Trust Your Supplier

CHAINYARD

TRUST YOUR SUPPLIER

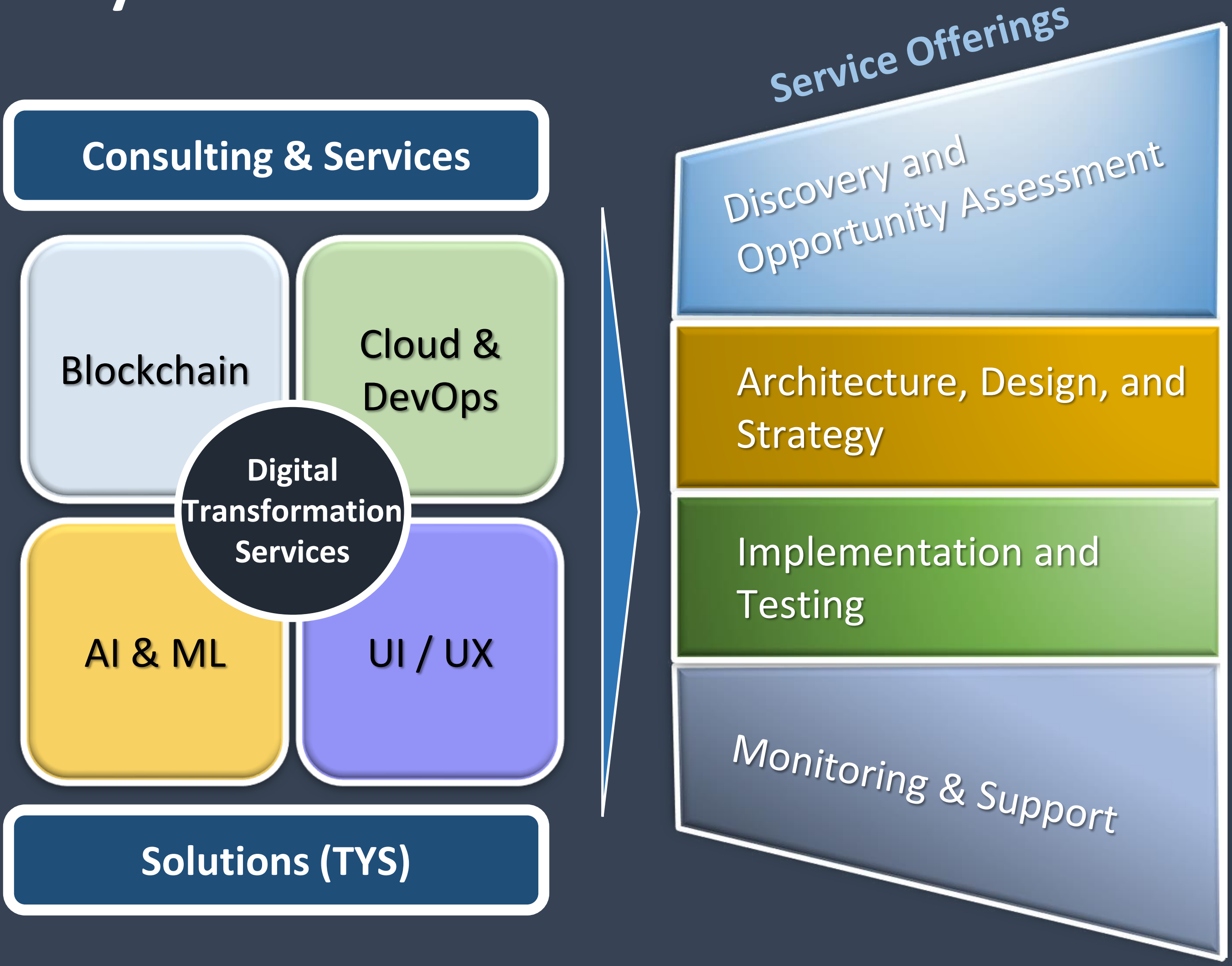
Hyperledger Fabric and AI to Deliver Trusted Enterprise AI Solutions

Hyperledger Meetup – SCM SIG 2024

June 14, 2024

Mohan Venkataraman

Chainyard – What do we do?



Consulting & Services

Blockchain

Cloud & DevOps

Digital Transformation Services

AI & ML

UI / UX

Solutions (TYS)

Service Offerings

Discovery and Opportunity Assessment

Architecture, Design, and Strategy

Implementation and Testing

Monitoring & Support

Clients

NPCI
Avaneer
Lenovo
CyberSettle
Prism
Dept. of Treasury
Shinogi Pharma

IBM
Lenovo
USPS
AAIS
Deloitte
RTI Bahrain & Dubai
Docuvisory
Saudi ARAMCO

Hyperledger Foundation Member since Inception

HELPS THE BUYERS AND SUPPLIERS MANAGE THEIR PARTNERSHIP

Data Governance

Clean, reliable data with ongoing controls

Supplier Digital Wallet

Blockchain-based, let's suppliers do business easily with multiple customers

Reporting & Analytics

AI driven, offers practical strategies for risk mitigation

Discovery & Onboarding

Easily find and engage new suppliers

Risk & Compliance

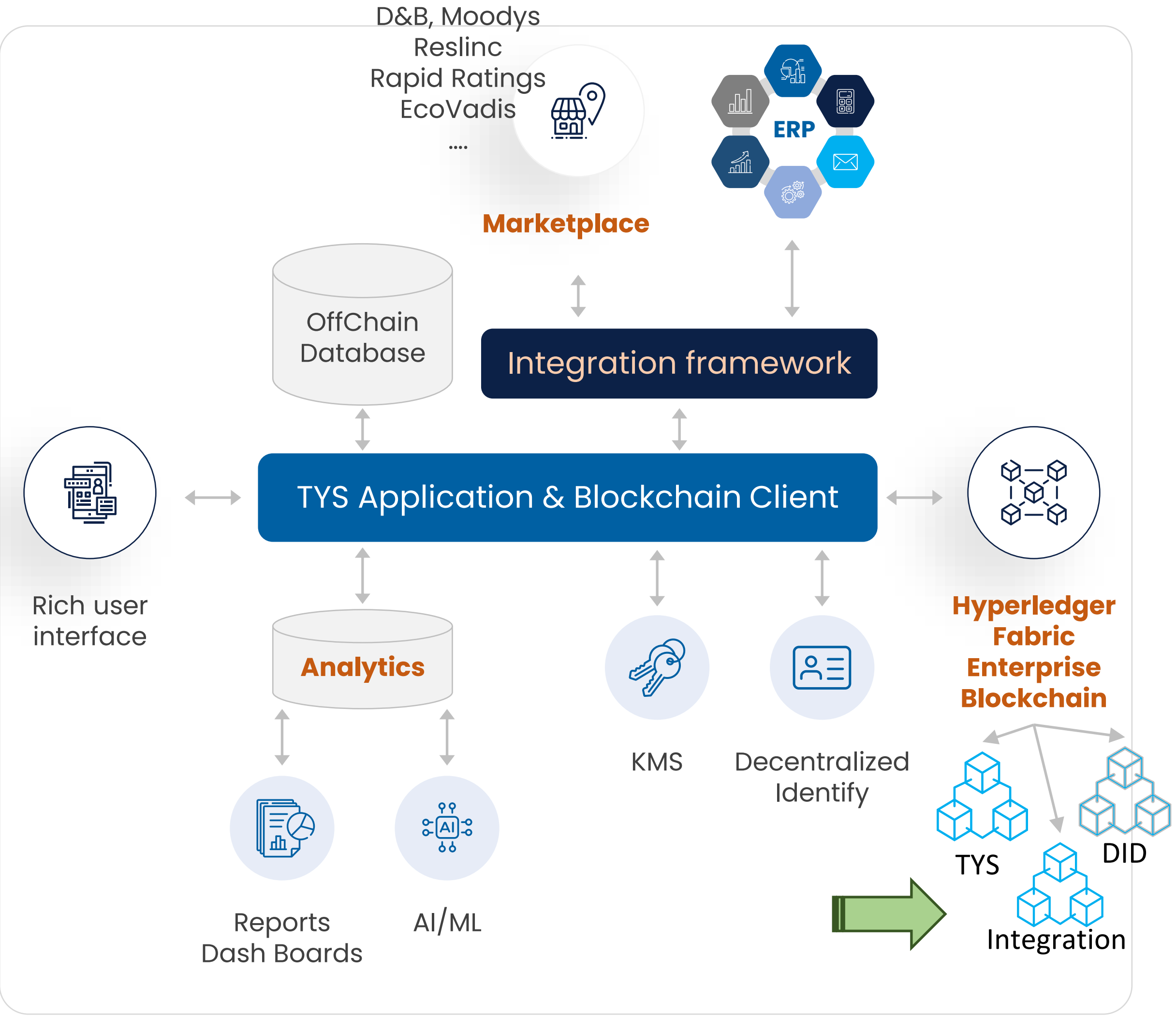
Rigorous ongoing Supplier Compliance Monitoring

Automation & Integration

Easy integration with business ecosystems

Trust Your Supplier enabled by Hyperledger Fabric

- Hyperledger Fabric Blockchain enabled Hybrid Decentralized Network with Fabric Certificate Authority
- Non-Invasive loosely-coupled integration framework
- NodeJS & FabricSDK-based client
- Supports Third Party Marketplace
- Off-Chain Database based on MongoDB
- Integrates with Enterprise ERPs and Solution
- Globally resolvable Digital Identity W3C standards with Enterprise Digital Wallet
- Advanced UI/UX Framework built with React JS
- Key Management Services support Supplier and human-user Public/Private Keys based on ECDSA
- Analytics Database with PowerBI integration for dashboards and analytics



D&B, Moodys
Resllnc
Rapid Ratings
EcoVadis
....

Marketplace

ERP

OffChain Database

Integration framework

Rich user interface

TYS Application & Blockchain Client

Hyperledger Fabric Enterprise Blockchain

Analytics

KMS

Decentralized Identify

Reports Dash Boards

AI/ML

TYS

DID

Integration

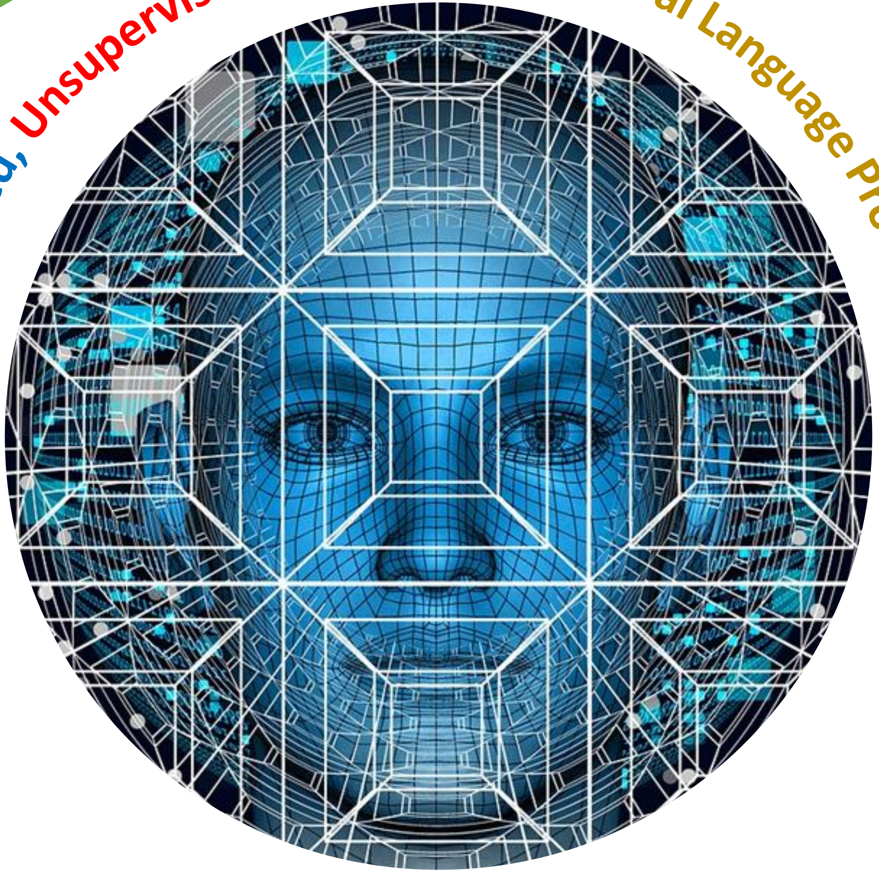
Multi-Channel | Private-Ledger Capability | Multi-Zone HA | Permissioned Architecture

Trust Your Supplier

Main Categories in AIML

- **Computer Vision:** Creating new ways for computers to gain a higher level of understanding of the visual world around us
- ✓ **Core Machine Learning**: Building algorithms inspired by, and compatible with human cognition
- **Embodied AI/Robotics:** Developing embodied agents that assist and collaborate with people in virtual and physical spaces
- ✓ **Generative AI**: Creating AI systems that empower anyone to bring their imagination to life
- ✓ **Natural Language Processing**: Advancing the state-of-the-art in natural language understanding and generation
- **Society & Responsible AI:** Delivering AI research innovations and guidelines designed to help everyone benefit from AI
- **Speech & Audio:** Creating spoken language technology to help people build community and connect with others

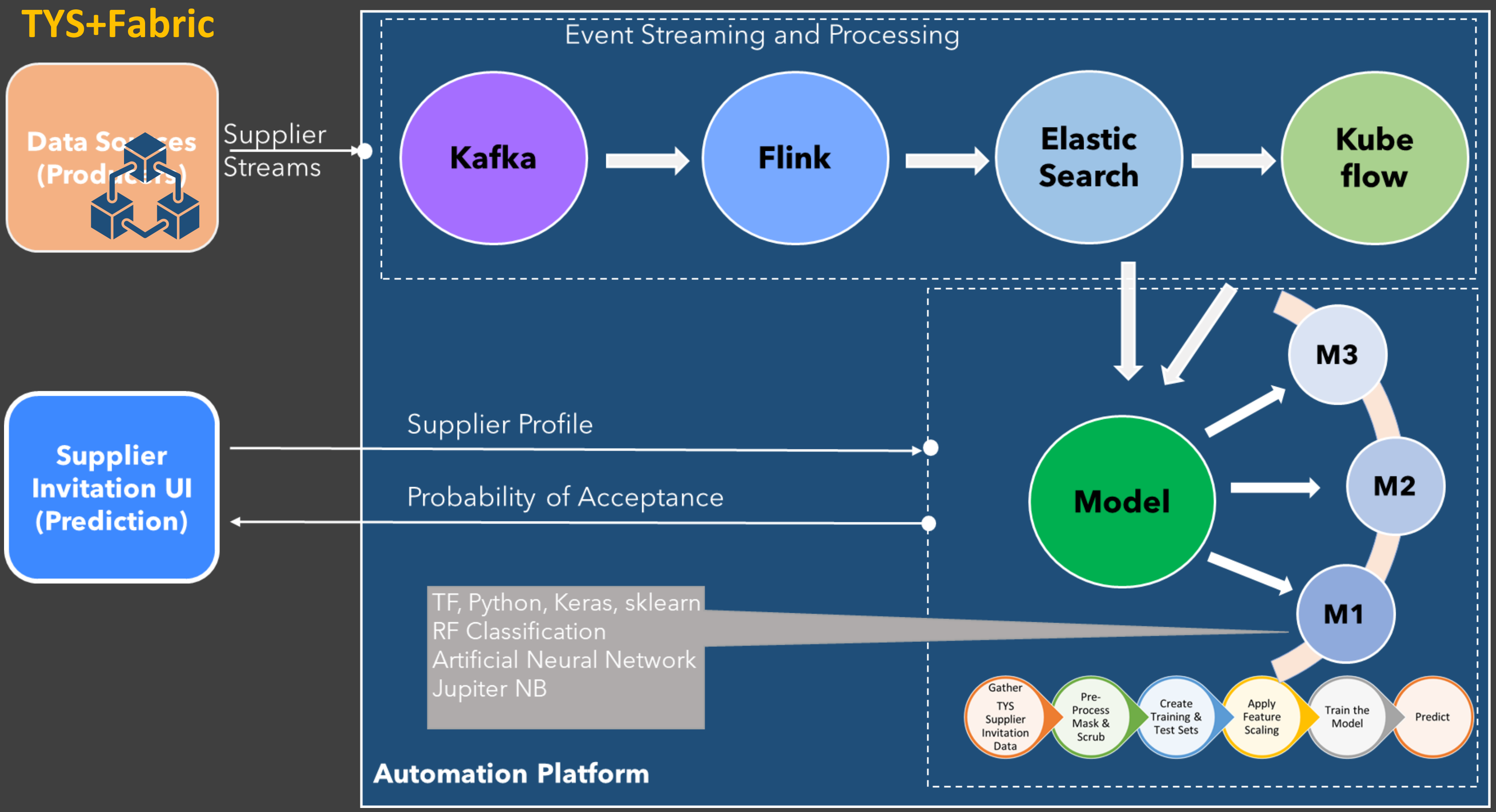
Supervised, Unsupervised, Reinforced, Natural Language Processing



TYS Focus

Supplier Invitation Process Optimization
IBM Automation Framework

CHAINYARD



TYS+Fabric

Data Sources (Producers)

Supplier Streams

Event Streaming and Processing

Kafka

Flink

Elastic Search

Kube flow

Supplier Invitation UI (Prediction)

Supplier Profile

Probability of Acceptance

Model

M3

M2

M1

TF, Python, Keras, sklearn
RF Classification
Artificial Neural Network
Jupiter NB

Gather TYS Supplier Invitation Data

Pre-Process Mask & Scrub

Create Training & Test Sets

Apply Feature Scaling

Train the Model

Predict

Automation Platform

Proof of Concept implementation of a Supply Chain Solution using ML and Process Automation

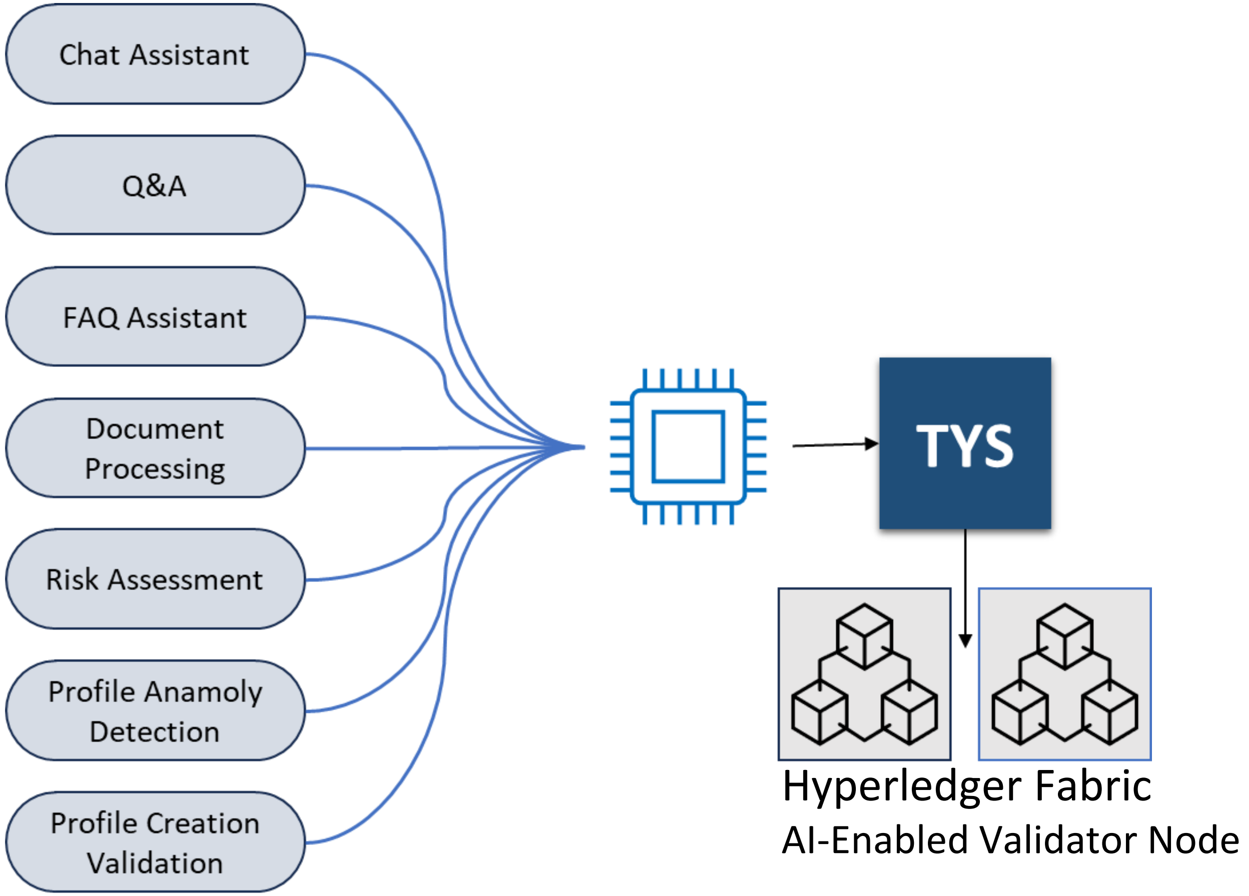
Demonstrated @IBM Think and Data & AI Developer Conference

Trust Your Supplier

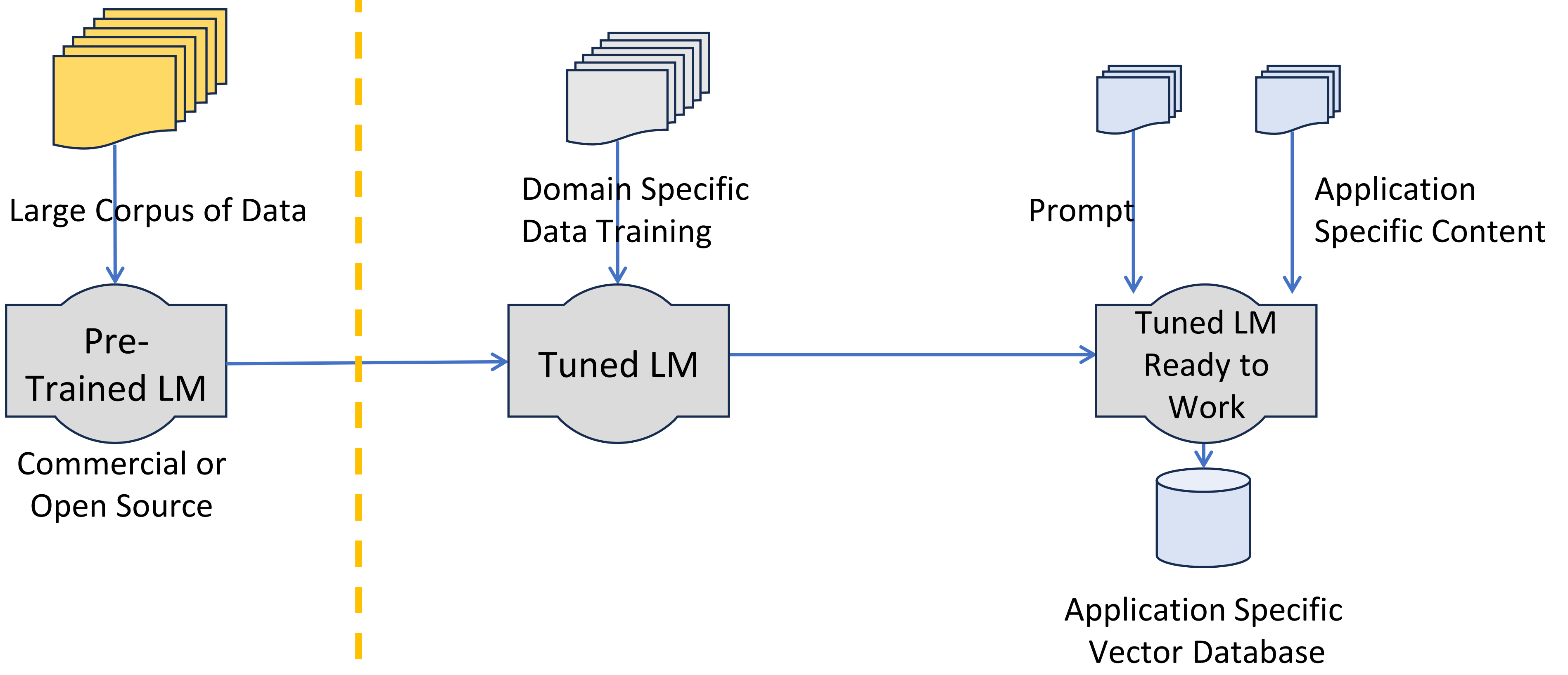
Trust Your Supplier AI Models and Use Cases

The Objectives and Goals of Trust Your Supplier are to enhance the Buyer and Supplier experience by leveraging AI and ML to support

- Automated Supplier Onboarding
- Efficient Partner Risk Management



Tuned TYS Models

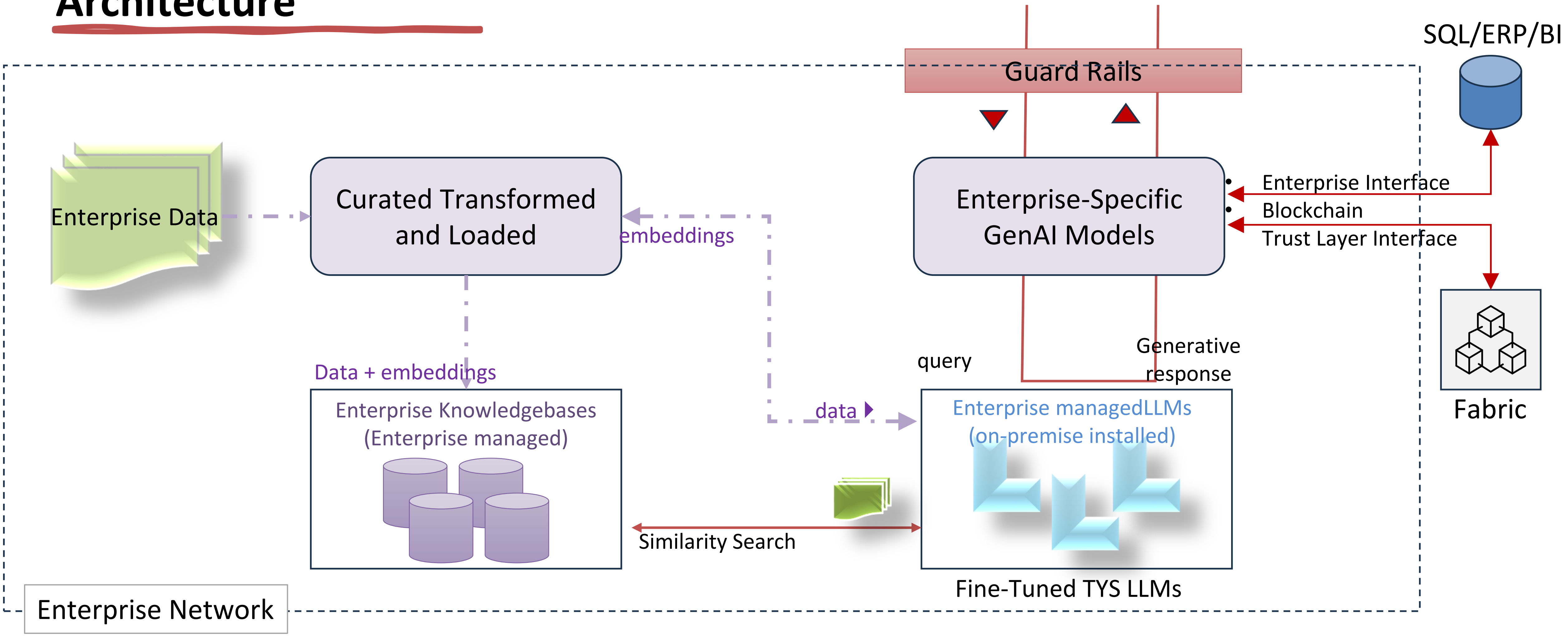

Large Corpus of Data
Pre-Trained LM
Commercial or Open Source
Domain Specific Data Training
Tuned LM
Prompt
Application Specific Content
Tuned LM Ready to Work
Application Specific Vector Database

After Graduation

After Specialization

Ready for Employment

Simplified TYS GenAI Architecture



Trusted Enterprise AI & ML

- *Key Challenges*
- *Trusted AI for the Enterprise*
- *Can Blockchain play a role?*

Critical Challenges to maintain

Design Time

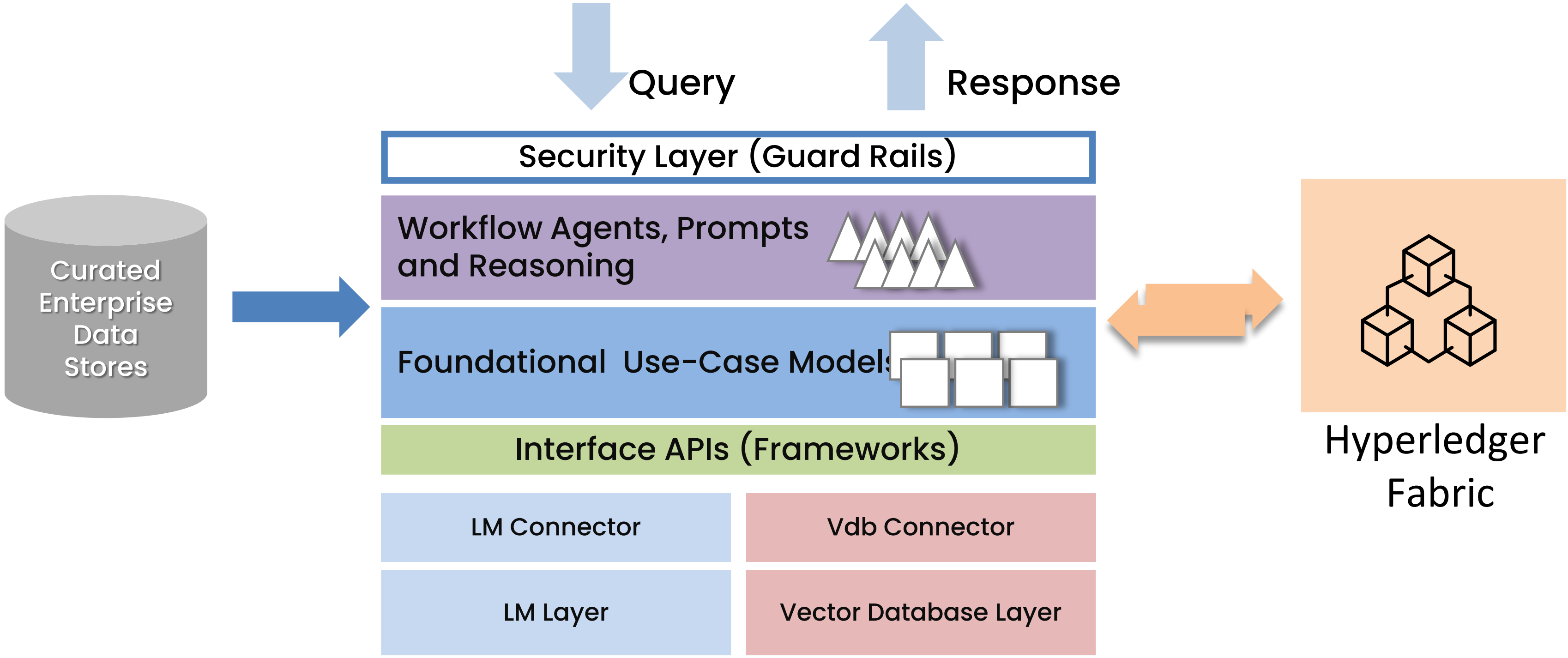
- Locating the right sources of data
- Choosing the right LMs and Agents
- Protect sensitive and private data
- Protect Intellectual Property
- Comply with regulations
- Eliminate Bias
- Track changes to model or its training

Run Time

- Protect Models from Prompt injection and in-appropriate prompts
- Reject bad and invalid actors
- Prevent Misinformation & Manipulation
- Ensure models are protected from malicious behavior
- Only approved models execute
- Traceback and prove outcomes

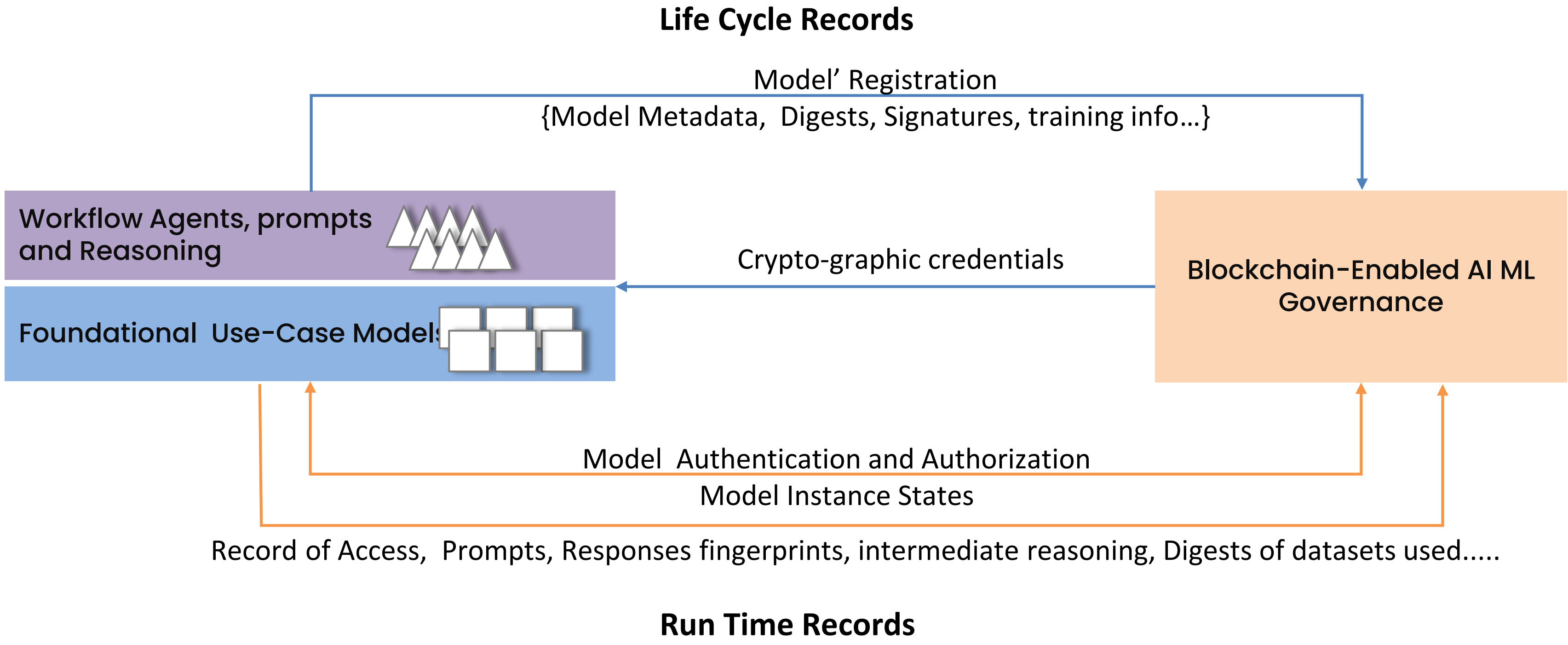
Simplified Stack

- **Input** Data Sources
- **Blockchain** enabled Trust
- **The foundation layer**
  - “Custom tuned” LMs or SLMs
  - Combination of Vector and Graph Databases
- **Interface Frameworks**
  - Langchain and LLamaIndex
- **Use Case Models**
  - Trained to Domain Specific Data
- **Workflow Components**
  - Agents
  - Prompts
- **Guard Rails**


Curated Enterprise Data Stores
Query
Response
Security Layer (Guard Rails)
Workflow Agents, Prompts and Reasoning
Foundational Use-Case Models
Interface APIs (Frameworks)
LM Connector
Vdb Connector
LM Layer
Vector Database Layer
Hyperledger Fabric

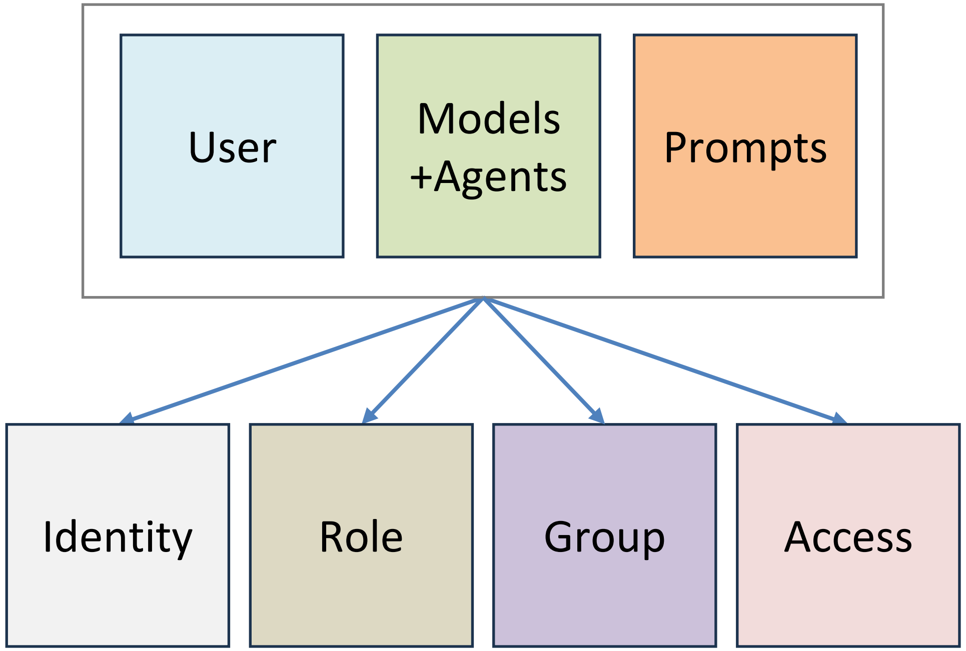
Hyperledger Fabric as a Trust Anchor

- **Governance**
  - Asset Registration
  - Asset Life-Cycle
- **Trust**
  - Asset Authentication & Authorization
  - Asset Execution Log
- **Reliability**
  - Sources of data, trainers
- **Quality**
  - Quality of trainers and training and test data
  - Outcomes are in line with business and use case expectations
- **Proofs**
  - Design time attestations
  - Run-Time Outcome attestations


Life Cycle Records
Model' Registration
{Model Metadata, Digests, Signatures, training info…}
Workflow Agents, prompts and Reasoning
Foundational Use-Case Models
Crypto-graphic credentials
Blockchain-Enabled AI ML Governance
Model Authentication and Authorization
Model Instance States
Record of Access, Prompts, Responses fingerprints, intermediate reasoning, Digests of datasets used.....
Run Time Records

Guard Rails (Run-Time)

Guard Rails help protect malicious, incorrect or sensitive usage, inputs and responses



Assets

- **Users** are Individuals or Applications that Invoke Models and Agents
- **Models** and **Agents** represent Foundational domain-related AI Apps
- **Prompts** represent user or application-provided reasoning and queries

Asset Attributes

- **Identity** - have cryptographic credentials associated with an ID
- **Role** - may have roles
- **Access -** Asset-to-Asset access. Users have access to models, agents and prompts
- **Group** – Assets may belong to logical groups bound by common interests

Guard Rail Objectives

- **Identity –** Verify identities, authenticate credentials and authorize
- **Role** – Verify user roles depending on the workflow or use-case
- **Access -** Determines User access to models and agents, and model access to data
- **Prompts** - Filter for PII, spurious and malicious material, and queries
- **Responses** - Filter for sensitive, PII, Fakes(Deep) and incorrect information

?

CHAINYARD

an IT People Company

WE TURN TECHNOLOGY INTO BUSINESS RESULTS.

Model Management

Model Registration on DLT:

- When a model is ready for deployment, it should be registered on the distributed ledger (DLT).
- Registration details may include model specifications, verification records, and information about the training data used.
- Successful validation and verification lead to the issuance of cryptographic credentials by the blockchain.

Model Lifecycle Management:

- The blockchain plays a crucial role in managing the entire lifecycle of models. This includes deployment, updates, and eventual retirement. Hyperledger Fabric is a mature enterprise blockchain platform.
- Similarly, pre-defined prompts and agents can also benefit from DLT-based lifecycle management.

Runtime Authentication and Recording:

- During runtime, models must be authenticated and authorized.
- Data recording encompasses various aspects, such as startup state, data consumption digests, and access details for applications or users.

Models and Prompts

Prompts are user or application-provided instructions or queries.

- When using prompts, it's essential to filter out any inappropriate content, including examples that exclude specific populations.

Models are AI functions that perform specific tasks based on their training.

- They leverage knowledge from a pre-existing dataset (often stored in a vector database) and apply it to generate insights or outcomes.
- Language models (LLMs) play a significant role in understanding and generating text.

User Trust and Model Assurance

- **User Trust**:
  - Users should trust the models they interact with.
  - This trust extends to the outcomes and insights provided by these models.
- **Model Assurance**:
  - Ensuring that models are reliable, accurate, and well-behaved is critical.
  - Audit trails and transparency play a key role here.

Image generated using DALL-E – Mohan