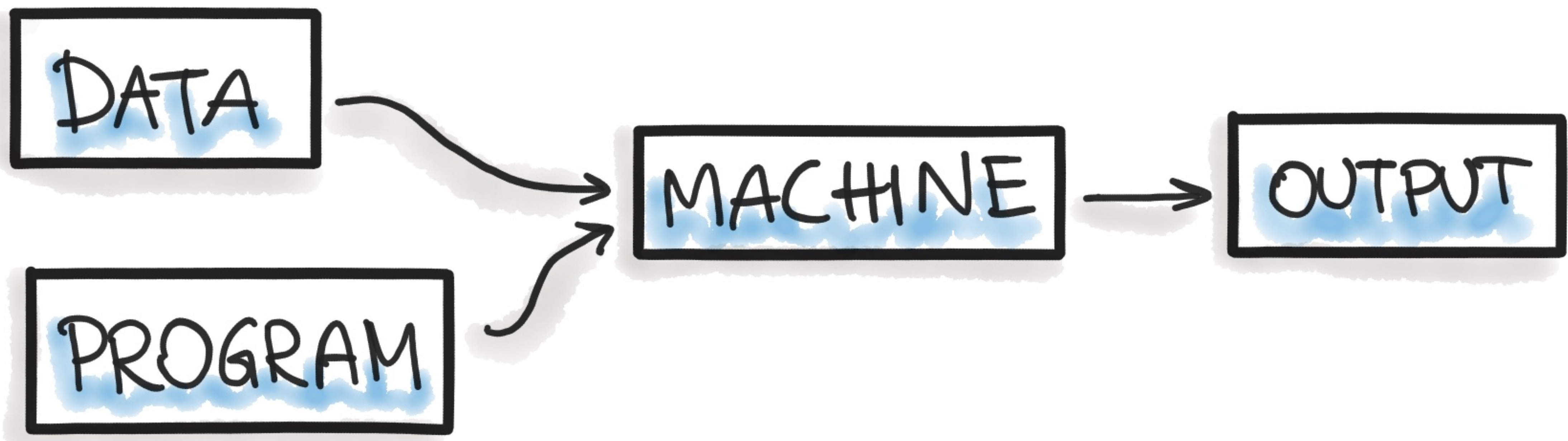


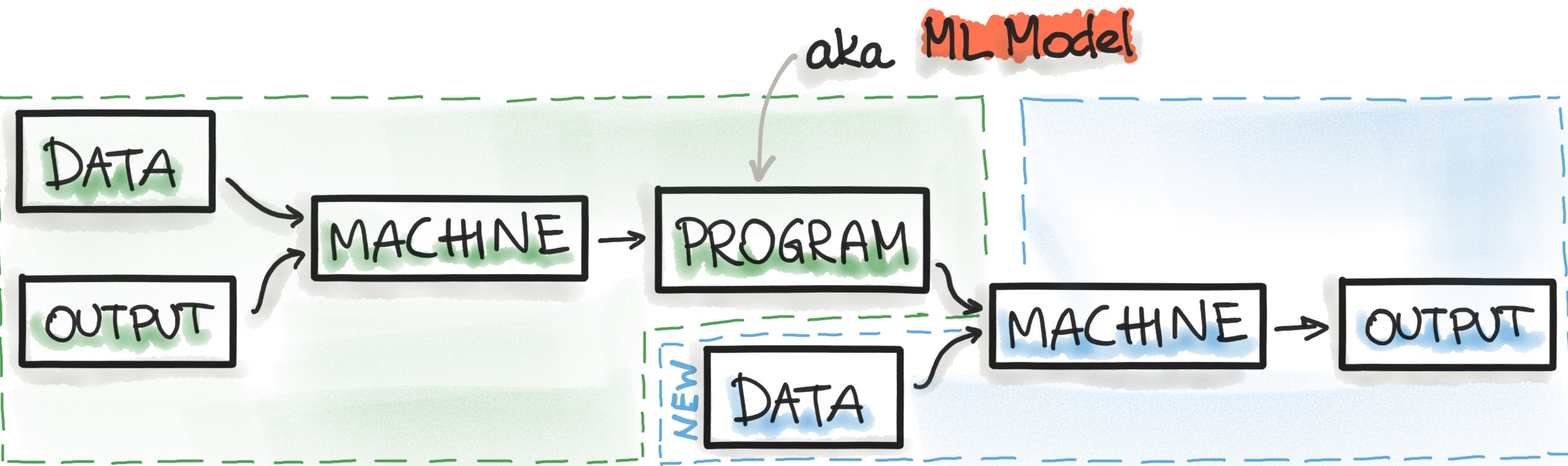
10 FOUNDATIONAL
PRACTICES
OF
MACHINE LEARNING
ENGINEERING

PROGRAMMING vs. MACHINE LEARNING

PROGRAMMING



MACHINE LEARNING

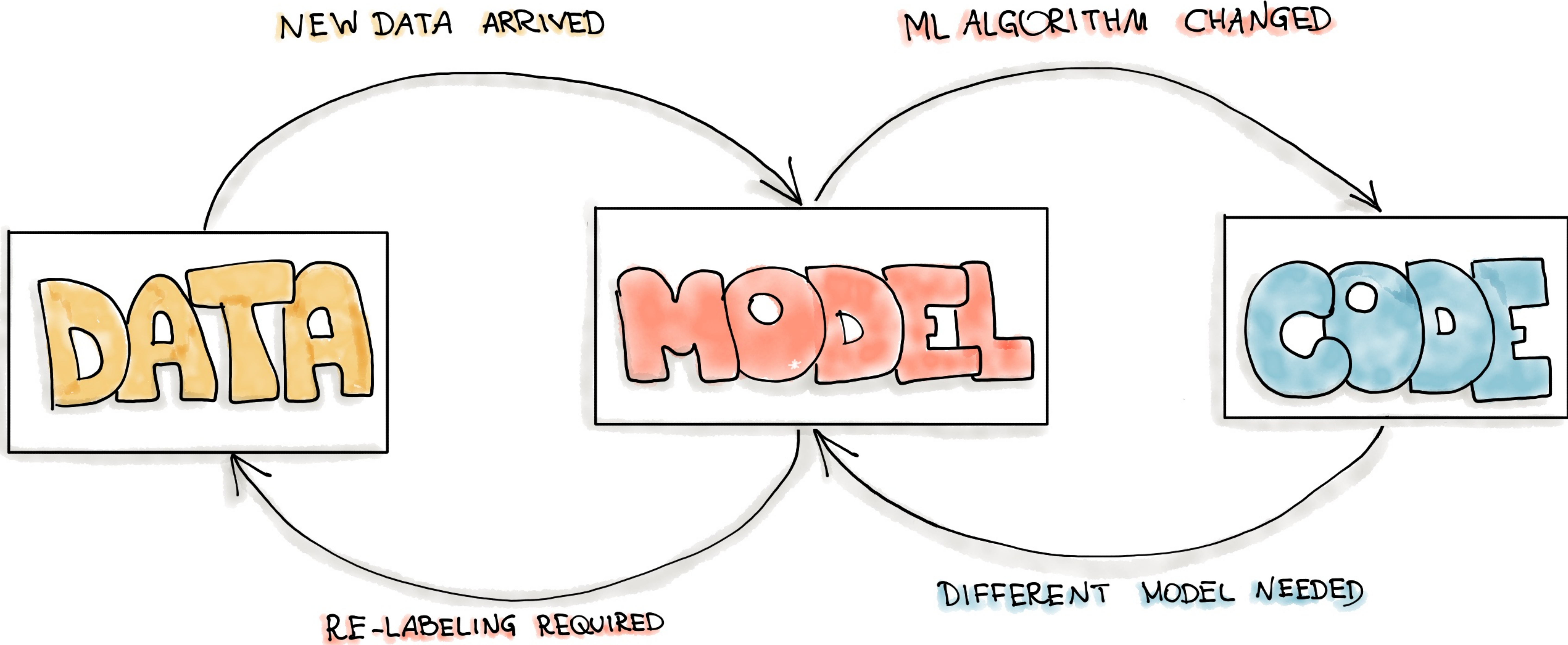


① TRAINING

② PREDICTION

— HISTORICAL DATA ————|—— UNSEEN DATA ~~~~~

3 LEVELS OF CHANGE



ML ENGINEERING HIERARCHY OF NEEDS



RESPONSIBLE AI

KNOW ML HIDDEN COSTS

DESIGN FOR ML

VERSIONING FOR ML

ML OPERATIONS

ML ALGORITHMS SIMPLICITY

NO AI WITHOUT IA

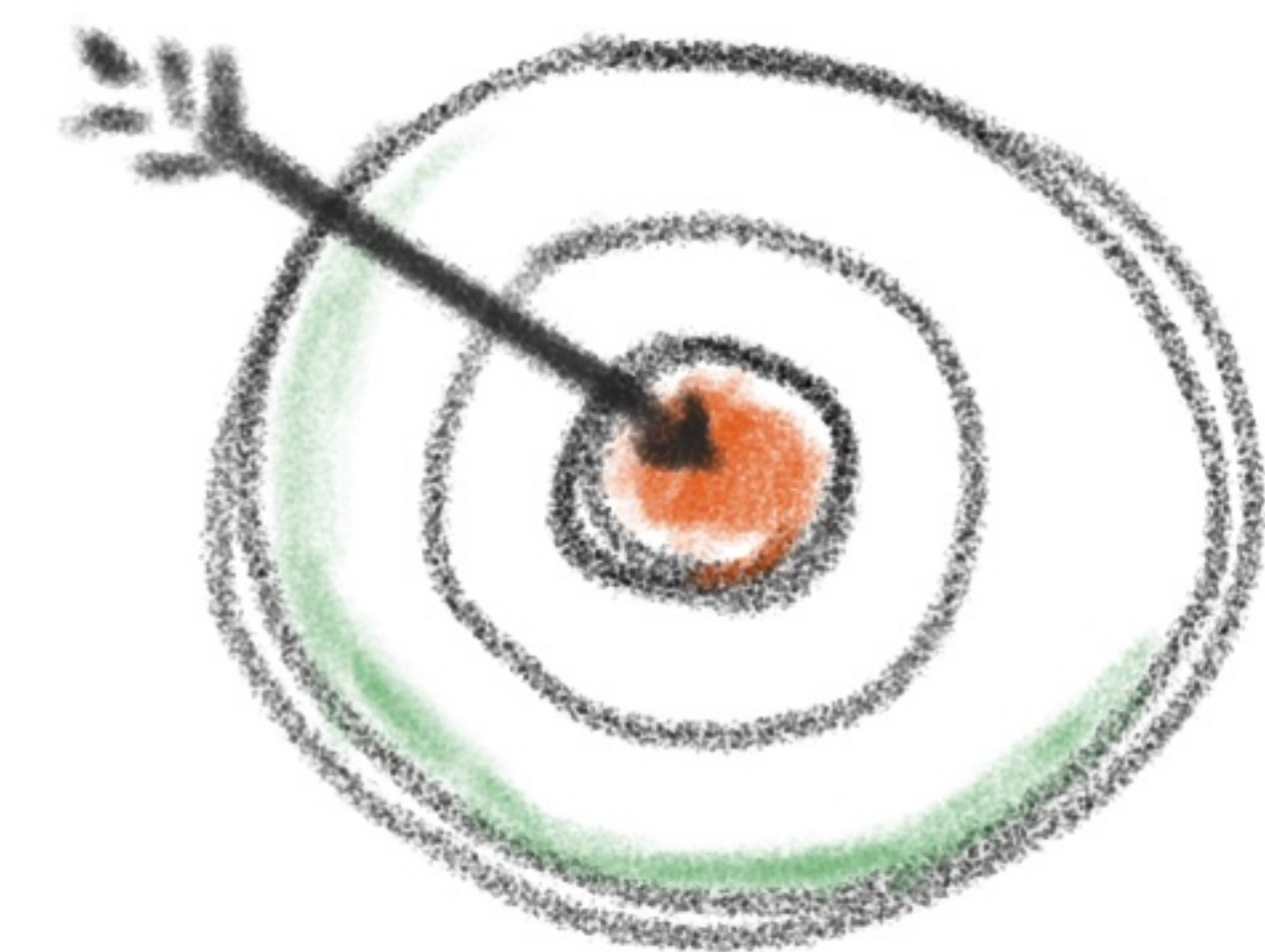
ML PROJECT MANAGEMENT

GET THE RIGHT TEAM / SKILLS

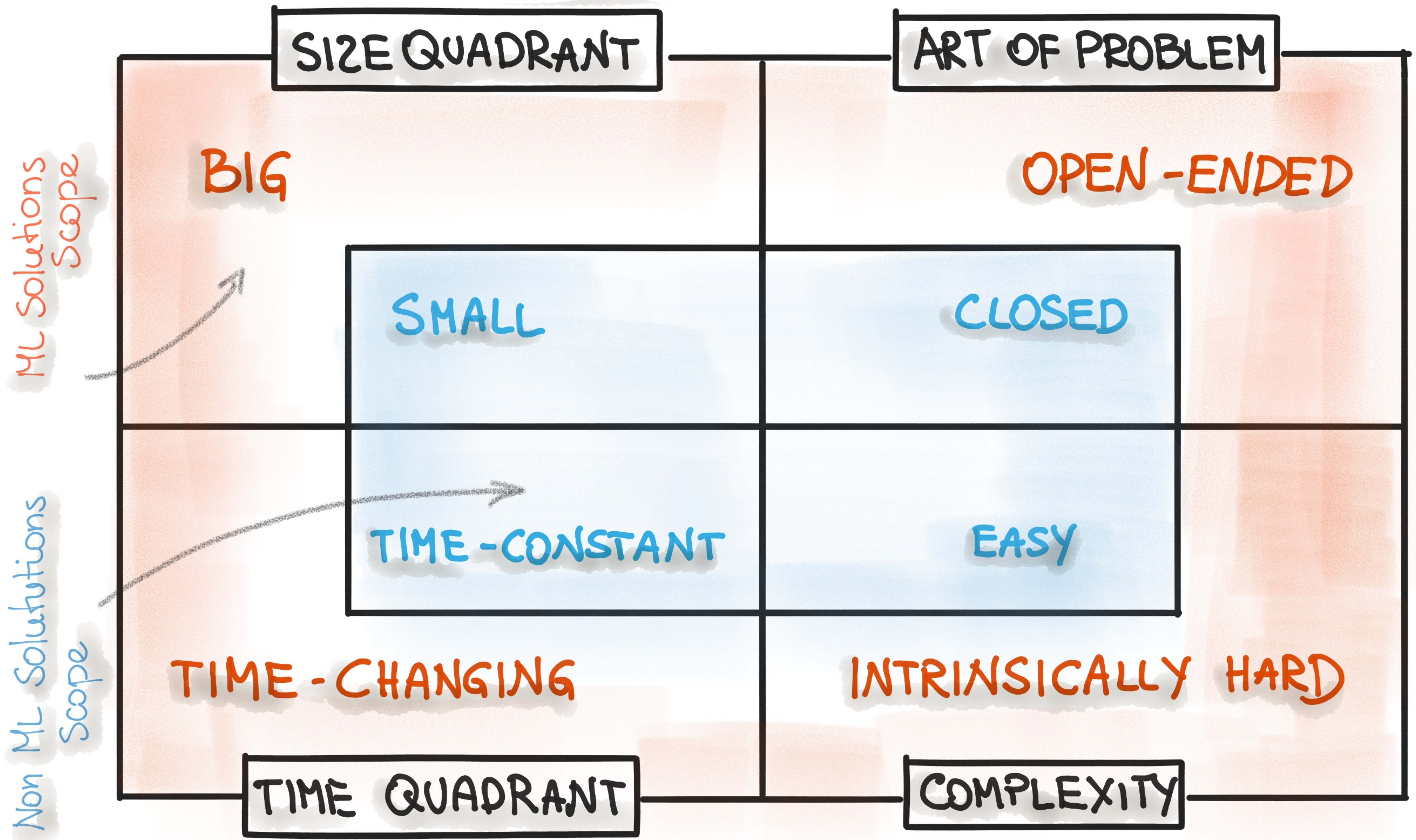
SOLVE ML PROBLEM

① AVOID ML-SOLUTIONISM

WHAT IS THE RIGHT
PROBLEM FOR AN
ML-SOLUTION ?



① AVOID ML-SOLUTIONISM

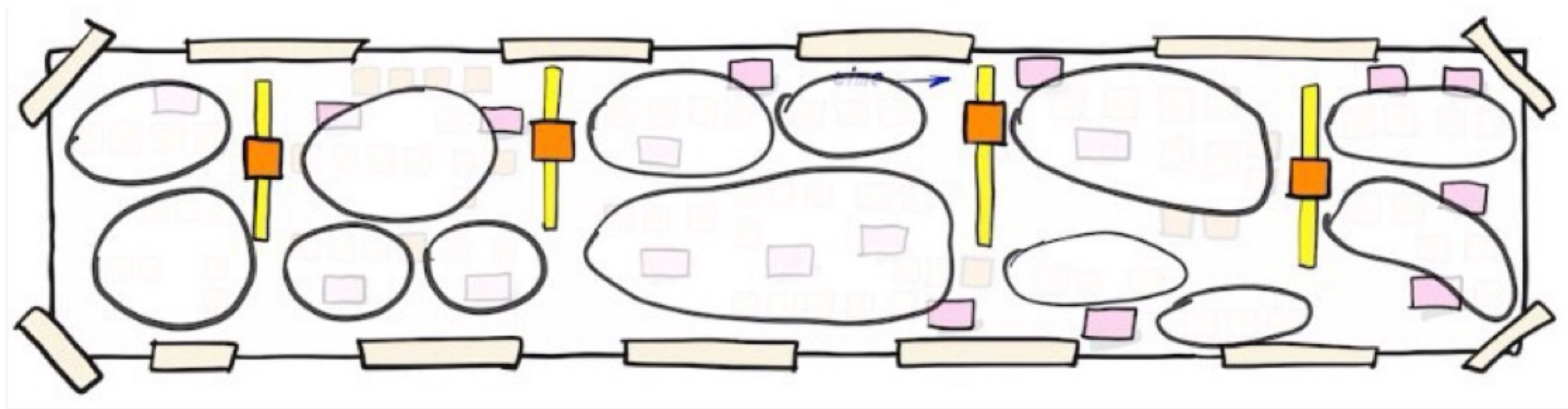


① AVOID ML-SOLUTIONISM

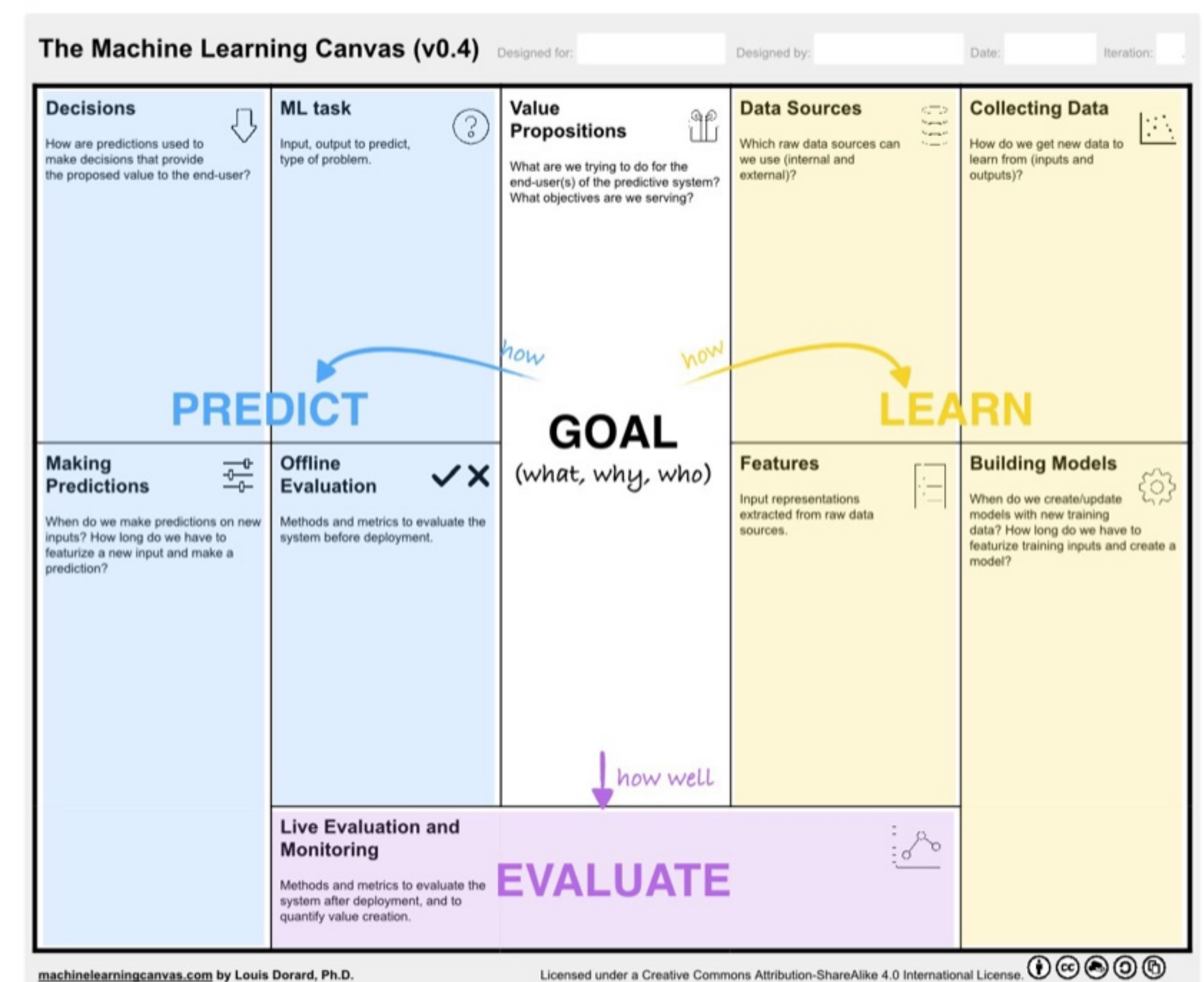
FIND THE OPPORTUNITY



STRUCTURE PROJECT



(picture by A. Brandolini)



DDD KNOWLEDGE CRUNCHING

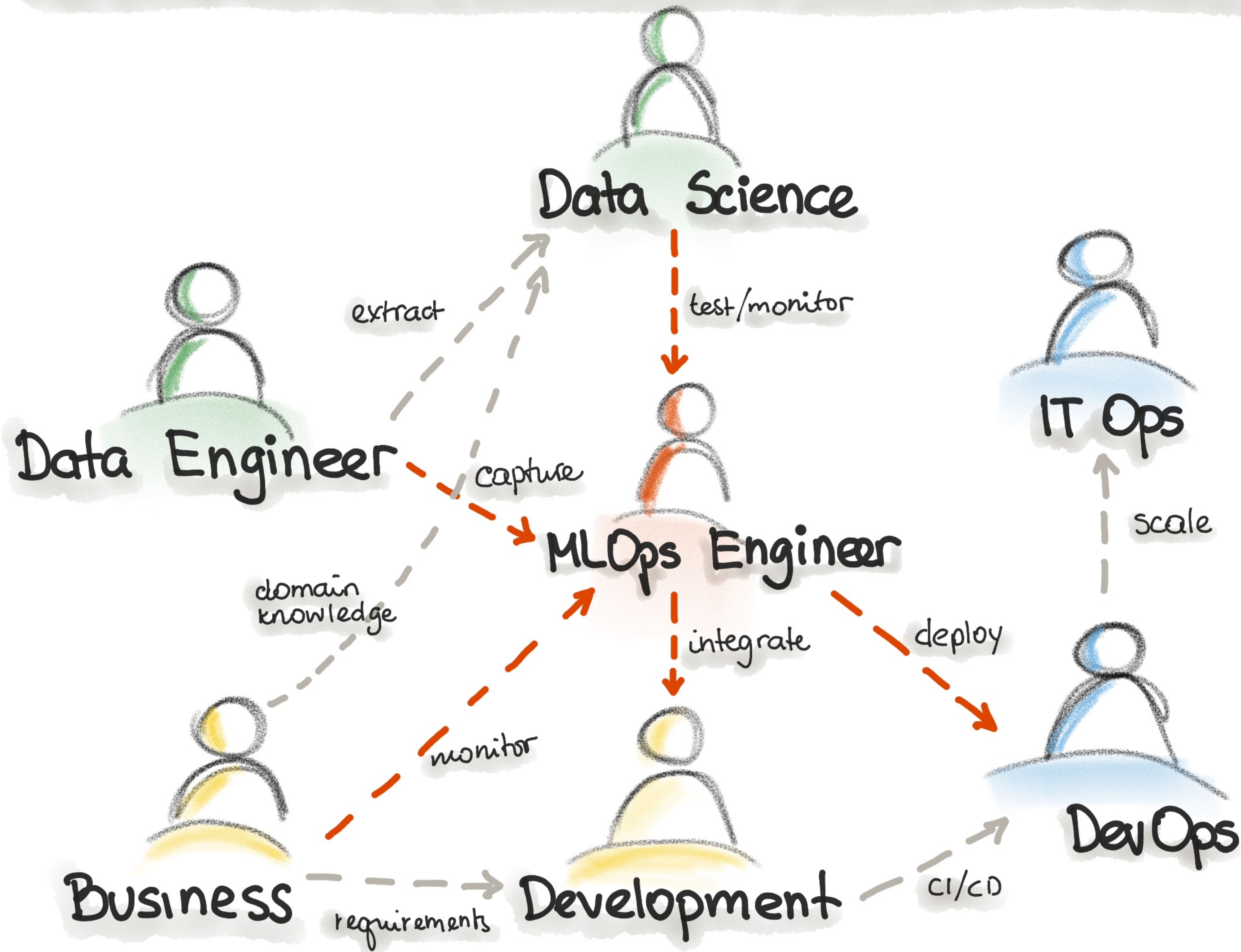
METHODS



EVENT STORMING

MACHINE LEARNING DESIGN CANVAS

② GET THE RIGHT ML-TEAM



from "MLOps: Operationalizing Data Science" by D. Sweeney et al.

③ ML-PROJECT ≠ SE-PROJECT

AIM

FINDING INSIGHTS
IN THE DATA

IMPLEMENTING A SOLUTION
FOR A SPECIFIC REQUIREMENT

FUNCTIONALITY

A MODEL IS NEVER
100% ACCURATE
AND ALWAYS CHANGES
**POST-DEPLOYMENT
PLANNING**

SOFTWARE EITHER WORKS
OR IT DOESN'T

TRACKING
PROGRESS

TRACKING DELIVERY:
- ML MODEL
- NEW LIBRARY
- NEW ALGORITHM

MEASURING PRODUCT
DELIVERY

③ ML-PROJECT ≠ SE-PROJECT

Problems

AD-HOC

NOT REPEATABLE

NOT SUSTAINABLE

NOT ORGANIZED

NOT DOCUMENTED

③ ML-PROJECT MANAGEMENT

CRISP-ML(Q)

2020

CROSS-INDUSTRY STANDARD
PROCESS FOR ML APPLICATIONS
WITH QUALITY ASSURANCE



ML Project Phases

1. Business & Data Understanding
2. Data Preparation
3. Modeling
4. Evaluation
5. Deployment
6. Monitoring & Maintenance

TDSP

TEAM DATA SCIENCE PROCESS

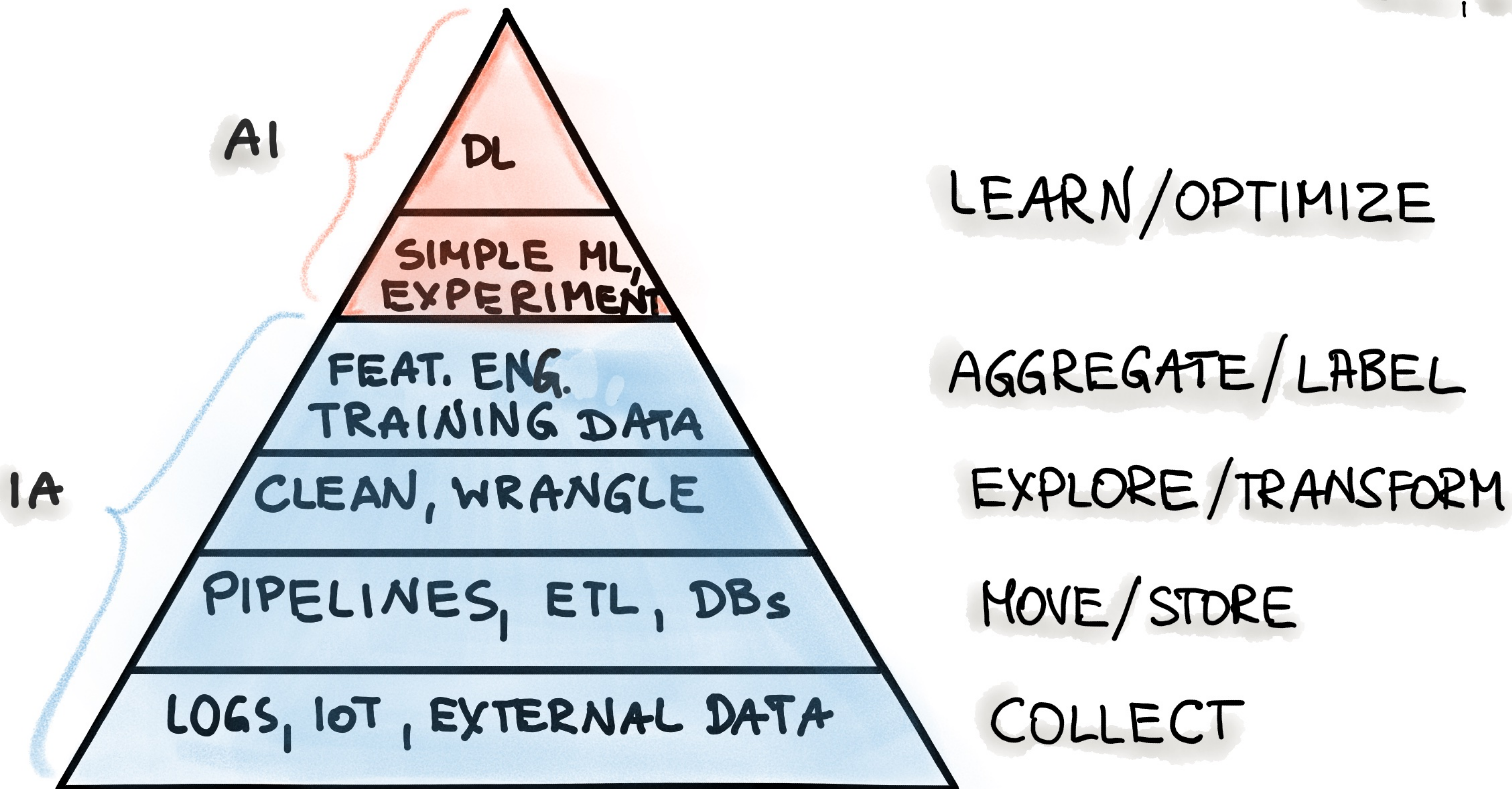
4 COMPONENTS

1. A Data Science Lifecycle
2. A Standardized Project Structure 
3. Infrastructure & Resources
4. Tools & Utilities 

④ "THERE IS NO AI WITHOUT IA"

INFORMATION ARCHITECTURE

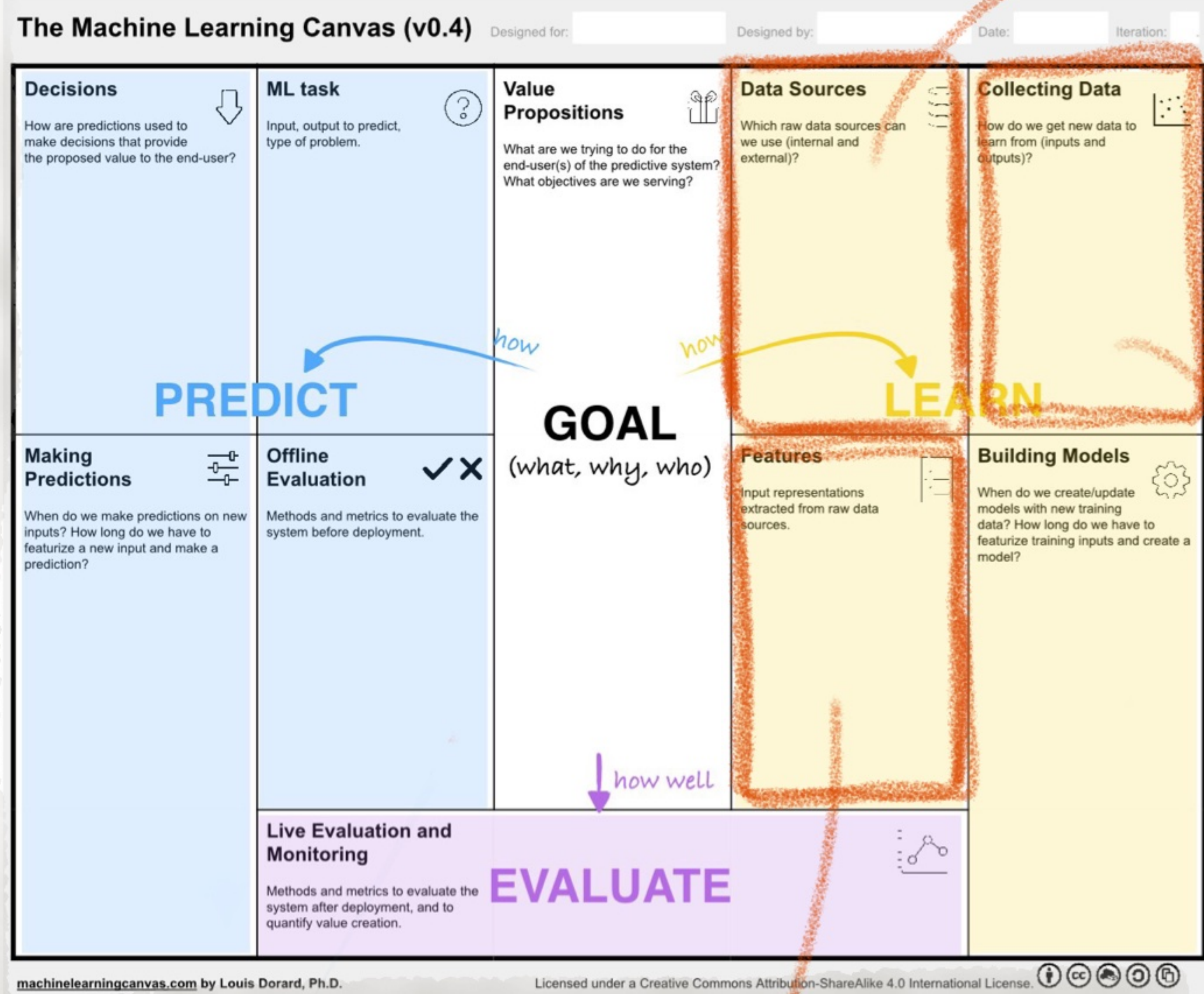
Seth Earley,
2017, IEEE Software



Monica Rogati, 2017

@visenger

④ "THERE IS NO AI WITHOUT IA"



WHICH **RAW DATA SOURCES** CAN WE USE TO TRAIN OUR ML MODEL?

HOW DO WE GET **NEW DATA** TO RE-TRAIN OUR MODEL?

WHAT **FEATURES** DO WE NEED?

(Features Store)

④ "THERE IS NO AI WITHOUT IA"

from
"Hidden Tech.
Debt in ML
Systems" 2015.

CONFIG

DATA
COLLECTION

TESTING
&
DEBUGGING

RESOURCE
MANAGE-
MENT

AUTOMA-
TION

DATA
VERIFICAT-
ION

ML
CORE

MODEL ANALYSIS

SERVICE
INFRA.

FEATURE
ENGINEERING

PROCESS
MANAGEMENT

METADATA MANAGEMENT

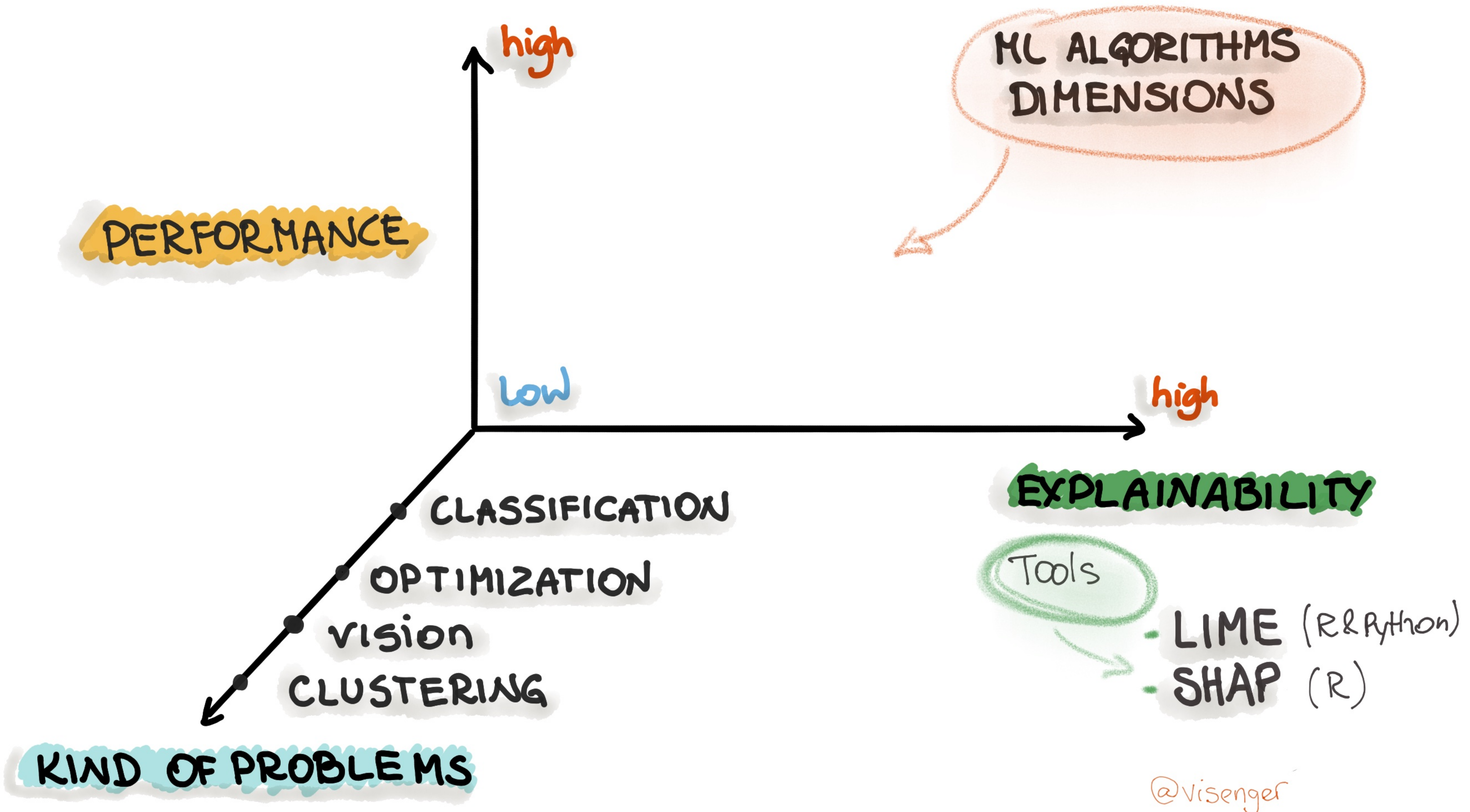
MONITORING

Model-centric

Data-centric

elements of ML-Systems

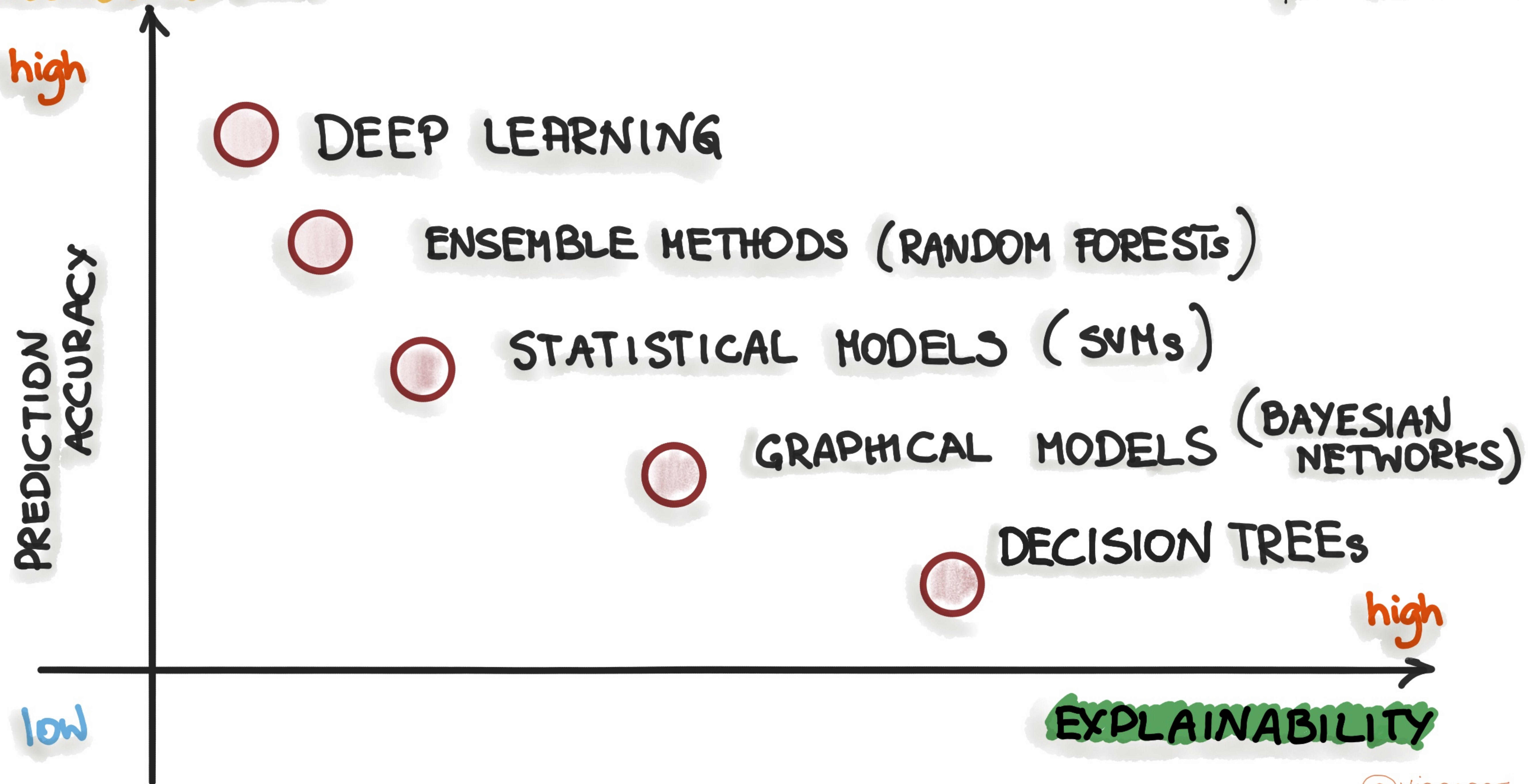
⑤ COMMON SENSE ML over EN VOGUE ML



⑤ COMMON SENSE ML over EN VOGUE ML

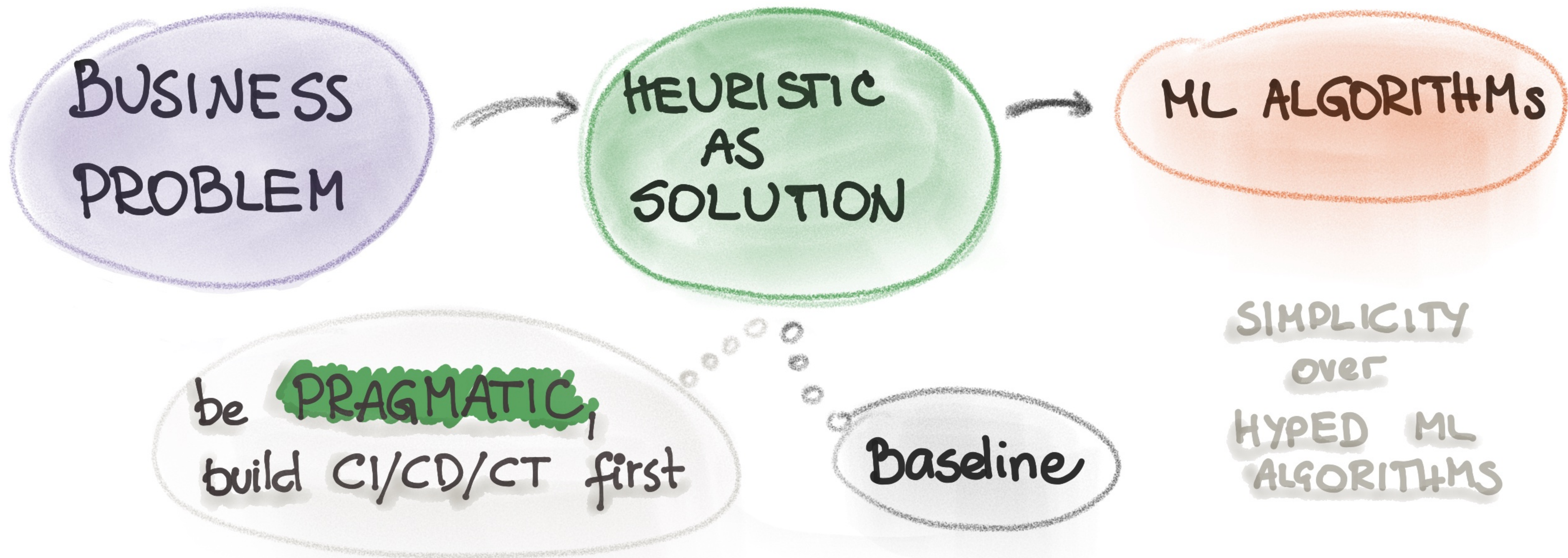
PERFORMANCE

from DARPA XAI



⑤ COMMON SENSE ML over EN VOGUE ML

NO-ML-SOLUTION FIRST

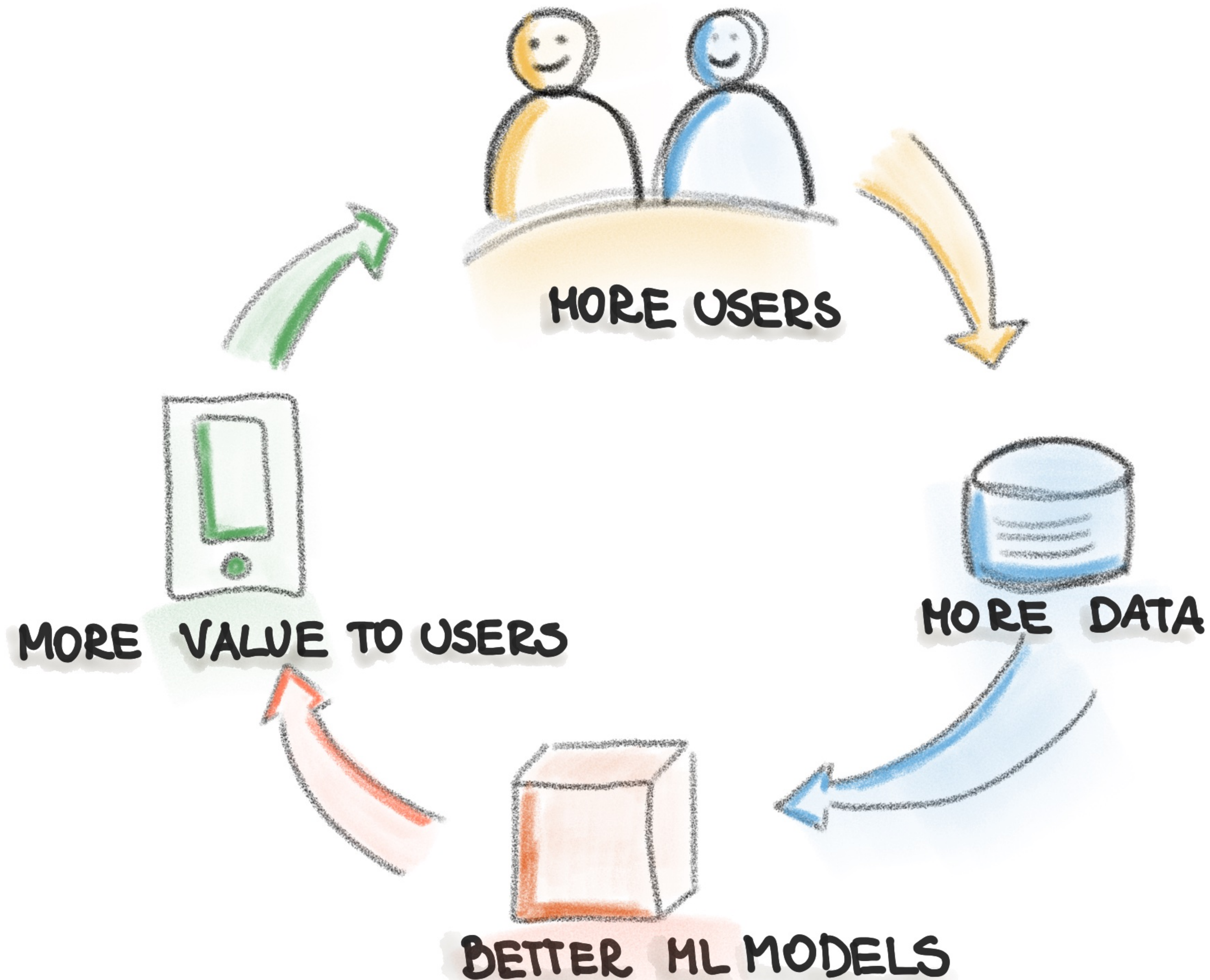


M. Zinkevich "RULES OF MACHINE LEARNING"

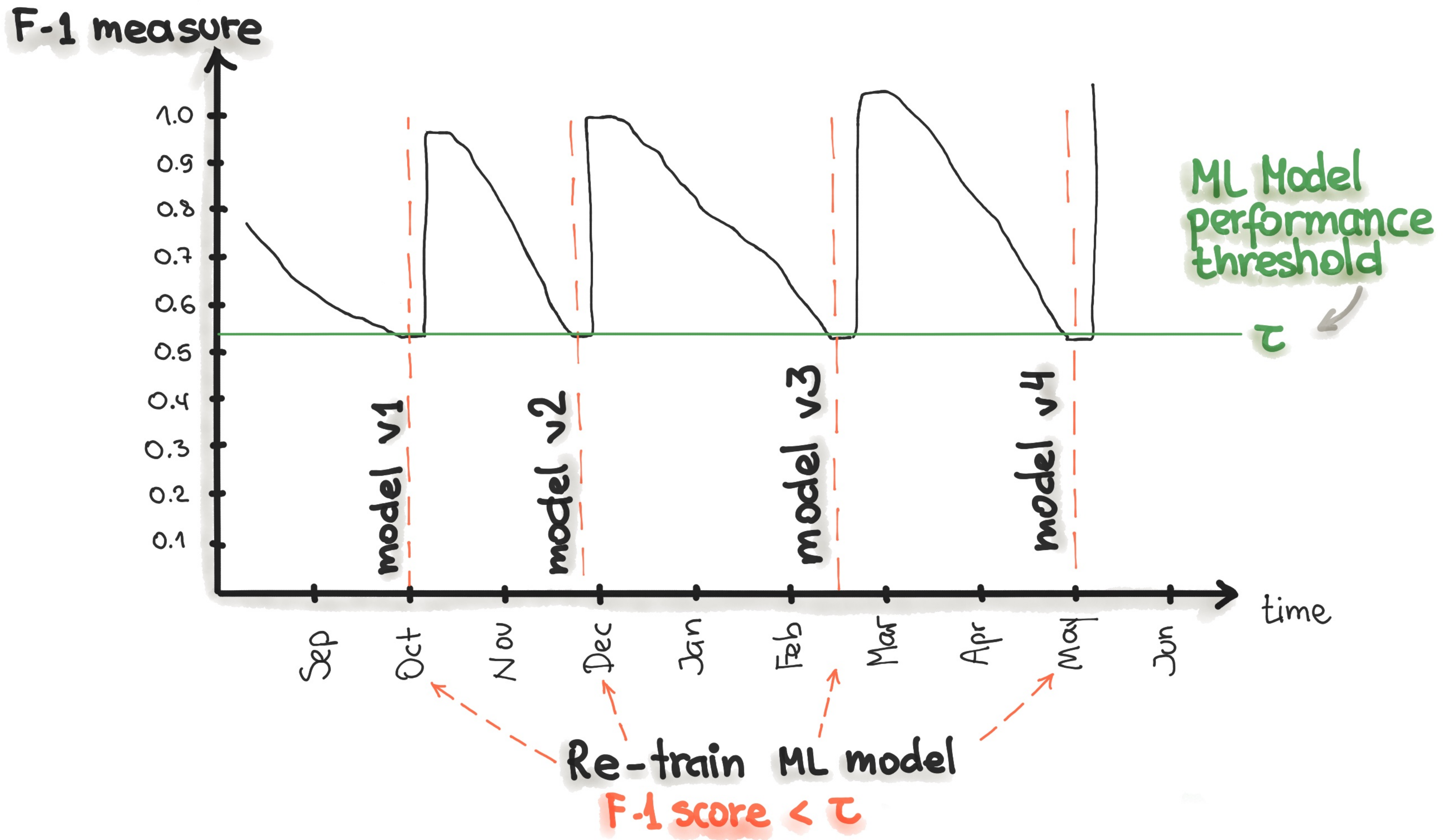
@visenger

⑥

THE FLYWHEEL OF ML SYSTEMS

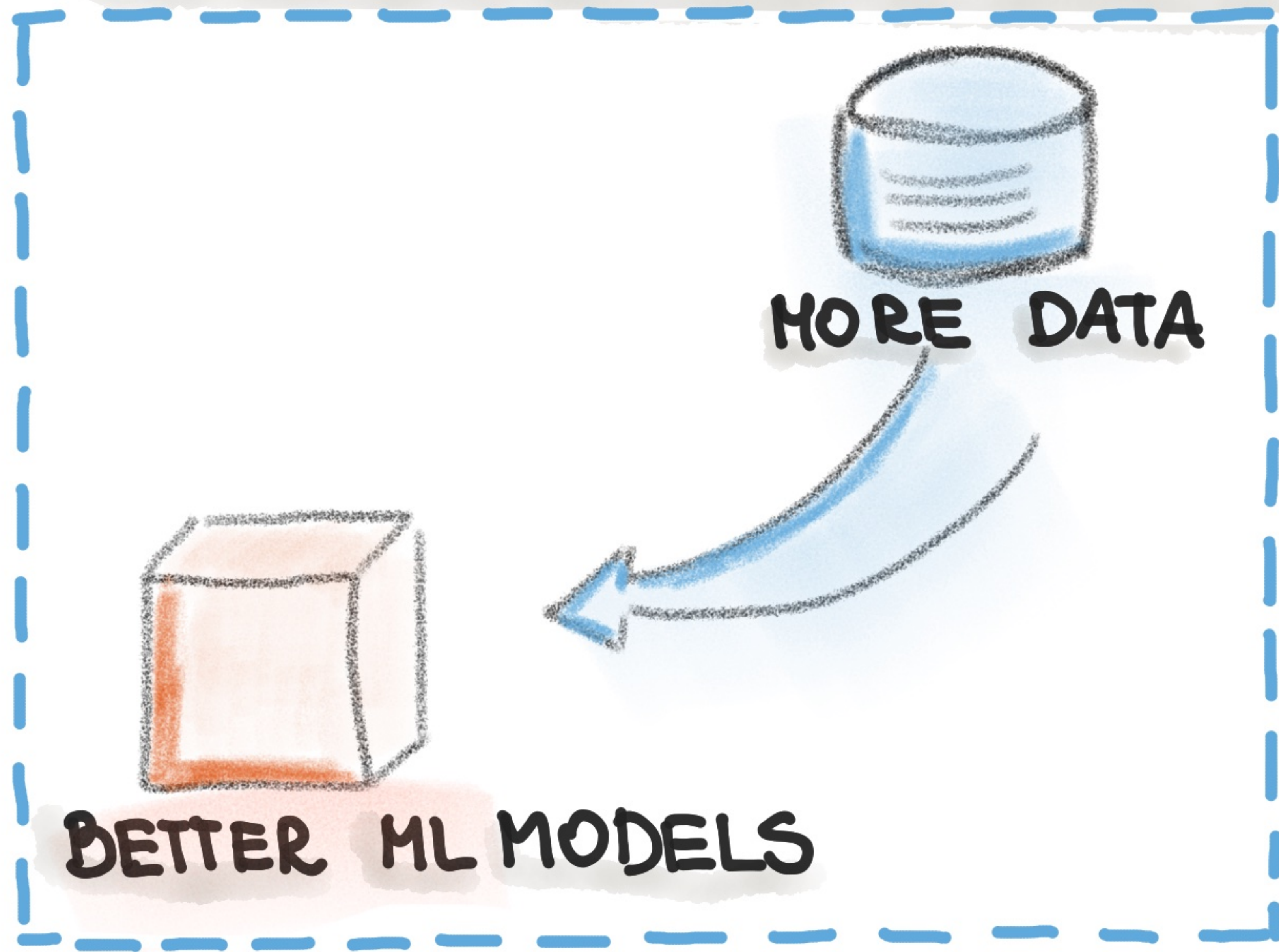


ML MODEL DECAY MONITORING



⑥

THE FLYWHEEL OF ML SYSTEMS



be **PRAGMATIC**,
build CI/CD/CT first

IMPROVING ML MODELS

RE-TRAIN

EXCHANGE

REPLACE
WITH
HEURISTICS

⑥

THE FLYWHEEL OF ML SYSTEMS

WHERE

- DATA PIPELINE
- TRAINING PIPELINE

HOW

- OFFLINE (TRAINING)
- ONLINE (PREDICTION) MONITORING

ML TESTING TAXONOMY

NON-FUNCTIONAL (QUALITY) TESTING

- Efficiency
- Robustness
- Fairness
- Privacy
- Security
- Interpretability

WHAT

FUNCTIONAL TESTING

- Correctness
- Model Relevance

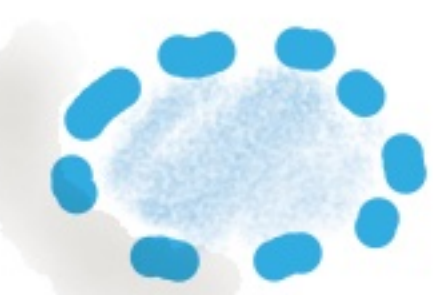
⑦ VERSIONING FOR ML SYSTEMS

CI/CT/CD TRIGGERS

CHECKPOINTS FOR



RECOVERY,



TRACEABILITY,



DECISIONS JUSTIFICATION

⑦ VERSIONING FOR ML SYSTEMS

CI/CT/CD TRIGGERS

ML MODELS

- TRAINING PIPELINE
- ML MODEL (OBJECT)
- HYPERPARAMETERS OPTIMIZATION
- EXPERIMENTS

DATA

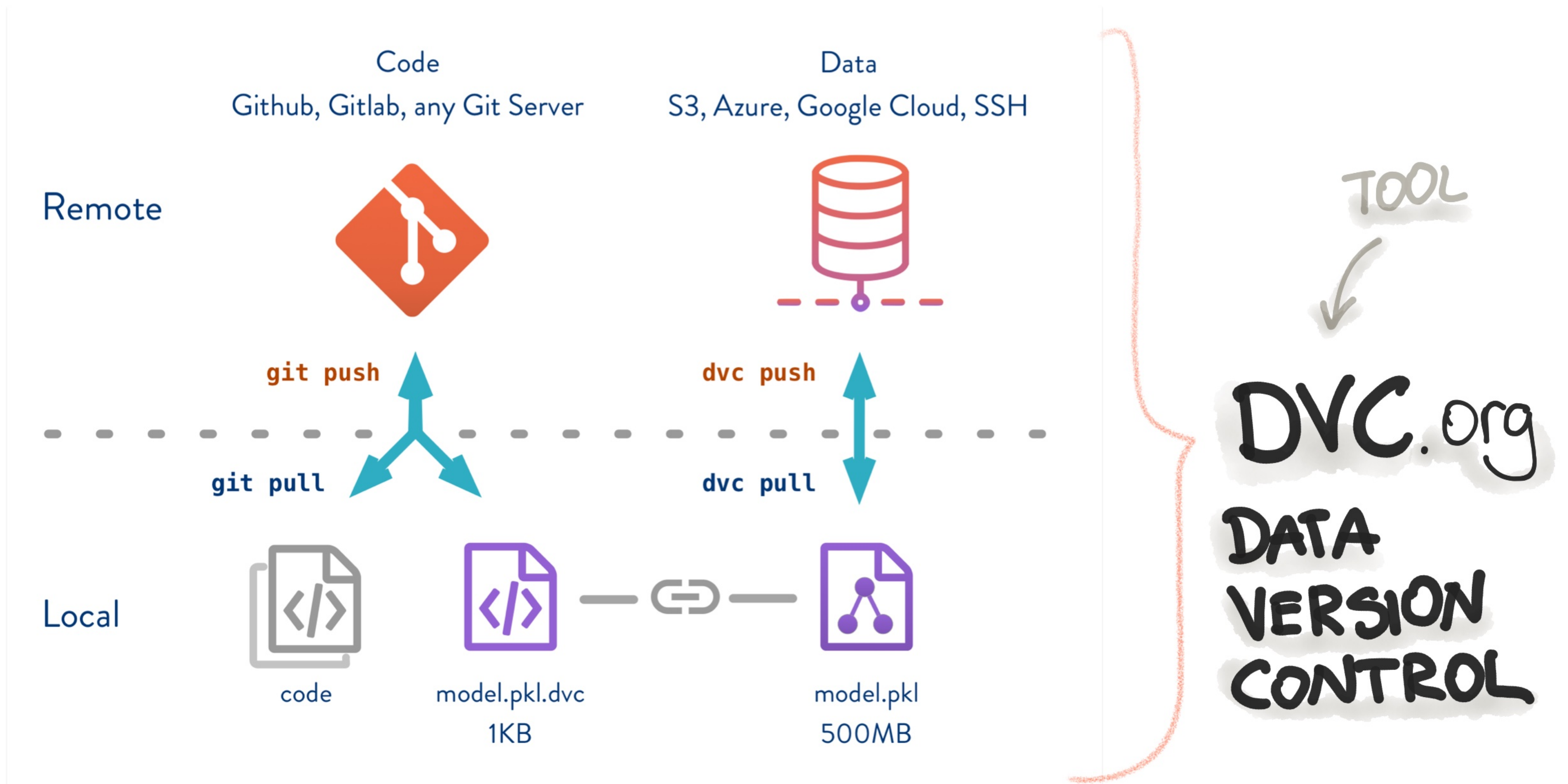
- DATA PREPARATION PIPELINE
- FEATURE STORES
- DATASETS
- METADATA

CODE

- APPLICATION CODE
- CONFIGURATION

⑦

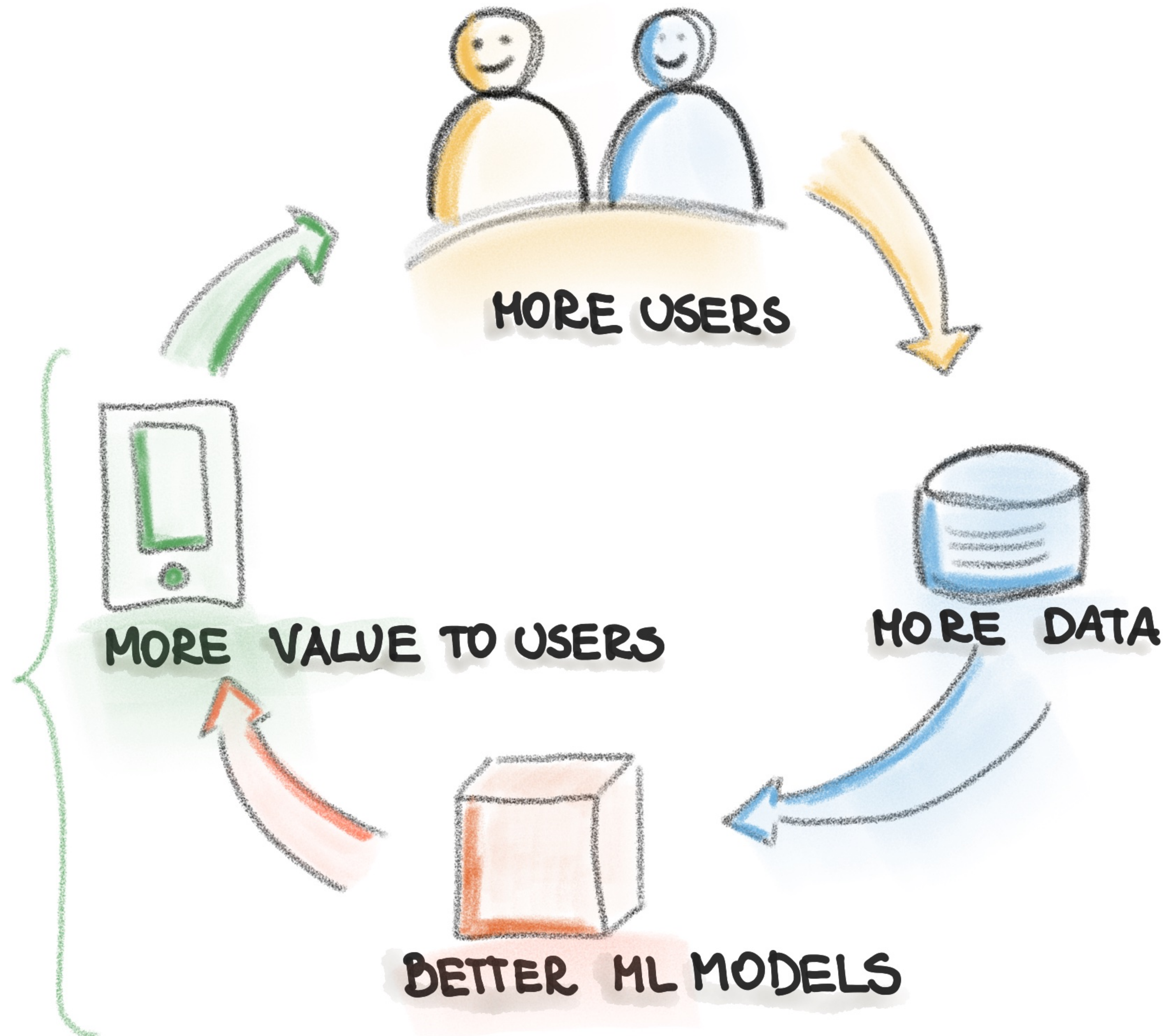
VERSIONING FOR ML SYSTEMS



⑧ DESIGNING ML-SYSTEMS

ML MODELS SHOULD BE
REPLACEABLE
ADAPTABLE FOR CHANGE

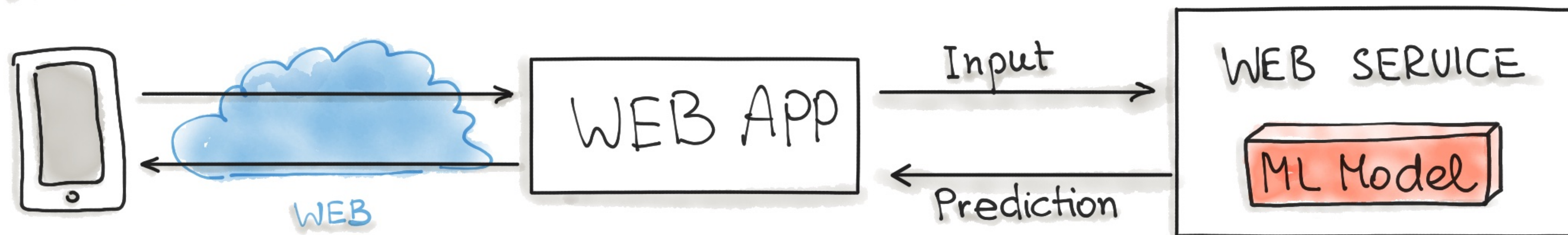
LOOSE COUPLING



⑧ DESIGNING ML-SYSTEMS

SERVING PATTERN FOR ML MODELS

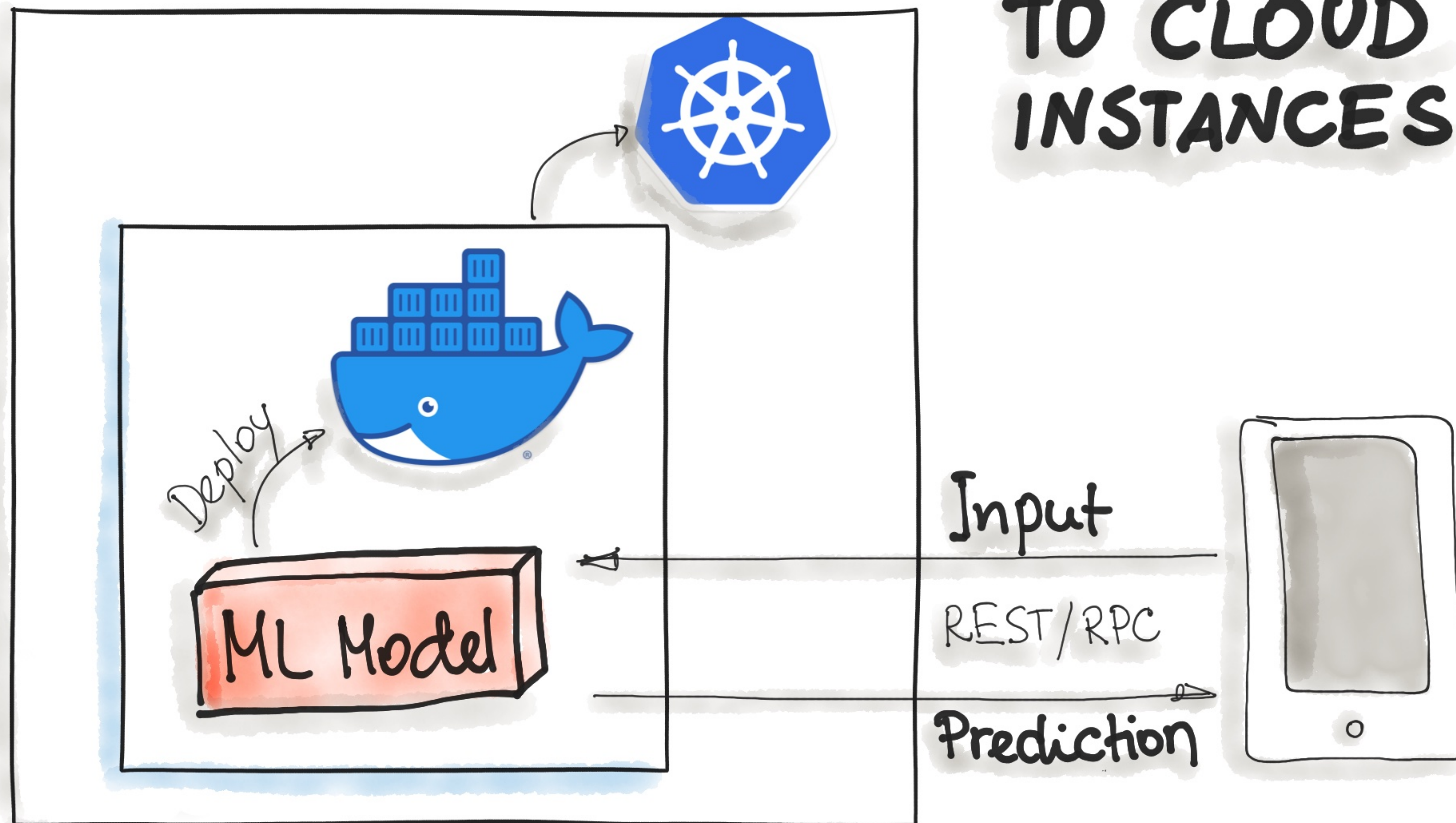
MODEL-as-SERVICE



⑧ DESIGNING ML-SYSTEMS

INFRASTRUCTURE: ML MODEL DEPLOYMENT

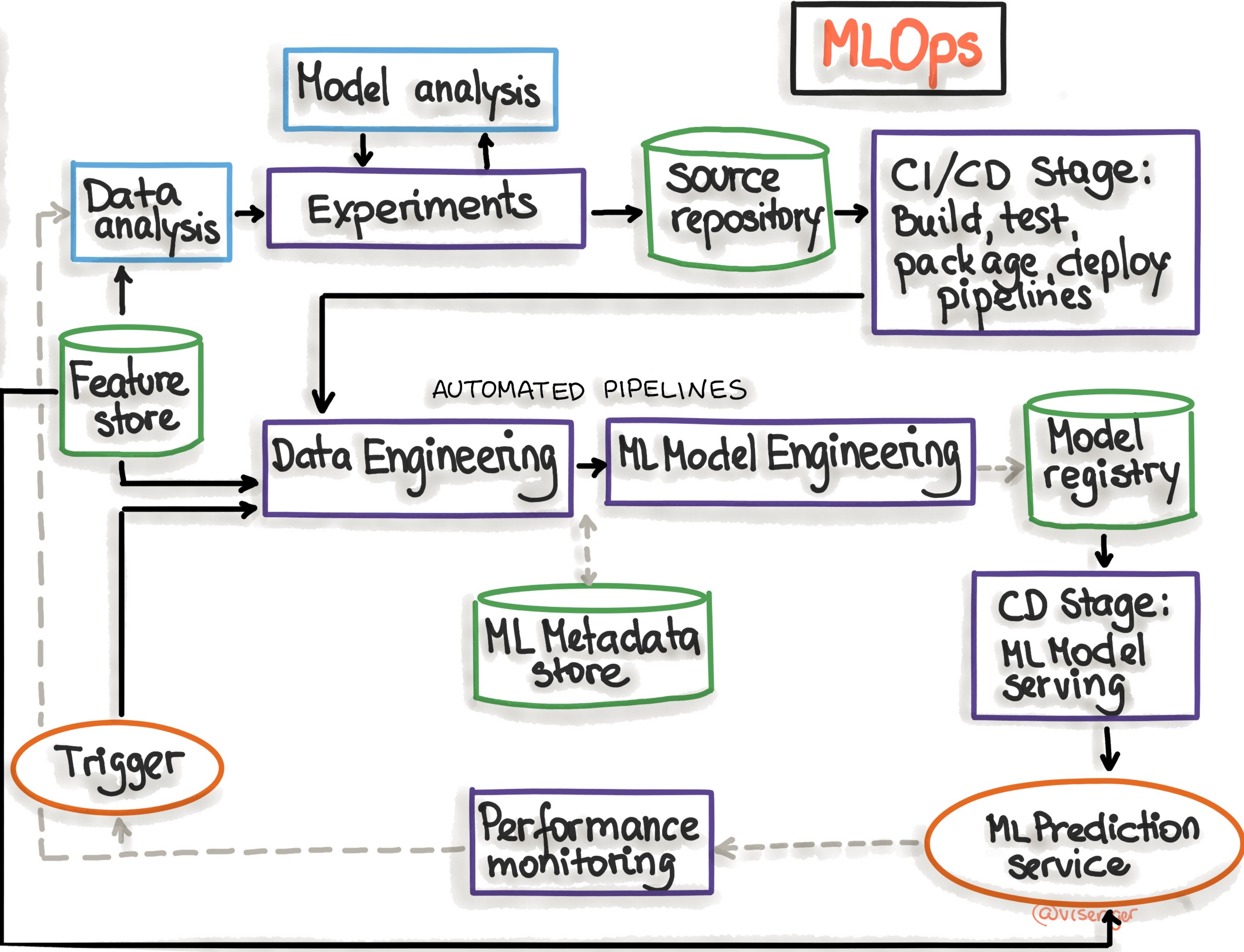
TO CLOUD INSTANCES



MLOps

MODEL DEVELOPMENT

ML OPERATIONS



@v1senger

@ KNOW THE HIDDEN COSTS OF ML ENGINEERING

EXPERTISE?

STORAGE?

(CLOUD) COMPUTING INFRASTRUCTURE?

HUMAN-IN-THE-LOOP?

LABELLING?

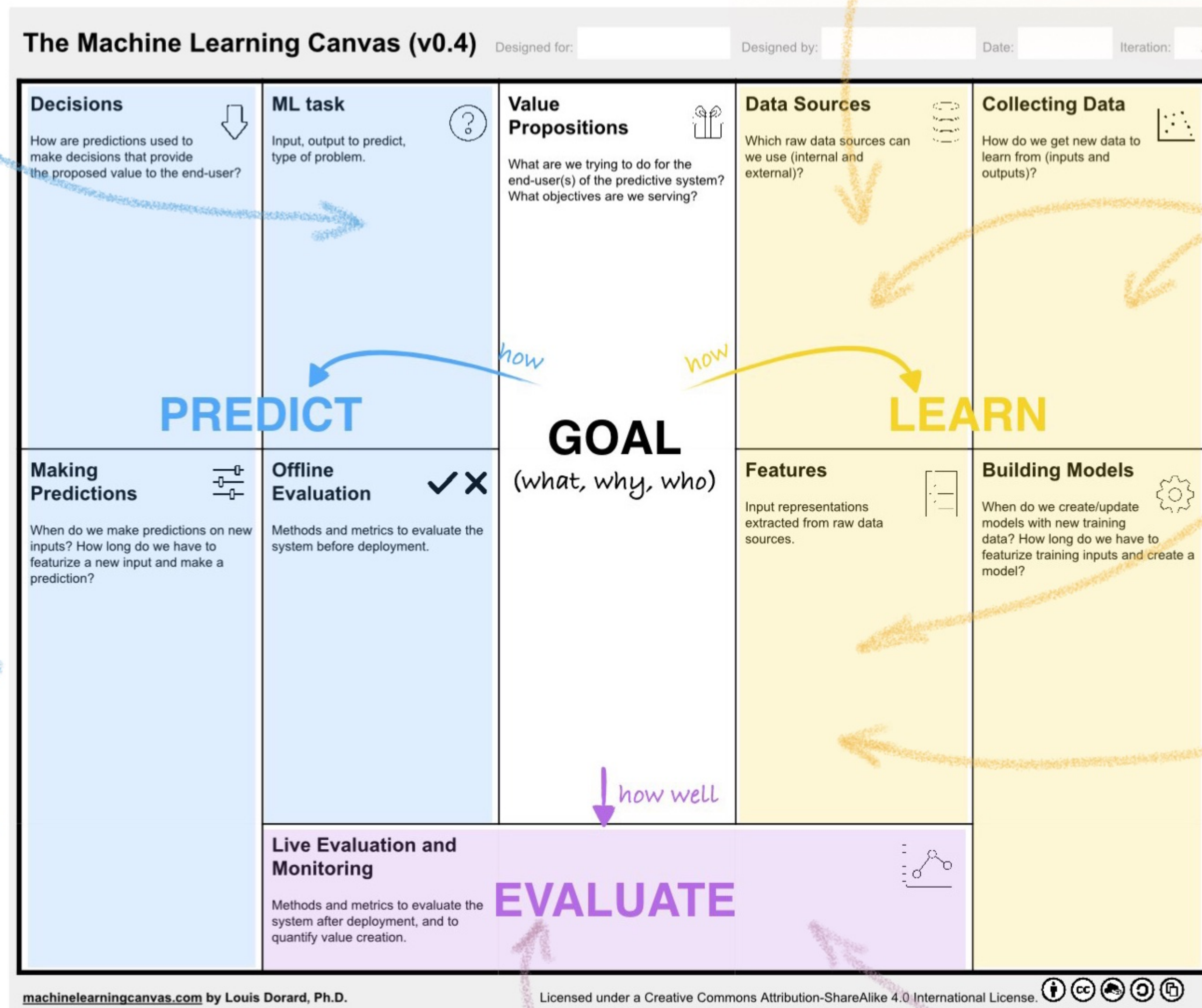
ML SYSTEM MAINTENANCE?

BANDWIDTH?

NETWORK?

INFERENCE TIME?

SHADOW RELEASE



10

BUILD RESPONSIBLE ML MODELS

be aware of ethical issues of AI

- DATA COLLECTION
- DATA REPRESENTATION
- ML MODEL STRUCTURE

- BIAS
- FAIRNESS
- PRIVACY
- INTERPRETABILITY

10

BUILD RESPONSIBLE ML MODELS

ethical issues of AI

- BIAS
- FAIRNESS
- PRIVACY
- INTERPRETABILITY

tools & resources

IBM Research Trusted AI | Home | Demo | Resources | Events | Videos | Community

AI Fairness 360 Open Source Toolkit

This extensible open source toolkit can help you examine, report, and mitigate bias and bias in machine learning models throughout the AI application lifecycle. It includes fairness metrics and 10 state-of-the-art bias mitigation algorithms developed by the community, it is designed to translate algorithmic research from the lab into the real world of domains as wide-ranging as finance, human capital management, healthcare, and more. The toolkit is available in both **Python** and **R**. We invite you to use it and improve it.

Python API Docs | Get Python Code | Get R Code

Not sure what to do first? Start here!

Read More
Learn more about fairness and bias mitigation concepts, terminology, and tools before you begin.

Try a Web Demo
Step through the process of checking and remediating bias in an interactive demo.

English | GitHub | Sign in

TensorFlow | Install | Resources | More | Search

Responsible AI tools for TensorFlow

The TensorFlow ecosystem has a suite of tools and resources to help tackle some of the questions above.

People + AI Guidebook

People + AI Research (PAIR) Guidebook

PAIR Explorables

Explore, via interactive visualizations, key questions and concepts in the realm of Responsible AI.

Microsoft | AI | Products & Services | Approach | AI for Good | Learn | Blog | All Microsoft

Responsible AI resources

Explore resources designed to help you responsibly use AI at every stage of innovation - from concept to development, deployment, and beyond.

Guidelines for responsible AI

Put responsible AI into practice with these guidelines designed to help you anticipate and address potential issues throughout the software development lifecycle.

Human-AI interaction guidelines
Use guidelines for designing AI systems across the user interaction and solution lifecycle.
Explore interaction guidelines >

Conversational AI guidelines
Learn how to design bots that put people first and build trust in your services, using guidelines for responsible conversational AI.
Get the bot guidelines >

Inclusive design guidelines
These guidelines can help you build AI systems that enable and draw on the full range of human diversity.
Get the design guidelines >

@visenger

ML ENGINEERING HIERARCHY OF NEEDS



RESPONSIBLE AI

KNOW ML HIDDEN COSTS

DESIGN FOR ML

VERSIONING FOR ML

ML OPERATIONS

ML ALGORITHMS SIMPLICITY

NO AI WITHOUT IA

ML PROJECT MANAGEMENT

GET THE RIGHT TEAM / SKILLS

SOLVE ML PROBLEM

MLOps @ INNOQ

The screenshot shows a web browser window with the address bar displaying "ml-ops.org". The page content includes the MLOps logo (three circles) and the text "Machine Learning Operations". Below this, a paragraph explains that MLOps aims to provide an end-to-end machine learning development process for reproducible, testable, and evolvable ML-powered software. At the bottom, a diagram consists of three overlapping circles in a horizontal line, labeled "Design", "Model Development", and "Operations" from left to right.

ml-ops.org

MLOps

Machine Learning Operations

With Machine Learning Model Operationalization Management (MLOps), we want to provide an end-to-end machine learning development process to design, build and manage reproducible, testable, and evolvable ML-powered software.

Design Model Development Operations