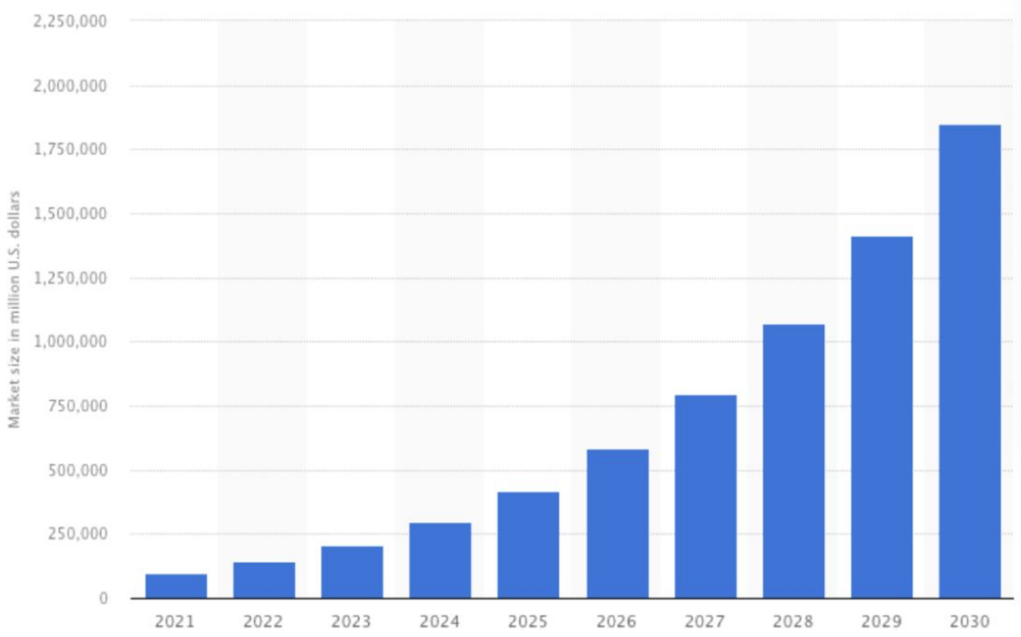
How Verifiable ML will shape the future of AI

PARIS 2023

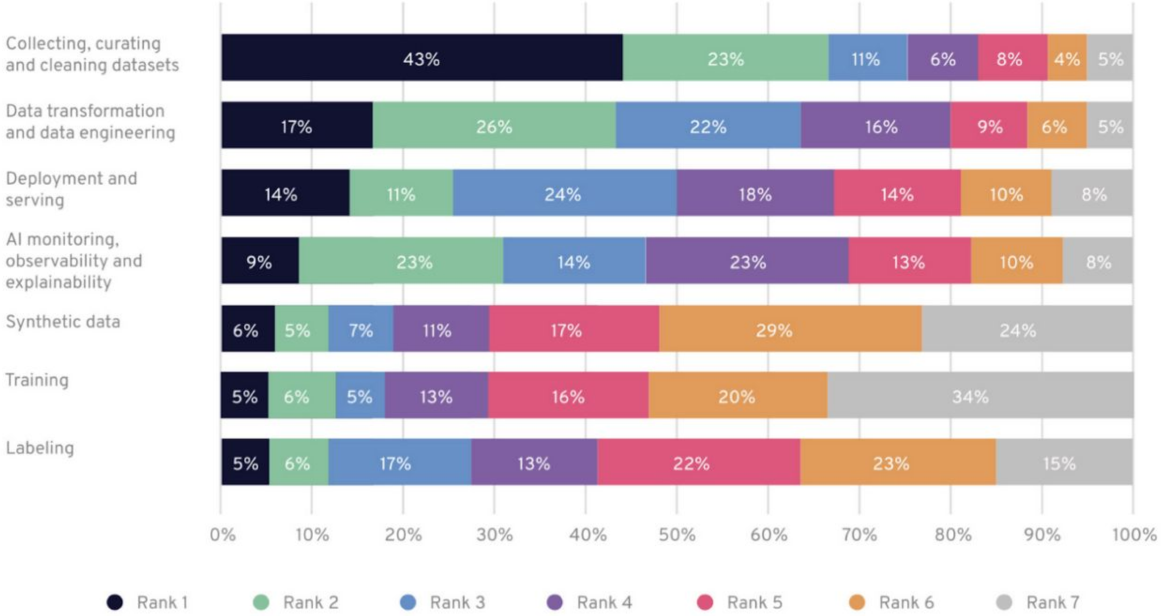
FRAN ALGABA | GIZA CO-FOUNDER

GIZA

AI annual growth rate (CAGR) of 37.3% from 2023 to 2030



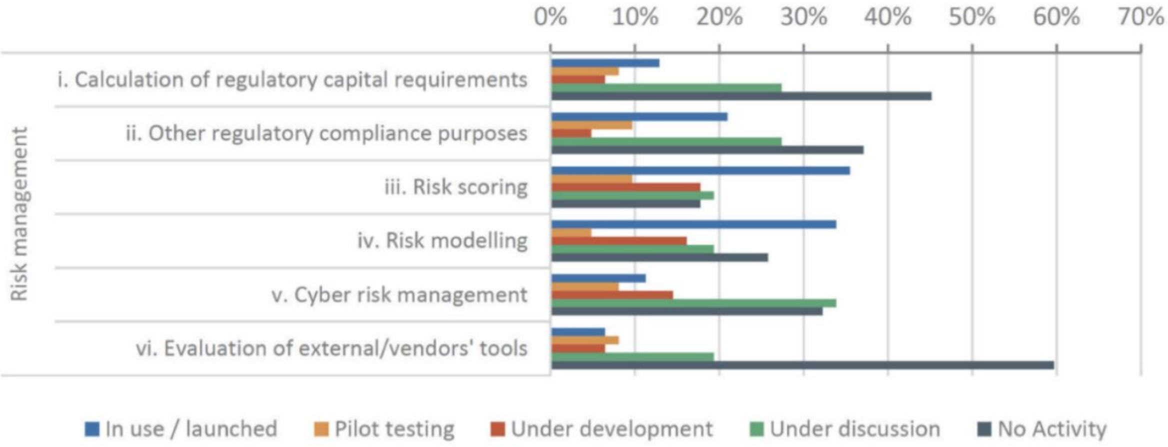
What parts of the AI/ML infrastructure should receive the most resources (i.e., talent, time, money)? Rank in order from most to least. (Ranked first)



How is AI being used?

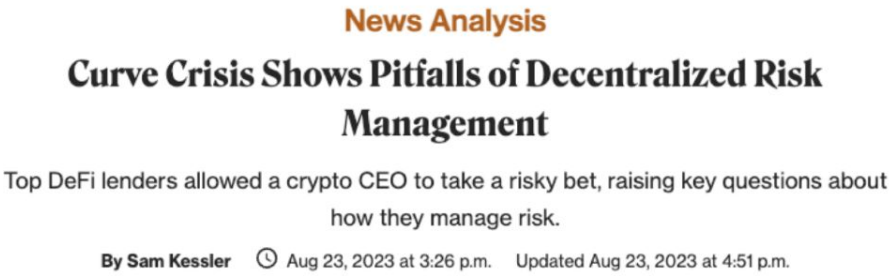
ML is widely used across banking

Figure 2: Risk management with AI and big data of European banks



Source: EBA risk assessment questionnaire (spring 2019).

What about DeFi?

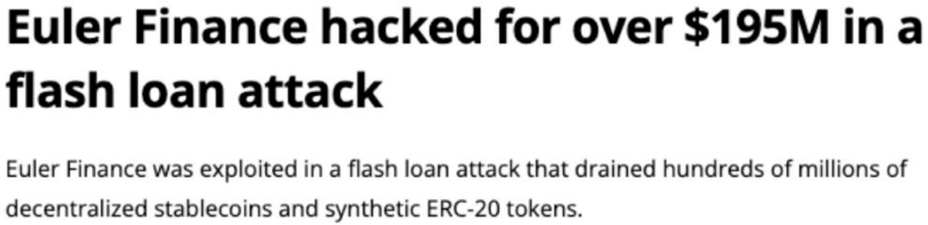


News Analysis

Curve Crisis Shows Pitfalls of Decentralized Risk Management

Top DeFi lenders allowed a crypto CEO to take a risky bet, raising key questions about how they manage risk.

By Sam Kessler Aug 23, 2023 at 3:26 p.m. Updated Aug 23, 2023 at 4:51 p.m.



Euler Finance hacked for over $195M in a flash loan attack

Euler Finance was exploited in a flash loan attack that drained hundreds of millions of decentralized stablecoins and synthetic ERC-20 tokens.

What it means for the blockchain?

- Leverage ML capabilities without trust assumptions
- Improved risk management for DeFi

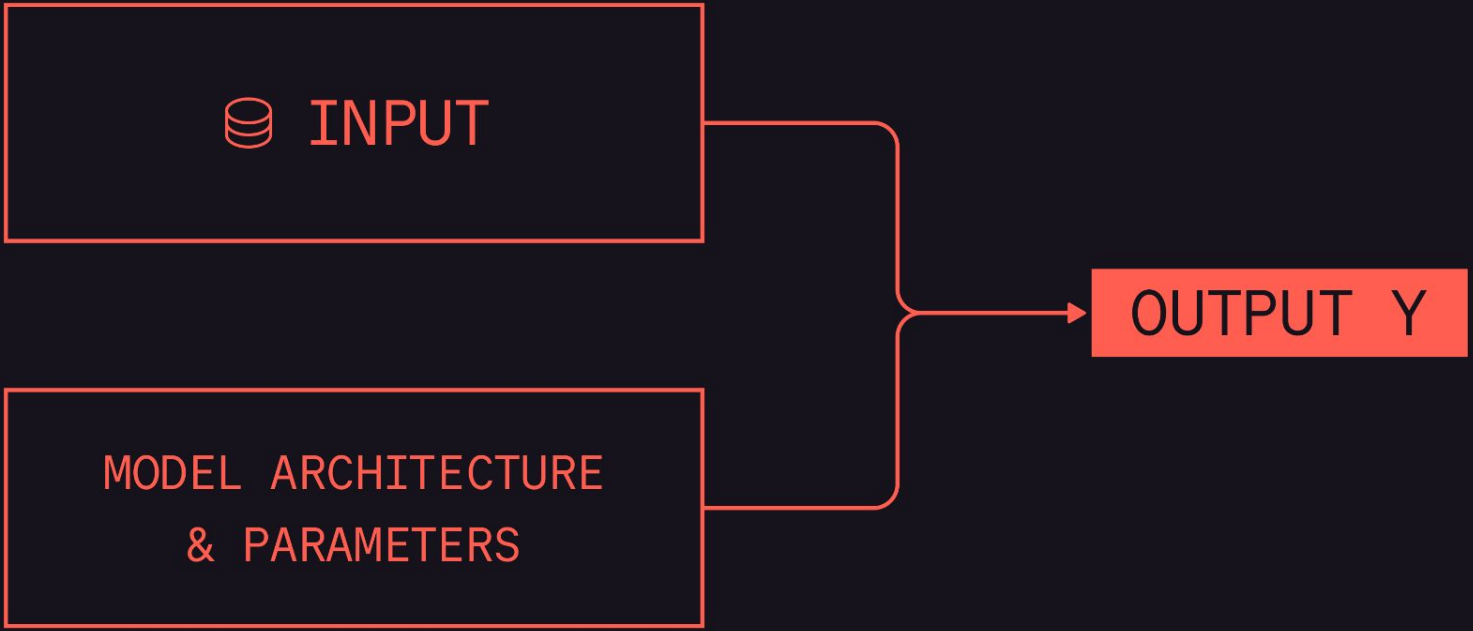
What is Verifiable ML?

TRAINING

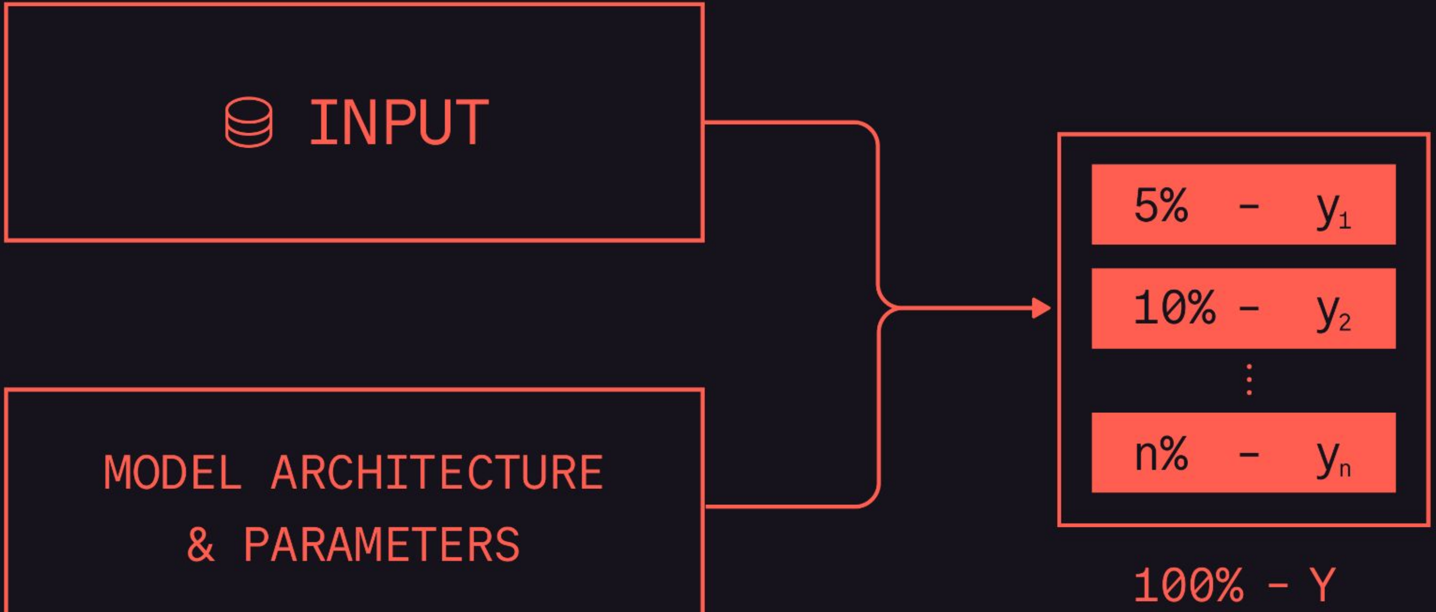
“Process of teaching a machine learning algorithm to make predictions or decisions by feeding it data”

INFERENCE

“Process of using a trained machine learning model to make predictions or decisions based on new, unseen data”



DETERMINISTIC

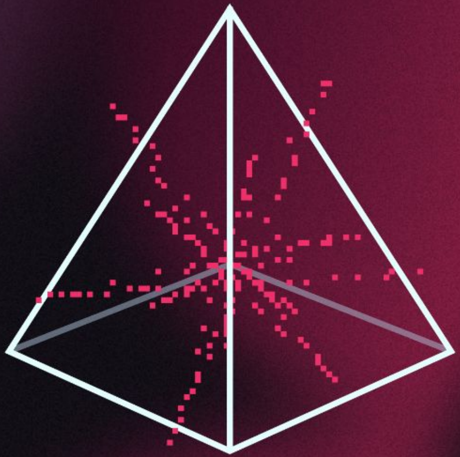


NON-DETERMINISTIC

CAIRO

ORION

ORION



open-source, community-driven ecosystem for Validity and ZK ML

ORION ECOSYSTEM

FRAMEWORK

A community-driven framework providing an ONNX runtime implementation for Validity and ZK ML.

HUB

A curated collection of ML models and spaces built by the community using Orion framework.

ACADEMY

Resources, tutorials and meet-ups for learning how to build ValidityML models using Cairo and Orion framework.

TOOLBOX

A collection of 3rd party tools built by the community to use with Orion, such as GIZA CLI, and more.

Features

Standardized API

Multi-backend support

+30 ML supported frameworks

Features

Standardized API

Multi-backend support

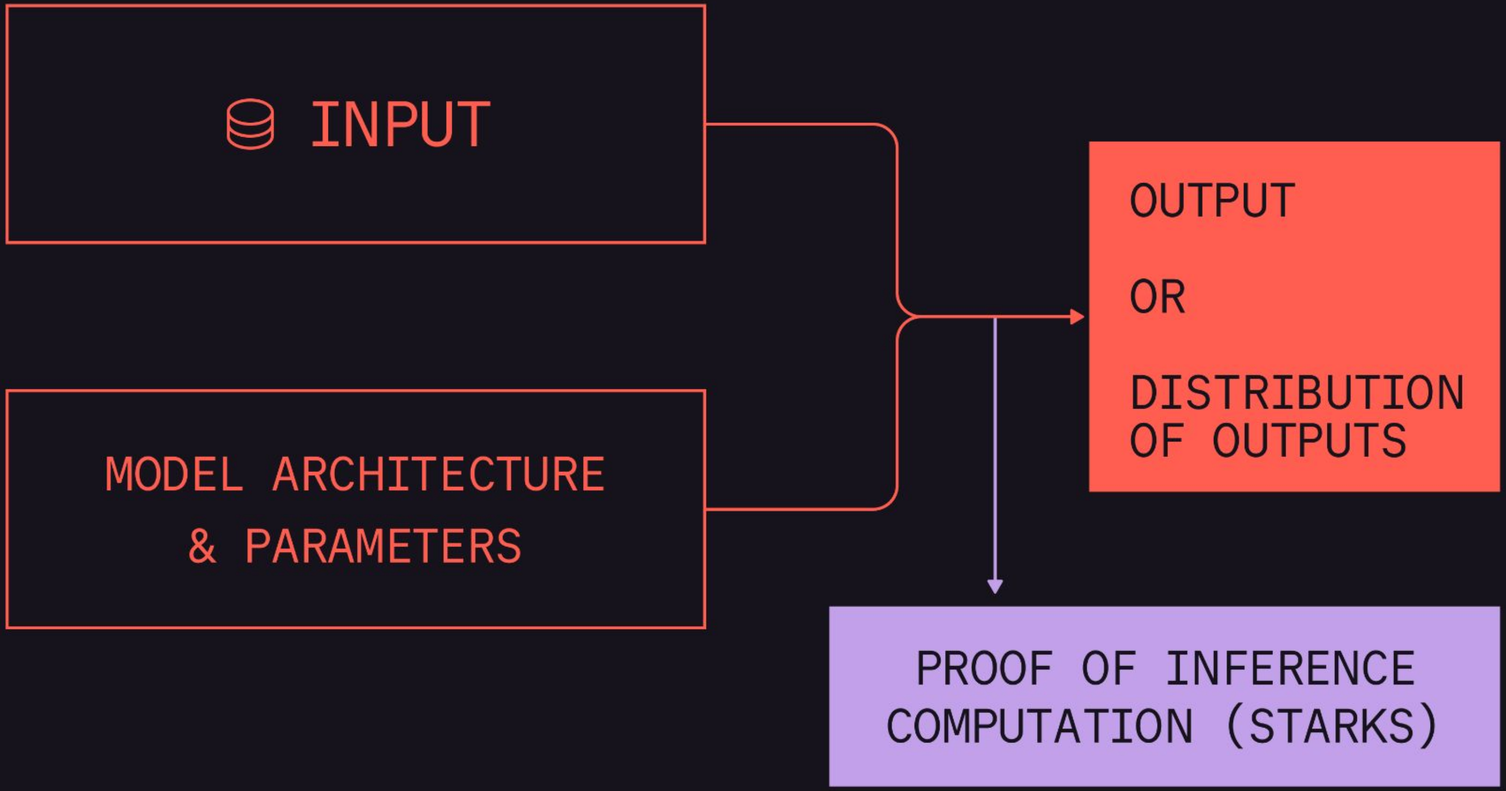
+30 ML supported frameworks

Features

Standardized API

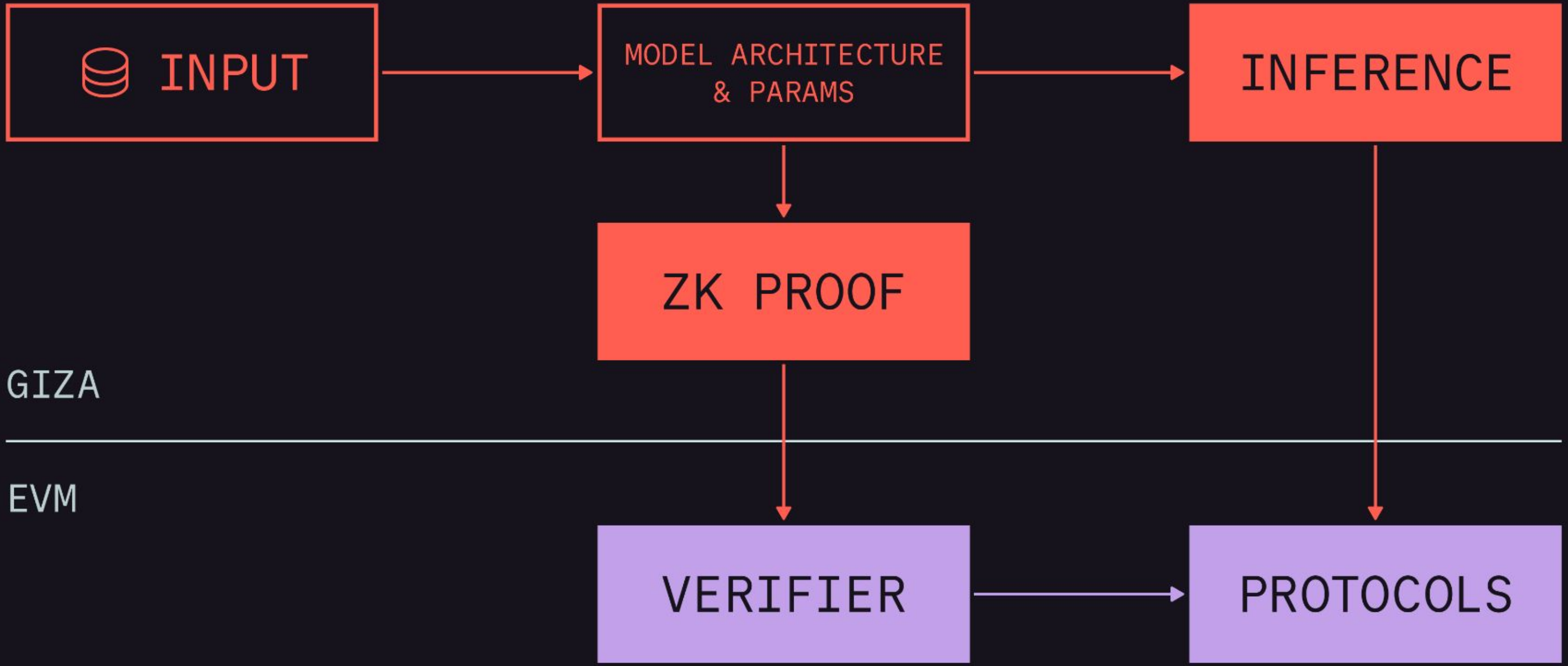
Multi-backend support

+30 ML supported frameworks


INPUT
MODEL ARCHITECTURE & PARAMETERS
OUTPUT
OR
DISTRIBUTION OF OUTPUTS
PROOF OF INFERENCE COMPUTATION (STARKS)

VERIFIABLE ML

How does onchain ML work?



Use Cases

01

Yearn Finance

- Improved risk management for users in vault creation
- Underlying assets analysis for risk scoring
- Permissionless risk assessment

Use Cases

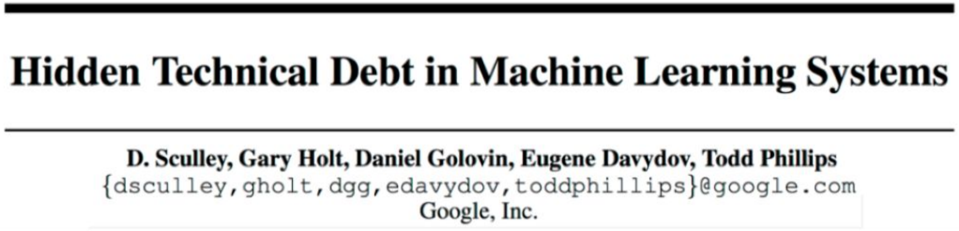
General

- Undercollateralized loans
- Onchain credit scoring
- Optimized yield aggregation
- Pool rebalancing

02

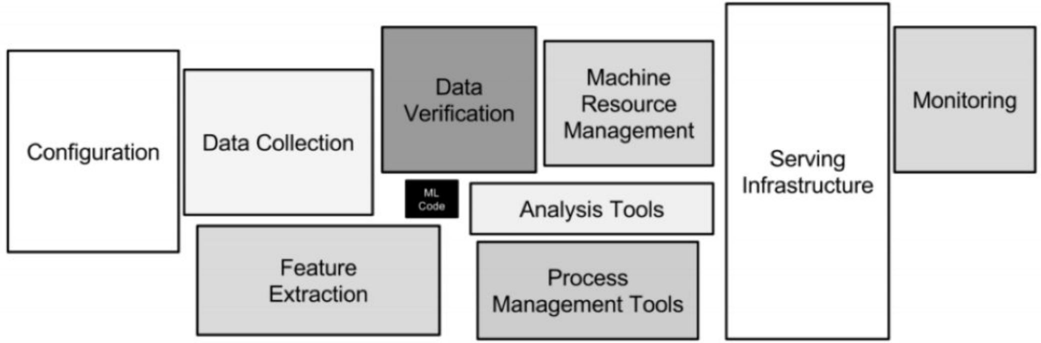
There is much more...

Complexity of the AI stack



Hidden Technical Debt in Machine Learning Systems

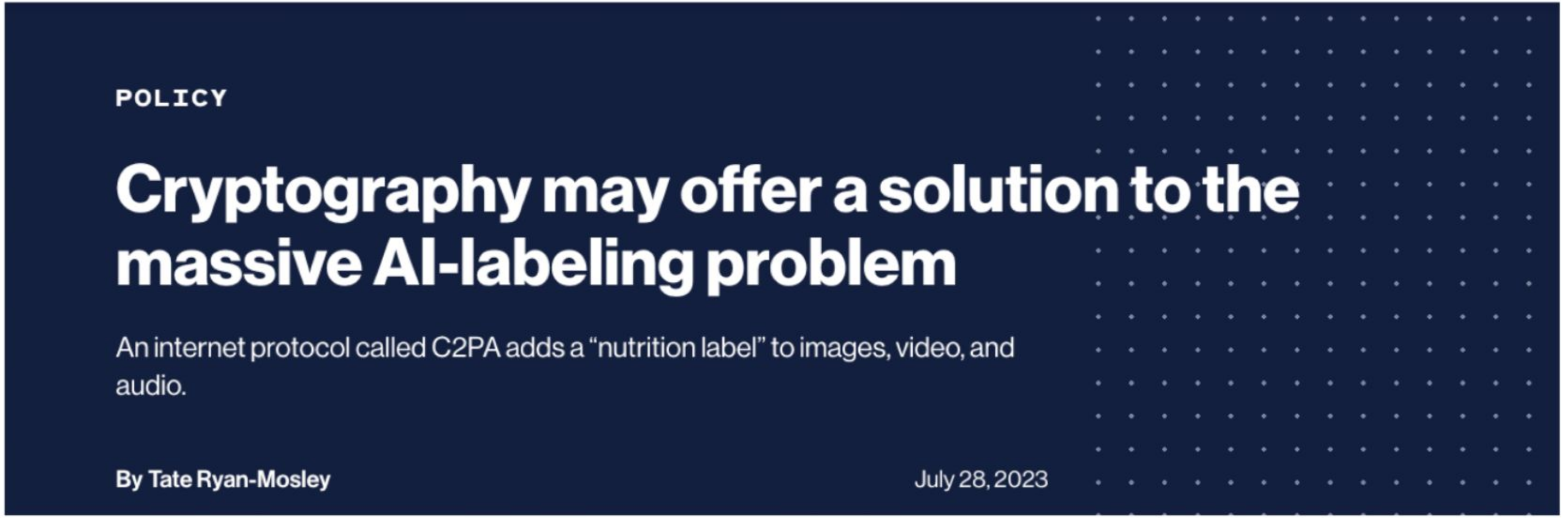
D. Sculley, Gary Holt, Daniel Golovin, Eugene Davydov, Todd Phillips
{dsculley,gholt,dgg,edavydov,toddphillips}@google.com
Google, Inc.



WHY VERIFIABLE ML IS IMPORTANT?

We need an easy way to have provenance in AI

Verifiability is a requirement



POLICY

Cryptography may offer a solution to the massive AI-labeling problem

An internet protocol called C2PA adds a “nutrition label” to images, video, and audio.

By Tate Ryan-Mosley

July 28, 2023

Verifiability is a requirement

“European policy-makers should grant data subjects a new right to challenge unreasonable high-risk inferences, which can also support challenges to subsequent decisions”

“For verifiable inferences, the data subject can provide supplementary information to rectify the inaccurate inference”

Policy Recommendations -- 'A Right to Reasonable Inferences: Re-thinking Data Protection Law in the Age of Big Data and AI'

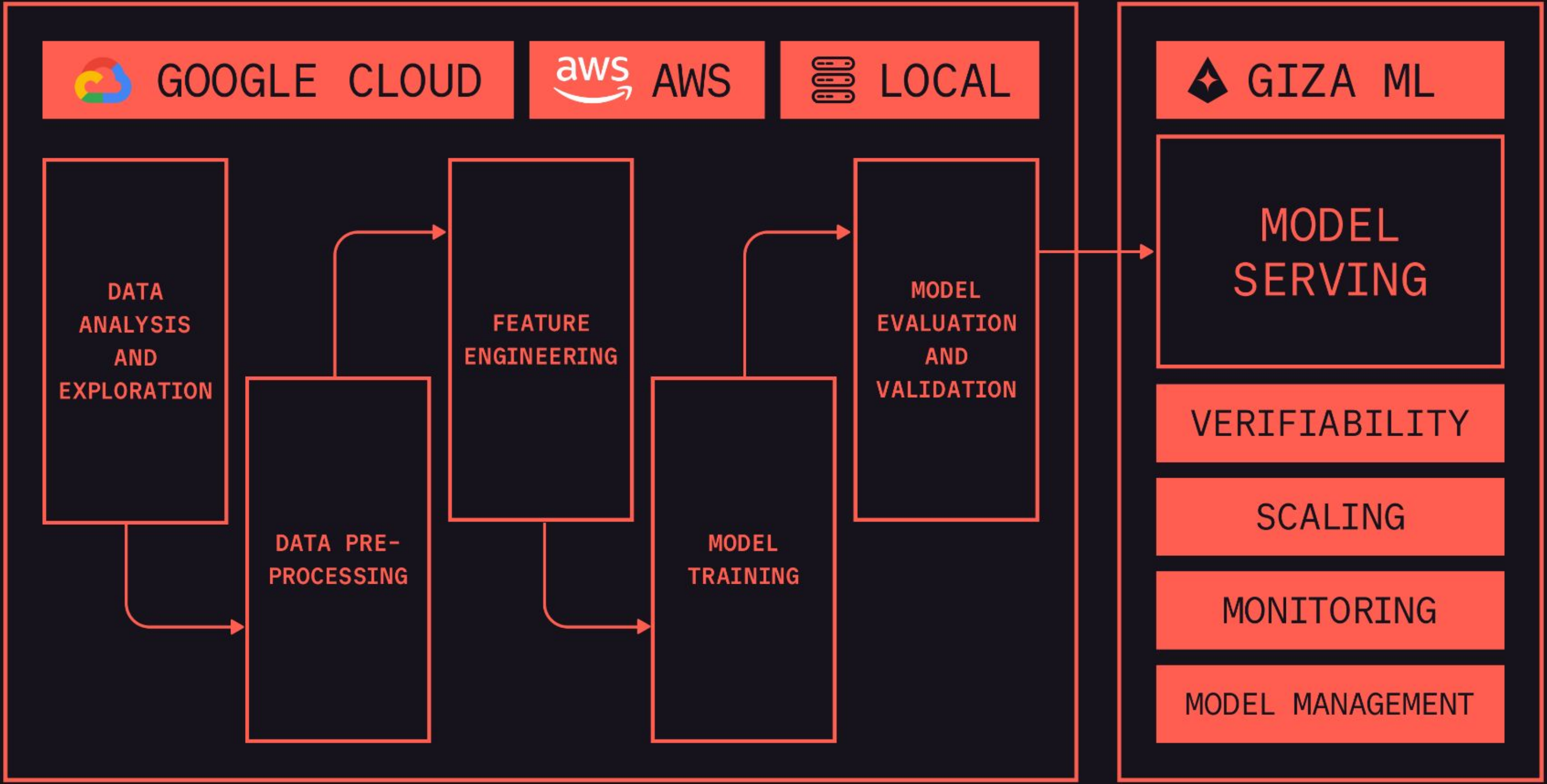
There is much more

- Simplified auditing processes
- Simplified AI monitoring stack
- Highly beneficial for regulated industries

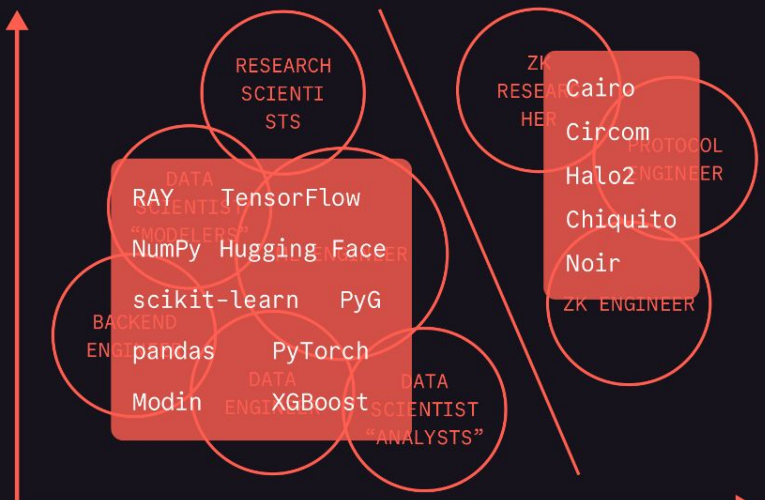
Our approach at Giza

- End to end MLaaS for Verifiable ML
- Abstracted ZK from the user

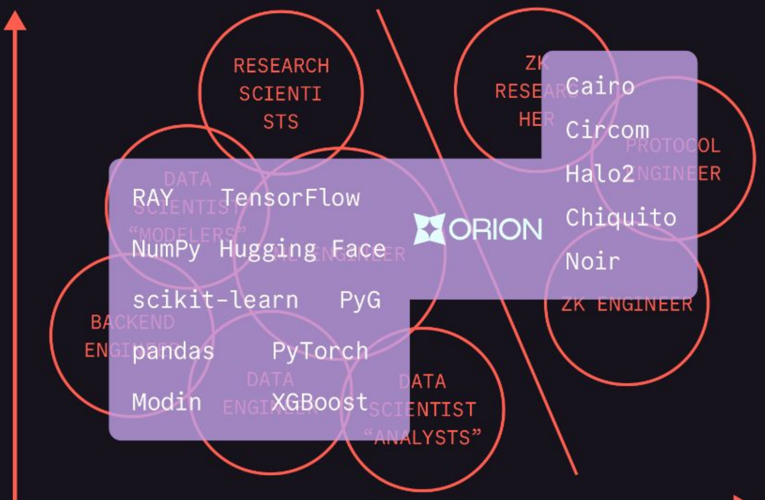
GIZA


GOOGLE CLOUD
AWS
LOCAL
DATA ANALYSIS AND EXPLORATION
DATA PRE-PROCESSING
FEATURE ENGINEERING
MODEL TRAINING
MODEL EVALUATION AND VALIDATION
GIZA ML
MODEL SERVING
VERIFIABILITY
SCALING
MONITORING
MODEL MANAGEMENT

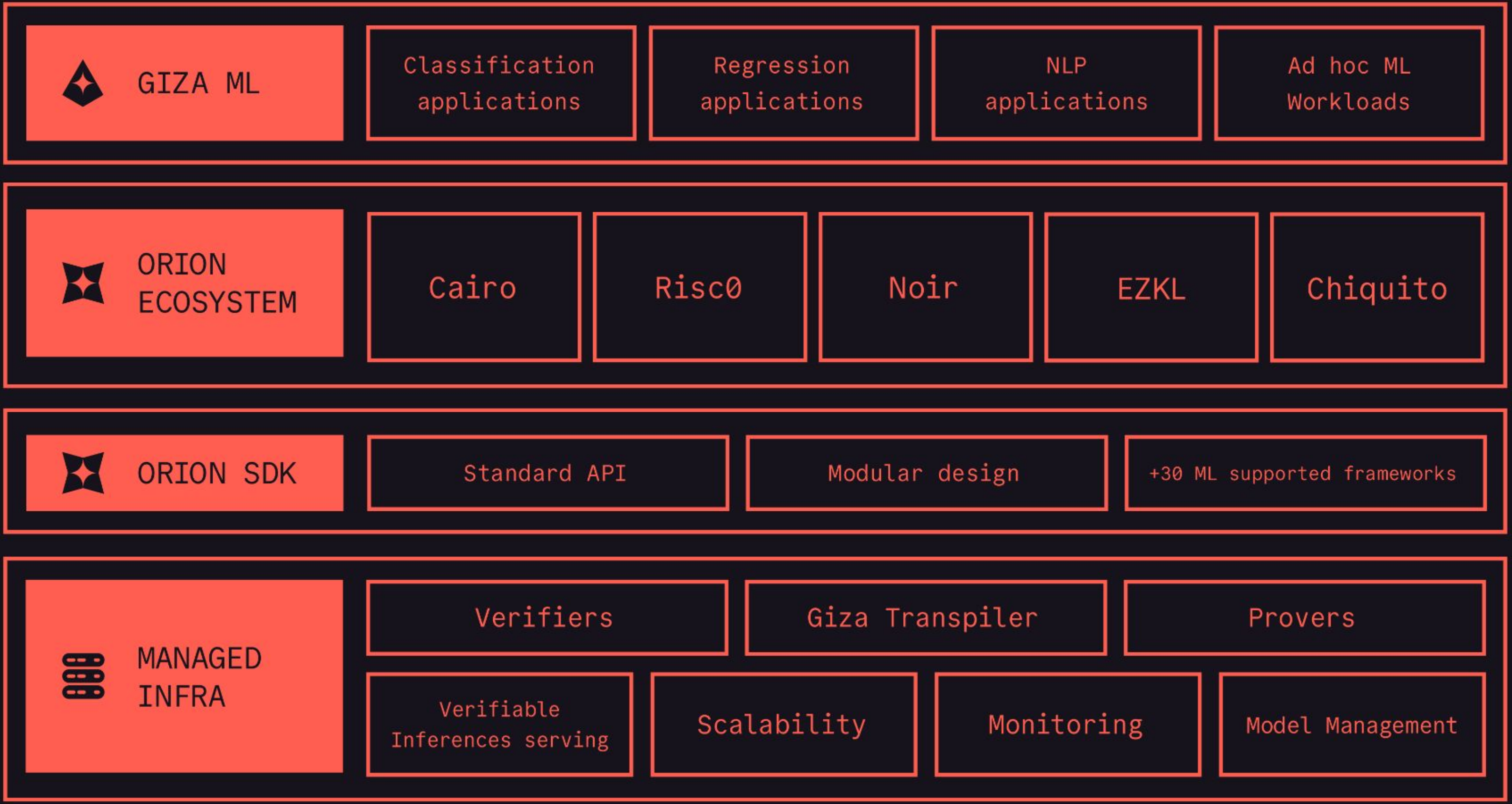
ML Platform Focus



CURRENT



FUTURE



GIZA ML

Classification applications

Regression applications

NLP applications

Ad hoc ML Workloads

ORION ECOSYSTEM

Cairo

Risc0

Noir

EZKL

Chiquito

ORION SDK

Standard API

Modular design

+30 ML supported frameworks

MANAGED INFRA

Verifiers

Giza Transpiler

Provers

Verifiable Inferences serving

Scalability

Monitoring

Model Management

Any questions?