# Decentralized AI Model Marketplace: A Blockchain-Powered Platform for Secure Model Sharing, Licensing, and Provenance

Vishal Subhash Chavan, Jambukeshwar Pujari
*Department of Computer Science and Business Systems*
*Kolhapur Institute of Technology's College of Engineering, Kolhapur, India*
vsc251044@gmail.com, pujari.jambukeshwar@kitcoek.in

**Abstract**

**The rapid growth of artificial intelligence and machine learning (AI/ML) has created a strong demand for high-quality models, but the lack of secure and transparent platforms for sharing and monetizing these models remains a challenge. This paper presents a decentralized AI model marketplace built on blockchain technology, designed to address issues of model provenance, licensing, and royalty management. The platform enables developers to upload their AI/ML models, ensuring ownership rights and receiving fair compensation for every transaction through smart contract-powered licensing. Buyers can securely purchase and download models with verified claims, while model validation is performed using file extensions without exposing sensitive data. Blockchain's immutable ledger records every purchase and usage, providing complete transparency and reducing the risk of intellectual property theft. Additionally, integrated data analytics offer insights into model performance and market demand, helping both developers and buyers make informed decisions. This decentralized approach fosters trust, encourages innovation, and creates a fair ecosystem for AI/ML model distribution. Through this work, we demonstrate how combining blockchain, AI, and data analytics can revolutionize the digital model marketplace.**

**Index Terms**

Decentralized Marketplace, AI Model Sharing, Blockchain Technology, Smart Contracts, Model Provenance, Royalty Management, Secure Licensing, Machine Learning, Data Analytics, Intellectual Property Protection, Model Validation, Digital Transactions.

## I. Introduction

The rapid advancement of artificial intelligence (AI) and machine learning (ML) has revolutionized industries like healthcare, finance, agriculture, and e-commerce. Despite the proliferation of sophisticated AI/ML models, the current landscape of model sharing and distribution remains plagued by security risks, lack of transparency, and inadequate compensation for developers. Centralized AI marketplaces often rely on intermediaries, leading to intellectual property theft, unauthorized usage, and revenue mismanagement. Developers hesitate to share models due to the absence of robust licensing and royalty enforcement, while buyers face challenges in verifying model credibility and performance. These issues hinder collaboration and innovation, emphasizing the need for a secure and transparent platform for AI model sharing and monetization.

Existing decentralized solutions attempt to address these challenges but remain limited. Kumar [1] proposed a model-sharing marketplace with basic licensing features but lacked comprehensive royalty management and data security. Nguyen et al. [2] integrated blockchain with IoT-driven data sharing, though its scope is restricted to IoT use cases. Pisano et al. [3] introduced Predictchain for collaborative model development but faced issues in ensuring fair compensation and model validation. Le [4] explored blockchain-powered ML model trading in the metaverse but encountered scalability challenges. Sarpatwar [5] emphasized trust via blockchain-secured transactions but lacked performance insights and market demand analytics. These studies highlight the need for a more robust and scalable platform for AI model sharing.

Blockchain technology provides an effective solution through decentralized, transparent, and immutable record-keeping. This paper proposes a decentralized AI model marketplace that leverages blockchain for secure transactions and smart contract-driven licensing. By integrating the MERN stack (MongoDB, Express.js, React.js, Node.js) with blockchain and AI/ML technologies, the platform ensures seamless model uploads, purchases, and automated royalty distribution. Smart contracts enforce licensing agreements, ensuring fair compensation for model creators. Model validation is achieved through file extension analysis without exposing underlying data, maintaining data privacy. Integrated analytics offer insights into model performance and market trends, empowering informed decision-making. This paper presents the system architecture, implementation, and performance evaluation, demonstrating the platform's potential to foster trust, transparency, and innovation in the AI ecosystem.

The diagram 1 illustrates the architecture and workflow of the Decentralized AI Model Marketplace, highlighting the interaction between sellers, buyers, and the Ethereum blockchain. The process begins with both sellers and buyers registering and connecting their crypto wallets. Sellers upload AI/ML model files in ZIP format, which are then securely stored on the blockchain, ensuring immutability and provenance. They can set and modify the price of their models, allowing for flexible

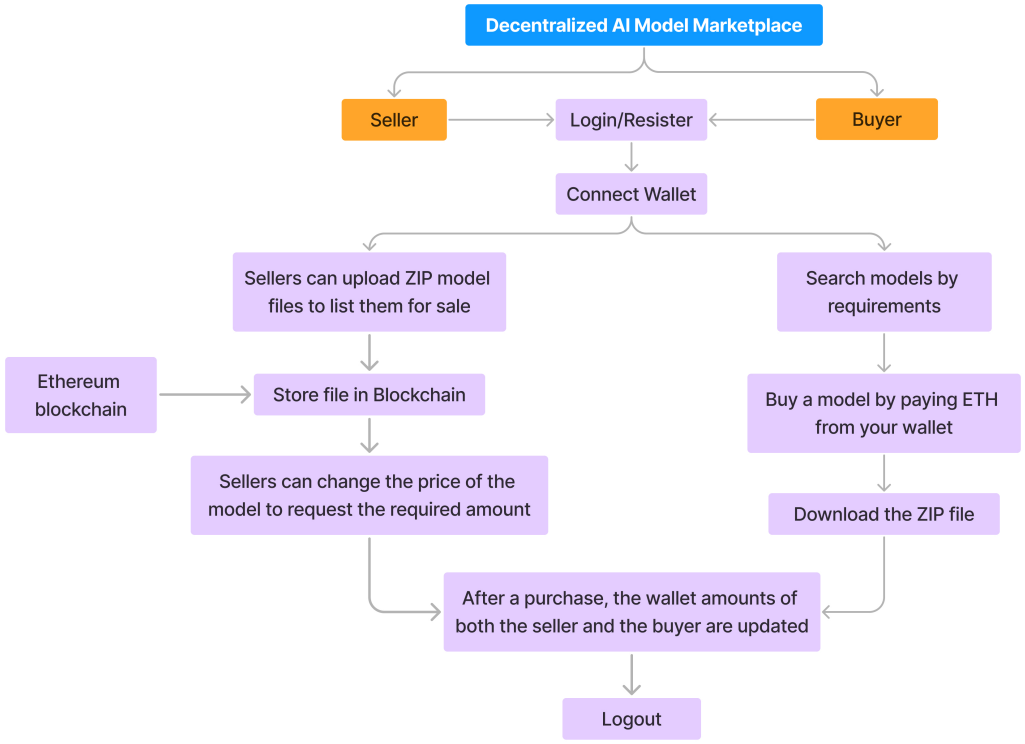


Fig. 1: System Architecture

pricing. Buyers can search for models based on their requirements and purchase them using ETH (Ethereum) from their connected wallets. Once the transaction is completed, the model file becomes available for download, and the wallet balances of both the seller and buyer are updated automatically. This decentralized approach eliminates intermediaries, ensuring transparent transactions and fair royalty distribution. Through the use of blockchain technology, the system guarantees data security, model authenticity, and equitable compensation for developers, creating a robust and efficient ecosystem for AI model trading.

## II. Methodology

This section outlines the design and implementation of the Decentralized AI Model Marketplace, covering system Architecture, technology stack, smart contract implementation, file storage mechanism, AI model validation, machine learning integration, security and scalability, and associated challenges.

### *A. System Architecture*

The Decentralized AI Model Marketplace is built on a blockchain-based infrastructure to ensure secure, transparent, and immutable transactions for AI model trading. The system consists of multiple key modules that interact through smart contracts, decentralized storage, and a MERN-based web platform.

The architecture comprises several core modules:

- **User Module:**
  Supports role-based authentication, allowing users to register as buyers or sellers.Utilizes Ethereum wallets (e.g., MetaMask) for authentication and transactions.Maintains user profiles with transaction history, purchased models, and earnings.
- **AI Model Management Module:**
  Enables sellers to upload AI models in a secure, tamper-proof manner. Utilizes file extension and metadata validation to verify the authenticity of models. Allows sellers to set model prices and licensing terms via smart contracts.
- **Smart Contract Module:**

Implements immutable contracts to handle model purchases, royalties, and usage rights. Automatically distributes payments and enforces licensing agreements. Maintains provenance tracking to ensure transparency in model ownership.

- **Blockchain Storage Module:**
  Utilizes decentralized storage solutions like IPFS or Arweave to store AI models securely. Links file hashes to blockchain transactions, ensuring integrity and preventing tampering. Provides buyers access to purchased models via cryptographic verification.
- **Marketplace Module:**
  Allows buyers to search, filter, and purchase AI models based on requirements. Displays model descriptions, performance metrics, and seller credibility ratings. Integrates with payment gateways for seamless Ethereum-based transactions.

.

The system ensures security, scalability, and efficiency using a combination of blockchain smart contracts, decentralized storage, and a web-based user interface. The next section details the technology stack used for implementation.

### *B. Technology Stack*

The Decentralized AI Model Marketplace leverages a robust and modern technology stack to ensure seamless functionality, security, and scalability. The stack combines web technologies, blockchain protocols, and machine learning tools to create an efficient and decentralized environment for AI model trading.

- **Frontend:**
  **React.js:** Used for building a dynamic and responsive user interface with efficient state management.
- **Backend:**
  **Node.js:** A lightweight and scalable runtime environment for building fast server-side applications. **Express.js:** A minimalist web framework for creating RESTful APIs and handling backend logic. **MongoDB:** A NoSQL database for flexible and efficient storage of user profiles, model metadata, and transaction history.
- **Blockchain:**
  **Ethereum:** The primary blockchain network for deploying smart contracts and handling transactions. **Solidity:** The programming language used to write smart contracts for managing model licensing, payments, and royalties. **Web3.js / Ethers.js:** Libraries for interacting with the Ethereum blockchain from the frontend, enabling wallet connections and contract calls.
- **Decentralized Storage:**
  **IPFS (InterPlanetary File System):** A peer-to-peer protocol for decentralized and secure storage of AI model files.
- **Wallet Integration:**
  **MetaMask:** A widely-used Ethereum wallet for managing user identities and facilitating blockchain transactions.

This technology stack ensures platform efficiency, security, and scalability, providing a seamless experience for AI model transactions. Next, we explore the smart contract implementation behind the platform's core functions.

### *C. Smart Contract Implementation*

The core functionality of the Decentralized AI Model Marketplace is powered by Ethereum-based smart contracts. The smart contract implementation covers model ownership, licensing, pricing, and royalty distribution.

- **Smart Contract Design:**
  **Model Registration:** Each AI/ML model uploaded by a seller is assigned a unique identifier and stored on the Ethereum blockchain. The smart contract records model metadata, pricing, and ownership details. **Licensing and Usage Rights:** Buyers purchase usage rights for a model by executing a transaction on the blockchain. The smart contract ensures that the buyer receives secure access to the model while the seller retains intellectual property rights.
- **Key Functions:**
  - `uploadModel(string modelHash, uint price)`: Allows sellers to list their AI model by providing a hashed file reference and price in ETH.
  - `buyModel(uint modelId)`: Enables buyers to purchase a model by transferring the required ETH amount to the smart contract.
  - `changePrice(uint modelId, uint newPrice)`: Allows the seller to update the model's price.
- **Security Measures:**
  **Ownership Verification:** Only the model's creator can modify or remove their listing. **Payment Security:** Funds are held in the smart contract until the transaction is confirmed on the blockchain. **Immutable Records:** All transactions and ownership changes are permanently recorded on the Ethereum blockchain.
- **Deployment and Interaction:**

**Hardhat:** Tools used to write, compile, and deploy the smart contract on the Ethereum testnet or mainnet. **Web3.js / Ethers.js:** Libraries integrated with the frontend to facilitate interaction between the user interface and the deployed smart contract. **MetaMask Wallet:** Used to sign and confirm transactions securely from the user's end.

The smart contract implementation ensures a trustless, transparent, and efficient marketplace, enabling seamless AI model transactions with automated royalty distribution and ownership validation.

### *D. File Storage Mechanism*

The decentralized nature of the AI Model Marketplace requires a secure, scalable, and immutable file storage solution for AI/ML models.

- **InterPlanetary File System (IPFS):**
  **Decentralized Storage:** IPFS distributes files across a peer-to-peer network, eliminating single points of failure. **Content Addressing:** Each uploaded AI model is hashed, and the resulting unique content identifier (CID) ensures file integrity and prevents duplication. **Efficient Retrieval:** IPFS provides fast and reliable access to model files by retrieving them from the nearest or most accessible node in the network.

### *E. AI Model Validation*

The platform implements both automated and community-driven validation to ensure that models meet their stated performance and functionality.

- **File Type and Structure Validation:**
  **File Extension Checks:** Ensures only legitimate AI/ML model formats (e.g., .h5, .pkl, .onnx) are accepted. **Model Compatibility:** Validates that the uploaded model file can be loaded and executed using common libraries like TensorFlow, PyTorch, or Scikit-learn. **Schema Verification:** Confirms that models contain expected parameters, weights, and configurations.

The combined approach of decentralized storage and rigorous validation mechanisms ensures that the AI Model Marketplace maintains high-quality, secure, and accessible AI/ML models. In the next section, we discuss the integration of machine learning algorithms for data analytics and performance insights.

### *F. Machine Learning Integration*

Machine learning plays a crucial role in enhancing the functionality and user experience of the decentralized AI Model Marketplace. ]

- **Chatbot for User Query Resolution:**
  **Natural Language Processing (NLP):** The chatbot is powered by advanced NLP techniques to understand and respond to user queries in a human-like manner.

### *G. Security and Scalability*

Ensuring the security of AI models, user data, and transactions is paramount in a decentralized environment. Simultaneously, the platform must scale efficiently to accommodate growing demand without compromising performance.

- **Data Encryption:**
  - **On-Chain Data Protection:** Sensitive model metadata is hashed and encrypted before being stored on the Ethereum blockchain.
  - **File Encryption:** AI models stored on IPFS are encrypted to prevent unauthorized access.
  - **End-to-End Encryption:** Communication between buyers, sellers, and the platform is encrypted using protocols like TLS and SSL.
- **Wallet and Payment Security:**
  - **Ethereum Wallet Integration:** Uses MetaMask or similar wallets for secure ETH transactions.
  - **Multi-Signature Transactions:** Ensures high-value transactions require multiple confirmations, reducing the risk of fraud.
  - **Transaction Audits:** All financial transactions are recorded on the blockchain, providing transparent and immutable logs.
- **Scalability Strategies:**
  - **Layer-2 Solutions:** Integrates protocols like `Polygon` to reduce network congestion and lower gas fees.
  - **Off-Chain Storage:** Uses IPFS for model file storage, reducing the on-chain data load and improving transaction speeds.
  - **Sharding:** Plans for future implementation of blockchain sharding to enhance throughput and support parallel processing.

The combined use of advanced machine learning, robust security protocols, and scalable architecture ensures that the AI Model Marketplace remains efficient, reliable, and future-proof.

## III. Results and Discussion

Here is a detailed description of the website's functionality and outputs, accompanied by screenshots. This section provides a comprehensive view of how the website operates and showcases the results, offering valuable insights for the discussion and evaluation of its performance and effectiveness.

### *A. Home Page*

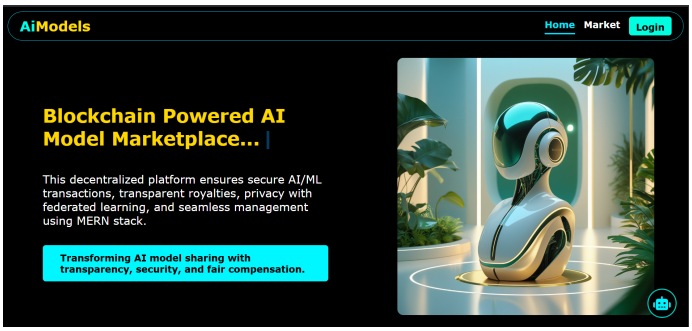


Fig. 2: Home page

The homepage of this platform serves as a comprehensive introduction to the Decentralized AI Model Marketplace, highlighting its significance, benefits, and potential impact on the AI community. It provides a clear overview of how the platform enables secure and transparent transactions for AI model sharing and monetization. The homepage also includes real-world examples of AI model marketplaces and a detailed, step-by-step guide on how users—whether developers or buyers—can participate and make the most of the platform. Designed with an intuitive and user-friendly layout, it features dedicated sections that explain the platform's purpose, showcase success stories and user testimonials, offer educational resources about blockchain and AI model licensing, and provide easy access to a contact form for connecting with the support team. This well-structured homepage ensures that users, even those new to blockchain or AI, can easily understand and navigate the platform's offerings.

### *B. Market Page*

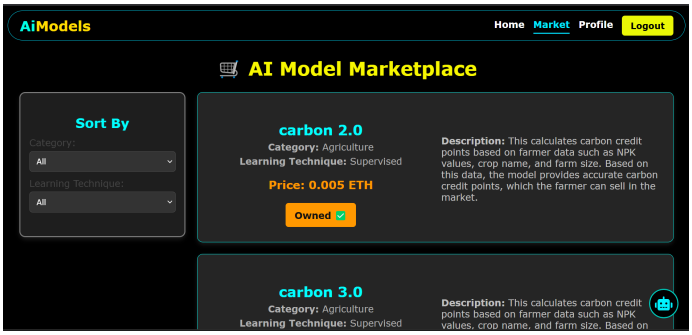


Fig. 3: Market page

The Market page of the platform is a dedicated space for facilitating the buying and selling of AI models. Here, developers can list their models, and buyers can explore a wide range of available options. Upon logging in, users connect their digital wallet, which is used to make secure and transparent transactions in ETH. Every purchase is recorded on the blockchain, ensuring authenticity and ownership. This page also provides filtering options, allowing users to refine their search based on specific requirements like model type, price, and popularity, making it easy to find the right model efficiently.

### *C. profile Page*

The Profile page serves as a personalized space where users can manage their AI models and account details. Through secure wallet-based transactions, users can upload their models to the marketplace and maintain ownership rights, which are immutably recorded on the blockchain. This page also provides options to update model pricing, ensuring flexible control over their offerings. Additionally, users can view a comprehensive list of their uploaded models, track their sales history, and manage their personal profile information, creating a seamless and efficient user experience.

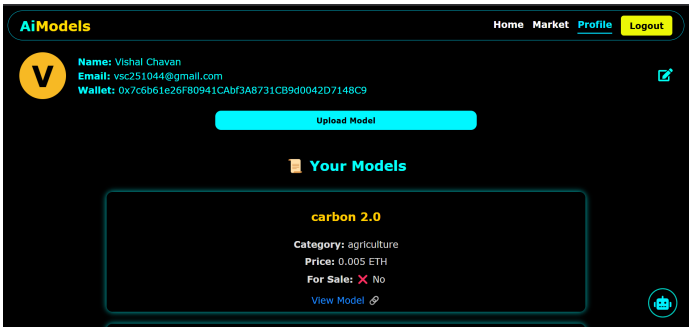


Fig. 4: profile page

### *D. Login Page*

The Login page offers users a simple and convenient way to access the platform. Users can log in either using their Google account or by entering their credentials manually. After logging in with Google, users have the option to set a password on their profile page for future manual login, if needed. The page is designed to be user-friendly and interactive, ensuring a smooth and engaging experience.

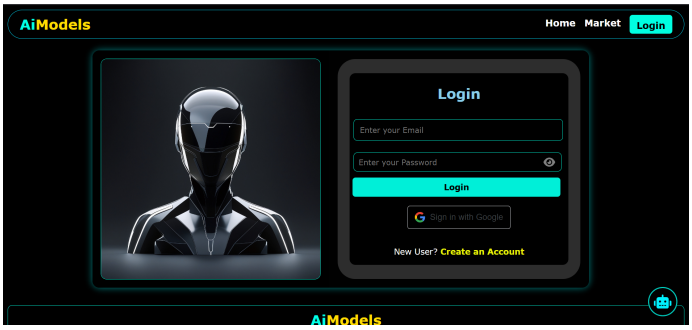


Fig. 5: Login page

In summary, the platform effectively ensures secure model transactions, efficient ownership management, and an intuitive user experience, offering a robust solution for decentralized AI model sharing and monetization.

## IV. Conclusion

In conclusion, the Decentralized AI Model Marketplace offers a secure, transparent, and efficient platform for trading AI and ML models, addressing key challenges like ownership rights, data integrity, and fair compensation. By leveraging the Ethereum blockchain, the platform ensures immutability and trust in transaction records, while decentralized storage through IPFS provides efficient file management. Smart contracts automate licensing and royalty distribution, ensuring model creators are fairly rewarded for each transaction. AI model validation mechanisms, based on file extension and metadata checks, maintain the quality of models without exposing sensitive data. The integration of a chatbot using Natural Language Processing (NLP) enhances user support by resolving queries efficiently. Additionally, the marketplace's security measures, including role-based access control and encrypted transactions, safeguard user data and assets. Scalability is achieved through microservices and off-chain storage, ensuring smooth performance as demand grows. This platform not only democratizes access to high-quality AI models but also sets a new standard for digital asset exchange, fostering global collaboration and innovation in the AI industry.

## References

[1] B. F. Abhishek Kumar, "Marketplace for ai models," Ph.D. dissertation, University of Helsinki, 2020.
[2] S. B. Lam Duc Nguyen, Shashi Raj Pandey, "A marketplace for trading ai models based on blockchain and incentives for iot data," Ph.D. dissertation, 2021.
[3] C. J. P. Matthew T. Pisano, "Predictchain: Empowering collaboration and data accessibility for ai in a decentralized blockchain-based marketplace," Ph.D. dissertation, Rensselaer Polytechnic Institute Troy, NY, USA, 2023.
[4] V. T. T. HUNG DUY LE, "Blockchain-empowered metaverse: Decentralized crowdsourcing and marketplace for trading machine learning data and models," Ph.D. dissertation, Institut national de la recherche scientifique (INRS), University of Quebec, Montreal, QC H5A 1K6, Canada, 2024.
[5] K. Sarpatwar, "Blockchain enabled ai marketplace: The price you pay for trust," Ph.D. dissertation, IBM Research, NY.