle;
    }
    function resolveDispute(bytes32 carbonCreditID)
public view returns (string memory) {
        // Query AI oracle for dispute resolution
        return "Dispute resolved: Verification
Successful: Carbon Credits Validated.";
    }
}
```

3.2 Adaptive Gas Fee Optimization

Transaction costs (gas fees) fluctuate based on network congestion, often leading to inefficient cost allocation. AI-driven predictive modeling can optimize gas fee calculations by analyzing network activity and recommending dynamic fee adjustments. Key components are:

- AI-Based Network Congestion Prediction: Uses historical transaction data to estimate future congestion levels.
- Dynamic Gas Fee Adjustments: Smart contracts adjust fees in real time based on AI-generated insights.
- Priority Transaction Scheduling: AI determines when to execute transactions at optimal gas prices.

A contract can interact with an AI model via an oracle to set optimal gas fees dynamically.

```
pragma solidity ^0.8.0;
contract EcoFriendlyGasOptimizer {
    address public gasOracle;
    constructor(address _gasOracle) {
        gasOracle = _gasOracle;
    }
    function getOptimizedGasFee() public view returns
(uint256) {
        // Query AI to find lowest energy-intensity block
        return 5000000000; // Example: 5 Gwei based on AI
estimation
    }
}
```

3.3 Automated Risk Assessment for Blockchain Transactions

Security risks such as fraudulent transactions, smart contract vulnerabilities, and Sybil attacks pose challenges to blockchain ecosystems. AI-driven fraud detection models can assess transaction legitimacy, reducing risks in environmental compliance systems. Key components are:

• Machine Learning-Based Greenwashing Detection: AI models analyze transaction patterns to identify anomalies.

• Risk Scoring Mechanism: Assigns risk scores to transactions, flagging suspicious activities.

• ZKPs for Privacy: AI risk assessments can be performed off-chain and verified on-chain without revealing sensitive data. To implement this, the AI risk assessment model would operate off-chain, potentially processing sensitive transaction details or user data. Upon calculating a risk score or classification, instead of transmitting the raw data or the full model output via the oracle, a ZKP (such as a zk-SNARK or zk-STARK) would be generated. This proof cryptographically attests that the AI computation was executed correctly on the (private) input data and yielded a specific result (e.g., 'low risk' or a specific score range) without revealing the input data itself. The oracle relays this compact proof to the smart contract, which then performs an efficient on-chain verification of the proof. If the proof is valid, the contract can trust the assessment outcome and proceed accordingly, ensuring both data privacy and computational integrity.

A Solidity contract that interacts with an AI model for fraud detection.

```
pragma solidity ^0.8.0;
contract EnvironmentalCompliance {
    address public riskOracle;
    constructor(address _riskOracle) {
        riskOracle = _riskOracle;
    }
    function assessTransaction(address user, uint256
amount) public view returns (string memory) {
        // Query AI oracle for risk assessment
        return "Compliance Verified: Sustainable
Practice";
    }
}
```

3.4 Framework Overview

The proposed AI-enhanced smart contract framework combines oracles, AI models, and blockchain to create a more intelligent, adaptive, and secure decentralized ecosystem. These integrations enable:

- More efficient dispute resolution in decentralized governance.
- Lower transaction costs through AI-driven gas fee optimization.
- Higher security in resource transactions via AI-based fraud detection.

By implementing these AI-powered features, smart contracts can evolve beyond static execution models into intelligent, self-optimizing blockchain applications.

4. Sample Smart Contracts for AI-Enhanced Blockchain Governance

To demonstrate the feasibility of AI-enhanced smart contracts, this section presents Solidity-based implementations for the three key applications discussed in Section 3: AI-assisted dispute resolution, adaptive gas fee optimization, and automated risk assessment. These smart contracts are designed to interact with AI oracles that provide off-chain intelligence to improve decision-making on the blockchain.

4.1 AI-Assisted Dispute Resolution Smart Contract

The Objective is to enable smart contracts to interpret contractual clauses and resolve disputes using an AI-powered oracle that analyzes contract terms.

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;
contract DisputeResolution {
    address public oracle; // AI-powered dispute resolution oracle
    mapping(bytes32 => string) public disputeOutcomes;
    event DisputeSubmitted(bytes32 indexed carbonCreditID, string outcome);
```

```
    constructor(address _oracle) {
        oracle = _oracle;
    }
    function    resolveDispute(bytes32    carbonCreditID)
public {
        //  Simulate  AI  verification  of  carbon  credit
validity
        string  memory  outcome  =  "Dispute  resolved:
Verification Successful: Carbon Credits Validated.";
        disputeOutcomes[carbonCreditID] = outcome;
        emit DisputeSubmitted(carbonCreditID, outcome);
    }
    function  getDisputeOutcome(bytes32  carbonCreditID)
public view returns (string memory) {
        return disputeOutcomes[carbonCreditID];
    }
}
```

The progress will be as follows:

1. A dispute is submitted by providing a contract hash.
2. The contract queries an AI oracle (simulated in this example) to determine the dispute resolution outcome.
3. The resolved outcome is stored on-chain and can be accessed later.

4.2 Adaptive Gas Fee Optimization Smart Contract

The Objective is to dynamically adjust gas fees based on network congestion predictions provided by an AI model.

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;
contract EcoFriendlyGasOptimizer {
    address public gasOracle; // AI-powered gas fee oracle
    event GasFeeUpdated(uint256 newGasFee);
    constructor(address _gasOracle) {
        gasOracle = _gasOracle;
    }
    function  getOptimizedGasFee()  public  pure  returns
(uint256) {
```

```
        // Simulated AI oracle prediction (In practice,
this would be fetched from an oracle)
        return 5000000000; // Example: 5 Gwei
    }
    function executeTransaction() public payable {
        uint256 optimizedGas = getOptimizedGasFee();
        emit GasFeeUpdated(optimizedGas);
        // Transaction logic using optimized gas fee
    }
}
```

The progress will be as follows:

1. The contract queries an AI oracle for the optimal gas fee based on predicted network congestion.
2. The returned gas fee is dynamically updated before executing transactions.
3. This allows users to minimize transaction costs by executing trades when network congestion is low.

4.3 AI-Powered Risk Assessment Smart Contract

The Objective is to assess transaction legitimacy using AI-driven fraud detection models to mitigate risks in blockchain compliance applications.

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;
contract EnvironmentalCompliance {
    address public riskOracle; // AI-powered risk analysis
oracle
    mapping(address => uint256) public riskScores;

    event RiskEvaluated(address indexed user, uint256
riskScore);
    constructor(address _riskOracle) {
        riskOracle = _riskOracle;
    }
    function assessTransaction(address user, uint256
amount) public {
```

```
        // Simulated AI risk assessment (In practice, this
would be fetched from an oracle)
        uint256 riskScore = (emissions > permittedLimit)
? 80 : 20; // Example: High-risk if carbon output exceeds
quota
        riskScores[user] = riskScore;
        emit RiskEvaluated(user, riskScore);
    }
    function getRiskScore(address user) public view
returns (uint256) {
        return riskScores[user];
    }
}
```

The progress will be as follows:

1.The contract queries an AI oracle to assign a risk score to each transaction.

2.If the transaction amount is high, it is flagged as high risk.

3.Risk scores are stored on-chain and can be used by regulatory applications to prevent fraud.

4.4 Privacy-Preserving AI Risk Assessment Implementation

To demonstrate the technical implementation of privacy-preserving AI risk assessment using Zero-Knowledge Proofs, an expanded architecture is presented that outlines the specific components and their interactions. The AI risk assessment model operates in a secure off-chain environment where it receives encrypted transaction data (e.g., sender/receiver addresses, amount, transaction history), processes this data through a pre-trained ML model (e.g., Random Forest or Neural Network), and produces a risk score or classification (e.g., on a scale of 0-100 or categorical labels).

After the AI model generates a risk assessment, a zk-SNARK or zk-STARK (Oude Roelink et al., 2024) proof is created. This process takes transaction data, AI model parameters, and risk assessment results as input. It defines a circuit that verifies the AI computation followed the specified algorithm, creates a witness of the computation without

revealing the private data, and generates a compact proof that can be verified on-chain. Sample pseudocode for the proof generation demonstrates this process:

```
function generateRiskAssessmentProof(transactionData,
modelParameters, riskScore) {
    // Define arithmetic circuit for AI model computation
    let circuit = defineAICircuit(modelParameters);
    // Generate witness from private data
    let witness = circuit.generateWitness({
        privateInputs: transactionData,
        publicOutput: riskScore
    });
    // Generate the actual ZKP
    let proof = circuit.generateProof(witness);
    return {
        proof: proof,
        publicInputs: riskScore
    };
}
```

The on-chain verification is handled through an enhanced EnvironmentalCompliance smart contract that includes ZKP verification:

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;
import "./ZKPVerifier.sol"; // Library for ZKP
verification
contract EnhancedEnvironmentalCompliance {
    address public riskOracle;
    ZKPVerifier public verifier;
    mapping(address => uint256) public riskScores;
    event RiskEvaluated(address indexed user, uint256
riskScore, bool verified);
    constructor(address _riskOracle, address _verifier) {
        riskOracle = _riskOracle;
        verifier = ZKPVerifier(_verifier);
    }
    function assessTransactionWithZKP(
        address user,
        bytes memory proof,
        uint256 claimedRiskScore
    ) public {
```

```
        // Verify the ZKP without revealing the
transaction details
        bool isValid = verifier.verifyProof(proof,
claimedRiskScore);
        require(isValid, "Invalid risk assessment
proof");
        // Store the verified risk score
        riskScores[user] = claimedRiskScore;
        emit RiskEvaluated(user, claimedRiskScore, true);
    }
    function getRiskScore(address user) public view
returns (uint256) {
        return riskScores[user];
    }
}
```

This implementation can leverage established ZKP frameworks, including libsnark or the Groth16 proving system for zk-SNARKs, and StarkWare's Cairo language or the Ethereum STARK prover for zk-STARKs.

4.5 Security and Efficiency Considerations

While AI-enhanced smart contracts offer numerous advantages, they also introduce security and efficiency concerns:

- *Oracle Security:* Since AI models operate off-chain, trust in oracles is crucial. Adversaries could manipulate oracle data to alter dispute resolutions, gas fees, or risk assessments.

- *Computational Overhead:* AI models require significant processing power. Lightweight models or off-chain processing via oracles help mitigate blockchain performance issues.

- *Bias in AI Models:* Smart contracts rely on AI-generated outputs, which can be biased if the training data is flawed. Ensuring transparency in AI model training is essential.

- *Privacy Considerations:* ZKPs can be integrated to provide privacy-preserving AI-driven decisions without exposing sensitive transaction data.

Table 1 summarizes sample smart contracts.

5. Challenges and Security Considerations

While AI-enhanced smart contracts introduce significant advancements in blockchain governance, they also pose various technical, security, and ethical challenges. This section discusses key issues associated with integrating AI into smart contracts, including oracle vulnerabilities, AI model reliability, computational overhead, regulatory concerns, and privacy risks.

5.1 Oracle Vulnerabilities and Data Integrity

AI-powered smart contracts rely on oracles to fetch off-chain intelligence, such as dispute resolution outcomes, gas fee predictions, and risk scores. However, oracles introduce security risks, including single points of failure, where a compromised centralized oracle can manipulate smart contract decisions. Data tampering attacks are another concern, as malicious actors may inject biased or incorrect AI-generated data to influence contract execution. Additionally, oracle

Table 1 - **Summary of sample smat contracts**

Feature	Smart Contract	Key Functionality	AI Role
Dispute Resolution	DisputeResolution	Resolves contract disputes using AI-powered analysis	NLP model for contract interpretation
Gas Fee Optimization	EcoFriendlyGasOptimizer	Adjusts gas fees dynamically based on network congestion	AI model predicts congestion levels
Risk Assessment	EnvironmentalCompliance	Assigns risk scores to transactions to prevent fraud	AI-driven fraud detection

downtime can cause smart contracts relying on AI insights to fail to function properly.

To mitigate these risks, decentralized oracles such as Chainlink (Breidenbach et al., 2021) can be implemented to reduce reliance on a single data source. Multi-oracle consensus mechanisms, where multiple AI models verify data accuracy, can further enhance reliability. Additionally, cryptographic proofs, such as zero-knowledge proofs, can be introduced to validate AI-generated outputs before execution.

5.2 AI Model Reliability and Bias

AI models are only as good as the data they are trained on. Poor training data or biased models can lead to unfair dispute resolutions, where AI-driven legal interpretations may produce biased outcomes. Incorrect fraud detection can also arise, causing AI to falsely flag legitimate transactions as fraudulent. Moreover, manipulated gas fee predictions can be exploited to favor specific user groups.

Ensuring AI models undergo transparent training and auditing can help minimize biases. The use of Explainable AI (XAI) techniques enhances the interpretability of AI decisions. Establishing a blockchain-based AI audit trail ensures that model updates and training data modifications remain immutable and verifiable.

5.3. Environmental Externalities and the Economics of Computation

The integration of AI into blockchain architectures introduces significant computational demands, creating a critical challenge in the context of environmental economics: the energy intensity of digital governance. While AI models optimize resource allocation and gas fees , the computational power required to train and query these models contributes to the overall carbon footprint of the network.

From an economic perspective, if the energy cost of running the AI governance model exceeds the value of the resources saved, the system

becomes economically inefficient. Running complex AI tasks directly on-chain is not only computationally prohibitive but also environmentally unsustainable due to the high energy consumption associated with redundant node verification.

To mitigate these environmental externalities, this framework proposes offloading heavy AI processing to off-chain networks and utilizing Layer 2 scaling solutions such as Optimistic Rollups and zk-Rollups. These mechanisms significantly reduce the energy intensity per transaction, ensuring that the smart contract ecosystem remains a viable tool for sustainable resource management rather than a contributor to energy waste. Furthermore, the adoption of "Green AI" principles—using lightweight models for inference —is essential to align the technical architecture with the sustainability goals of environmental and natural resource economics.

5.4 Economic Scalability and Barriers to Entry

AI models require significant computational resources, making on-chain AI execution impractical. Running AI-driven tasks such as dispute resolution, gas fee optimization, or fraud detection directly on a blockchain may increase gas costs, making transactions expensive. High computational requirements translate into prohibitive transaction costs (gas fees), potentially excluding smaller environmental stakeholders (e.g., local NGOs or small-holder farmers) from participating in the governance model. This creates an economic barrier to entry that must be addressed via Layer 2 solutions to ensure equitable access.

To address these issues, AI processing can be offloaded to off-chain computing networks like Fetch.ai (Fetch AI: Open Platform to Build AI Apps & Services, n.d.) and Bittensor (Rao et al., 2020), with results retrieved via oracles. Using lightweight AI models for on-chain inference reduces execution overhead. Additionally, implementing

Layer 2 scaling solutions, such as Optimistic Rollups and zk-Rollups, can lower computation costs while maintaining efficiency.

5.5 Privacy and Security Risks

AI-enhanced smart contracts process sensitive data, such as emission records and dispute resolutions. If not managed properly, this can lead to privacy breaches, where unauthorized parties gain access to transaction details. AI-driven identity tracking may also compromise user anonymity in DeFi and DAO ecosystems. Furthermore, attackers may exploit AI decision-making by manipulating AI models to alter contract outcomes.

Addressing these risks involves leveraging cryptographic techniques like zero-knowledge proofs to generate verifiable proofs without revealing sensitive data. Federated Learning can be utilized to enable decentralized AI model training without exposing raw data. Additionally, Homomorphic Encryption can allow AI models to process encrypted data securely, preserving confidentiality.

5.6 Regulatory and Legal Considerations

Integrating AI into smart contracts presents legal and compliance challenges, particularly in jurisdictions with strict data protection and environmental regulations. Key concerns include the legal status of AI dispute resolutions, as courts may not recognize AI-based contract interpretations as legally binding. Compliance with sustainability regulations is another challenge, as AI-driven gas fee optimization and risk assessments may require regulatory approval. Additionally, liability issues arise when determining legal responsibility for erroneous AI-driven contract decisions.

To navigate these challenges, hybrid AI-human dispute resolution systems can be implemented, where AI suggests outcomes but human oversight ensures compliance. AI-based financial smart contracts should be designed to adhere to Anti-Money Laundering (AML) and Know Your Customer (KYC) regulations. Establishing regulatory

sandboxes allows AI-enhanced smart contracts to be tested under controlled legal frameworks before full deployment.

Table 2 Summarizes the challenges and mitigation strategies.

6. Conclusion and Future Directions

The integration of AI with blockchain-based smart contracts presents a transformative approach to enhancing decentralized governance, dispute resolution, gas fee optimization, and risk assessment. By leveraging AI-driven smart contracts, blockchain networks can achieve greater efficiency, adaptability, and intelligence, overcoming some of the current limitations of deterministic contract execution. This paper explored the theoretical underpinnings of AI-powered smart contracts, introduced sample implementations in Solidity, and analyzed critical security and regulatory challenges associated with AI-enhanced decision-making in blockchain environments. While AI can

Table 2 - **Summary of challenges and mitigation strategies**

Challenge	Potential Risk	Mitigation Strategy
Oracle Vulnerabilities	Data manipulation, single point of failure	Use decentralized oracles, multi-source validation, cryptographic proofs
AI Model Bias	Unfair decisions, incorrect fraud detection	Transparent AI training, XAI, blockchain-based AI audit trails
Computational Overhead	High gas costs, slow execution	Off-chain AI processing, lightweight AI models, Layer 2 scaling solutions
Privacy Risks	Data exposure, identity tracking	ZKPs, federated learning, homomorphic encryption
Regulatory Challenges	Legal recognition, compliance issues	Hybrid AI-human decision-making, AML/KYC compliance, regulatory sandboxes

significantly improve contract automation, several technical and ethical challenges—such as oracle vulnerabilities, AI model bias, computational overhead, and regulatory uncertainty—must be addressed to ensure trust and reliability. AI-enhanced smart contracts have the potential to redefine digital governance models, making decentralized ecosystems more adaptive and intelligent, but their adoption requires robust security mechanisms, transparent AI models, and compliance with legal frameworks to ensure fair, accountable, and scalable implementations.

While this study establishes a theoretical foundation for AI-powered smart contracts, several areas require further research and development. One critical focus is the advancement of decentralized AI models for blockchain governance, which could operate without centralized control to enhance dispute resolution and resource trading applications. The integration of federated learning may enable AI models to be trained across multiple blockchain nodes while preserving privacy. Additionally, the development of privacy-preserving AI mechanisms, such as ZKPs and homomorphic encryption, could allow AI-powered decisions without exposing sensitive transaction data or enable encrypted AI computations directly within smart contracts. Improving AI oracles and data integrity is also crucial, as multi-source AI oracles could mitigate data manipulation risks and enhance contract execution reliability. Leveraging decentralized oracle networks like Chainlink (Breidenbach et al., 2021) and Witnet (de Pedro et al., 2017) would further strengthen the resilience of AI-driven smart contracts. Moreover, AI-powered auditing tools could automatically detect vulnerabilities before deployment, providing real-time security analysis for blockchain applications and reducing the risk of exploits and errors.

Regulatory frameworks must also evolve to accommodate AI-driven smart contracts, recognizing AI-based contract decisions in arbitration and dispute resolution while ensuring fairness, accountability, and compliance in smart contract automation. The convergence of AI and blockchain is still in its early stages, but it has the potential to

revolutionize decentralized decision-making by making smart contracts more adaptive and intelligent. Achieving this vision requires a multidisciplinary approach, combining advancements in blockchain security, AI ethics, cryptographic privacy, and regulatory compliance. As research progresses, AI-driven smart contracts could bridge the gap between traditional legal systems and decentralized governance, unlocking new possibilities for automated trading systems, fair dispute resolution, and secure digital transactions. By addressing the challenges and leveraging innovative solutions, AI-enhanced smart contracts can play a pivotal role in shaping the future of Web3, DeFi, and decentralized governance models.

Funding

This research received no specific grant from any funding agency.

Conflict of Interest

The authors declare no conflict of interest.

ORCID

References

Alp, E. C., Băsescu, C., Tennage, P. N., Kocher, N., Bosson, G., & Ford, B. A. (2022). *Efficient Deterministic Execution of Smart Contracts*.

Armstrong, S., & O'Rorke, X. (2017). *Good and safe uses of AI Oracles*. http://arxiv.org/abs/1711.05541

Atzei, N., Bartoletti, M., & Cimoli, T. (2017). *A Survey of Attacks on Ethereum Smart Contracts (SoK)* (pp. 164–186). https://doi.org/10.1007/978-3-662-54455-6_8

Badruddoja, S., Dantu, R., He, Y., Upadhayay, K., & Thompson, M. (2021). Making Smart Contracts Smarter. *2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, 1–3. https://doi.org/10.1109/ICBC51069.2021.9461148

Breidenbach, L., Cachin, C., Chan, B., Coventry, A., Ellis, S., Juels, A., Koushanfar, F., Miller, A., Magauran, B., & Moroz, D. (2021). Chainlink 2.0: Next steps in the evolution of decentralized oracle networks. *Chainlink Labs*, *1*, 1–136.

Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and Informatics*, *36*, 55–81. https://doi.org/10.1016/j.tele.2018.11.006

de Pedro, A. S., Levi, D., & Cuende, L. I. (2017). *Witnet: A Decentralized Oracle Network Protocol*. https://doi.org/10.13140/RG.2.2.28152.34560

Ezzat, S. K., Saleh, Y. N. M., & Abdel-Hamid, A. A. (2022). Blockchain Oracles: State-of-the-Art and Research Directions. *IEEE Access*, *10*, 67551–67572. https://doi.org/10.1109/ACCESS.2022.3184726

Ferenczi, A., & Bădică, C. (2024). Prediction of Ethereum gas prices using DeepAR and probabilistic forecasting. *Journal of Information and Telecommunication*, *8*(1), 18–32. https://doi.org/10.1080/24751839.2023.2250113

Fetch AI: Open platform to build AI Apps & Services. (n.d.). Retrieved March 30, 2025, from https://fetch.ai/

Gao, B., Wang, Y., Wei, Q., Liu, Y., Goh, R. S. M., & Lo, D. (2025). *AiRacleX: Automated Detection of Price Oracle Manipulations via LLM-Driven Knowledge Mining and Prompt Generation*. http://arxiv.org/abs/2502.06348

Gupta, R., Tanwar, S., Al-Turjman, F., Italiya, P., Nauman, A., & Kim, S. W. (2020). Smart Contract Privacy Protection Using AI in Cyber-Physical Systems: Tools, Techniques and Challenges. *IEEE Access*, *8*, 24746–24772. https://doi.org/10.1109/ACCESS.2020.2970576

Gupta, S., Ghardallou, W., Pandey, D. K., & Sahu, G. P. (2022). Artificial intelligence adoption in the insurance industry: Evidence using the technology–organization–environment framework. *Research in International Business and Finance*, *63*, 101757. https://doi.org/10.1016/j.ribaf.2022.101757

Hupe, A. (2024). *When to Use Smart Contracts Instead of Traditional Contracts–A Conceptual Analysis*.

Hussain, A. A., & Al-Turjman, F. (2021). Artificial intelligence and blockchain: A review. *Transactions on Emerging Telecommunications Technologies*, *32*(9). https://doi.org/10.1002/ett.4268

Kalpinagarajarao, G. K. (2025). AI-enhanced oracle platforms: A new era of predictive healthcare analytics and cybersecurity. *International Journal of Multidisciplinary Research and Growth Evaluation*, *6*(1), 1823–1830. https://doi.org/10.54660/.IJMRGE.2025.6.1-1823-1830

Karthikeyan, C. (2024). AI (Artificial Intelligence) for Conflict Resolution and Negotiation. In *Navigating Organizational Behavior in the Digital Age With AI* (pp. 21–50). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3693-8442-8.ch002

Kontos, C., Panagiotakopoulos, T., & Kameas, A. (2024). Applications of Blockchain and Smart Contracts to Address Challenges of Cooperative, Connected, and Automated Mobility. *Sensors*, *24*(19), 6273. https://doi.org/10.3390/s24196273

Kowalski, I. (2024). AI-Driven Decentralized Financial Networks: Emerging Challenges, Technological Advancements, and Future Research Directions. *International Journal of AI, BigData, Computational and Management Studies*, *5*(2), 1–8. https://doi.org/10.63282/n7a3x375

Krichen, M. (2023). Strengthening the Security of Smart Contracts through the Power of Artificial Intelligence. *Computers*, *12*(5), 107. https://doi.org/10.3390/computers12050107

Liang, X., Shetty, S., Tosh, D., Kamhoua, C., Kwiat, K., & Njilla, L. (2017). ProvChain: A Blockchain-Based Data Provenance Architecture in Cloud Environment with Enhanced Privacy and Availability. *2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID)*, 468–477. https://doi.org/10.1109/CCGRID.2017.8

Luo, B., Zhang, Z., Wang, Q., Ke, A., Lu, S., & He, B. (2025). AI-powered Fraud Detection in Decentralized Finance: A Project Life Cycle Perspective. *ACM Computing Surveys*, *57*(4), 1–38. https://doi.org/10.1145/3705296

Mohanta, B. K., Panda, S. S., & Jena, D. (2018). An Overview of Smart Contract and Use Cases in Blockchain Technology. *2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, 1–4. https://doi.org/10.1109/ICCCNT.2018.8494045

Mosa, M. J., Barhoom, A. M., Alhabbash, M. I., Harara, F. E. S., Abu-Nasser, B. S., & Abu-Naser, S. S. (2024). *AI and Ethics in Surveillance: Balancing Security and Privacy in a Digital World*.

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*.

Noei Teymoordash, S., Zendehdel, H., Norouzi, A. R., & Kashian, M. (2025). Diagnostic accuracy of artificial intelligence algorithms to predict remove all macroscopic disease and survival rate after complete surgical cytoreduction in patients with ovarian cancer: a systematic review and meta-analysis. *BMC Surgery*, *25*(1), 27. https://doi.org/10.1186/s12893-025-02766-3

Oude Roelink, B., El-Hajj, M., & Sarmah, D. (2024). Systematic review: Comparing zk-SNARK, zk-STARK, and bulletproof protocols for privacy-preserving authentication. *SECURITY AND PRIVACY*, *7*(5). https://doi.org/10.1002/spy2.401

Ouyang, L., Zhang, W., & Wang, F.-Y. (2022). Intelligent contracts: Making smart contracts smart for blockchain intelligence. *Computers and Electrical Engineering*, *104*, 108421. https://doi.org/10.1016/j.compeleceng.2022.108421

Pasupuleti, M. K. (2025). *Automated Smart Contracts: AI-powered Blockchain Technologies for Secure and Intelligent Decentralized Governance*. https://doi.org/10.62311/nesx/rrv425

Patel, O. (2024). AI-Driven Smart Contracts. *Journal of Artificial Intelligence & Cloud Computing*, 1–9. https://doi.org/10.47363/JAICC/2024(3)E120

Paul, C. (2021). *AI-Powered Simulations for Smart Contract Testing*.

Pranto, T. H., Hasib, K. T. A. M., Rahman, T., Haque, A. B., Islam, A. K. M. N., & Rahman, R. M. (2022). Blockchain and Machine Learning for Fraud Detection: A Privacy-Preserving and Adaptive Incentive Based Approach. *IEEE Access*, *10*, 87115–87134. https://doi.org/10.1109/ACCESS.2022.3198956

Rao, Y., Steeves, J., Shaabana, A., Attevelt, D., & McAteer, M. (2020). Bittensor: A peer-to-peer intelligence market. *ArXiv Preprint ArXiv:2003.03917*.

Ravisankar, P. (2025). SMART CONTRACTS: UNDERSTANDING THE TECHNOLOGY BEHIND SELF-EXECUTING BLOCKCHAIN AGREEMENTS. *INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING AND TECHNOLOGY*, *16*(1), 3288–3300. https://doi.org/10.34218/IJCET_16_01_229

Reshi, I., Khan, M., Shafi, S., Sholla, S., Assad, A., & Shafi, H. (2023). *AI-Powered Smart Contracts: The Dawn of Web 4. O*. https://doi.org/10.36227/techrxiv.22189438.v1

Sajid, M. I. (2025). Reviewing the New AI Paradigm in Property and Casualty Insurance. *Open Journal of Applied Sciences*, *15*(02), 480–500. https://doi.org/10.4236/ojapps.2025.152031

Salah, K., Rehman, M. H. U., Nizamuddin, N., & Al-Fuqaha, A. (2019). Blockchain for AI: Review and Open Research Challenges. *IEEE Access*, *7*, 10127–10149. https://doi.org/10.1109/ACCESS.2018.2890507

Shaverdian, P. (2019). Start with trust: Utilizing blockchain to resolve the third-party data breach problem. *UCLA L. Rev.*, *66*, 1242.

Sirena, P., & Patti, F. P. (2021). Smart Contracts and Automation of Private Relationships. In *Constitutional Challenges in the Algorithmic Society* (pp. 315–330). Cambridge University Press. https://doi.org/10.1017/9781108914857.017

Szabo, N. (1997). Formalizing and securing relationships on public networks. *First Monday*.

T, M., Makkithaya, K., V. G., N., & T, V. M. (2025). Blockchain oracles for decentralized agricultural insurance using trusted IoT data. *Frontiers in Blockchain*, *7*. https://doi.org/10.3389/fbloc.2024.1481339

Vijay Shelake. (2025). Blockchain and AI in Digital Contracts: A Legal Review of Smart Contract Enforcement. *Journal of Information Systems Engineering and Management*, *10*(23s), 166–170. https://doi.org/10.52783/jisem.v10i23s.3689

Vionis, P., & Kotsilieris, T. (2023). The Potential of Blockchain Technology and Smart Contracts in the Energy Sector: A Review. *Applied Sciences*, *14*(1), 253. https://doi.org/10.3390/app14010253

Virovets, D., Obushnyi, S., Zhurakovskyi, B., Skladannyi, P., & Sokolov, V. (2024). Integration of smart contracts and artificial intelligence using cryptographic oracles. *Classic, Quantum, and Post-Quantum Cryptography 2024*, *3829*, 39–46.

Wu, C., Xiong, J., Xiong, H., Zhao, Y., & Yi, W. (2022). A Review on Recent Progress of Smart Contract in Blockchain. *IEEE Access*, *10*, 50839–50863. https://doi.org/10.1109/ACCESS.2022.3174052

Zou, W., Lo, D., Kochhar, P. S., Le, X.-B. D., Xia, X., Feng, Y., Chen, Z., & Xu, B. (2021). Smart Contract Development: Challenges and Opportunities. *IEEE Transactions on Software Engineering*, *47*(10), 2084–2106. https://doi.org/10.1109/TSE.2019.2942301

JEL Classification: Q56 , E01 , C23