Decentralized MLOps and Model Governance via Blockchain and Smart Contracts

Alexandra Ciupahina

Abstract:
This white paper[1] proposes a decentralized platform for orchestrating Machine Learning Operations (MLOps) using blockchain technology and smart contracts. The core idea is to govern and automate key MLOps tasks—including model monitoring, evaluation, retraining, and registration—through programmable smart contracts that interact with a public or permissioned blockchain ledger. A complementary "Model Universe" will serve as a decentralized repository for registered models. Model usage, retraining triggers, and promotion decisions will be handled in a trustless and auditable manner, with an optional native cryptocurrency to power transactions and pay-per-use model inference.

Introduction

As artificial intelligence becomes more widely adopted, the need for transparent, secure, and reproducible machine learning workflows is growing. Traditional MLOps platforms often rely on centralized infrastructure and manual checkpoints for promoting models or triggering retraining. This introduces challenges in accountability, governance, and scalability.

We propose a decentralized MLOps platform that integrates blockchain, smart contracts, and decentralized Oracles to automate and govern the ML lifecycle. The system enables both public and private stakeholders to register, evaluate, and promote machine learning models in a secure and transparent way, while introducing incentives for open-source collaboration and reproducibility.

Proposed Architecture

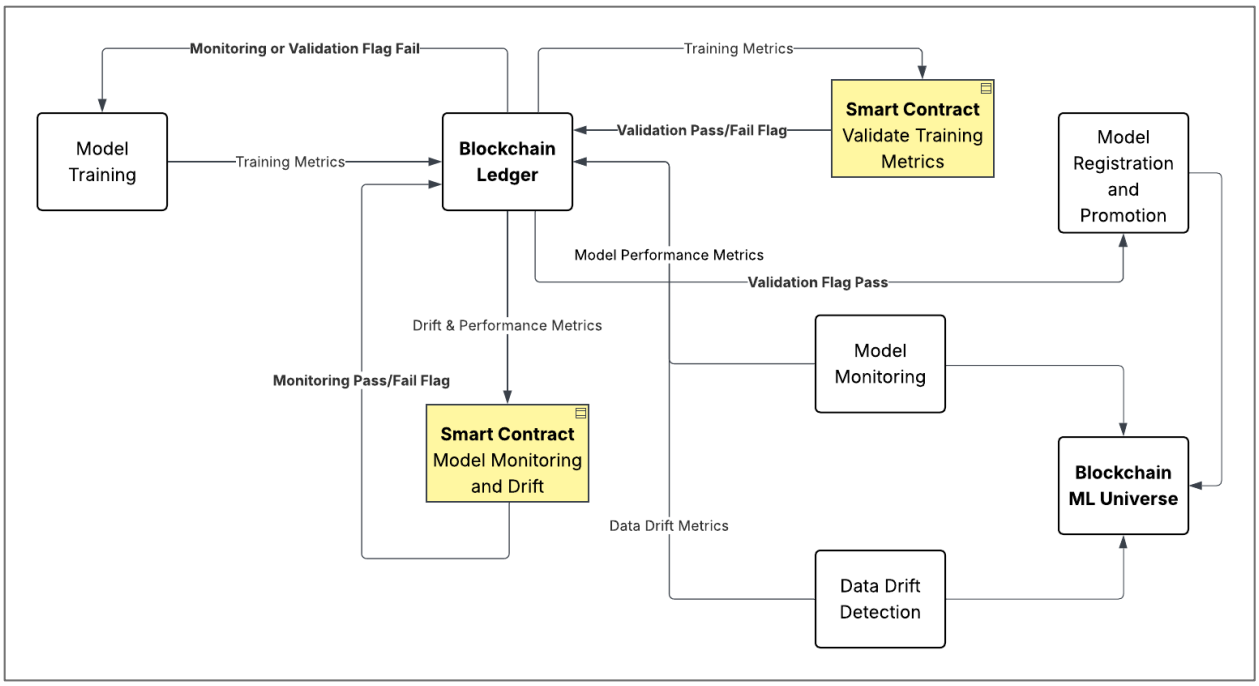
At the core of the system is a blockchain ledger and a set of smart contracts that enforce governance logic.

- **Smart Contracts**: Define the conditions under which a model is eligible for promotion, retraining, or deprecation. These contracts are triggered by updates to the blockchain ledger.

- **Blockchain Ledger**: Stores immutable records of model performance metrics, drift scores, promotion flags, and model registry metadata.
- **Cloud Listener**: A process that continuously monitors the ledger for flags or conditions, and executes corresponding MLOps workflows (e.g., triggering a training job or registering a model).
- **Decentralized Oracles**: Services such as Chainlink (or similar decentralized oracle networks) are used to securely execute off-chain ML tasks (e.g., model training, evaluation, and monitoring) and report results back to the blockchain.

Workflow

1. **Model Evaluation & Monitoring**:
    - After a model completes training or inference tasks, its metrics (e.g., accuracy, precision, drift detection stats) are written to the blockchain via Oracles.
    - Smart contracts monitor these metrics and evaluate whether the model meets the criteria for promotion, retraining, or deprecation.
2. **Model Promotion**:
    - If performance metrics satisfy predefined governance rules, the smart contract updates the ledger with a promotion flag.
    - The cloud listener detects this flag and triggers the model registration workflow.
3. **Model Registration to the Model Universe**:
    - Once promoted, the model is registered on-chain to the **Model Universe**, a decentralized marketplace and repository for ML models.
    - Models can be designated as public or private. Public models are openly accessible to the community, promoting the **democratization of AI** by enabling smaller developers and researchers to share, discover, and monetize pre-trained models.
    - Private models are encrypted and access is governed by smart contracts that act as programmable access control policies, preserving intellectual property for sensitive use cases like finance or defense.
4. **Cryptocurrency and Incentives**:
    - A dedicated cryptocurrency facilitates platform operations:
        - Paying for smart contract execution
        - Logging and querying from the blockchain
        - Pay-per-use inference or model evaluation
        - Monetization of public models



Benefits

- **Trustless Governance**: All model lifecycle decisions are enforced by smart contracts, reducing the risk of human error or bias.
- **Transparency**: Every model registration, promotion, and deprecation event is recorded on-chain.
- **Security & IP Protection**: Sensitive models remain encrypted, and smart contracts control access policies.
- **Incentivization**: Open-source developers are rewarded for publishing performant models to the Model Universe.
- **Decentralization**: Tasks are executed off-chain through decentralized Oracles such as Chainlink, minimizing reliance on centralized compute resources.

Future Work

- Expansion to support multi-cloud orchestration
- Integration with version control for datasets and code
- Reputation scores for contributors and models
- Federated training and edge ML integration

Conclusion

This paper proposes a novel fusion of blockchain, smart contracts, and MLOps automation to create a secure, decentralized ecosystem for model governance. By registering models on-chain through the Model Universe and enabling lifecycle automation through smart contracts and decentralized Oracles, the platform aims to unlock a more open, auditable, and equitable future for artificial intelligence.
