



QuantUniversity, LLC

www.quantuniversity.com

OLFAI & DATA DAY

ONNX Community Virtual
Meetup October 2021

October 21

Auditing Considerations for ONNX Models and Benchmarking with QuSandbox

Presented By:

Sri Krishnamurthy, CFA, CAP

sri@quantuniversity.com

www.quantuniversity.com

QuantUniversity

- Boston-based Data Science, Quant Finance and Machine Learning AI Risk Advisory
- Specialties include Algorithmic audits, Model Risk Management and AI project enablement
- Training programs for more than 1000 students in Quantitative methods, Data Science, Machine Learning and AI Risk Management
- Building **QuSandbox**, a platform for AI and Machine Learning Governance and Risk Management
- Associate Member of the LFAI since 2021



QuantUniversity, LLC



Algorithmic Auditing

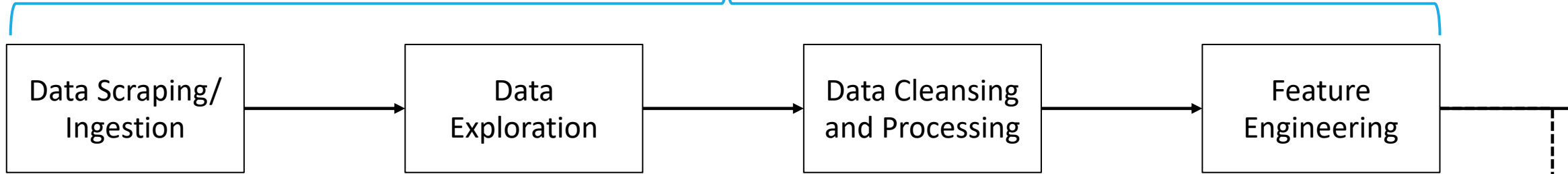
- Algorithmic auditing is a structured process conducted internally or by a qualified independent third party that involves:
 - Verifying and/or validating the working of the algorithm along with the data, model, environment, process, contextual to the use-cases in which the algorithm is intended to be used.
 - Identifying issues that are clearly articulated and scoped for the algorithm. Criteria could include:
 - Bias, fairness, discrimination, explainability, interpretability etc.
 - Documenting the understanding of the algorithm's behavior, uses, performance as observed and evaluated by a qualified individual.
 - Recommending mitigation, control and elimination of noted risks.



Machine Learning Workflow



Data Engineer, Dev Ops Engineer



Robotic Process Automation (RPA) (Microservices, Pipelines)

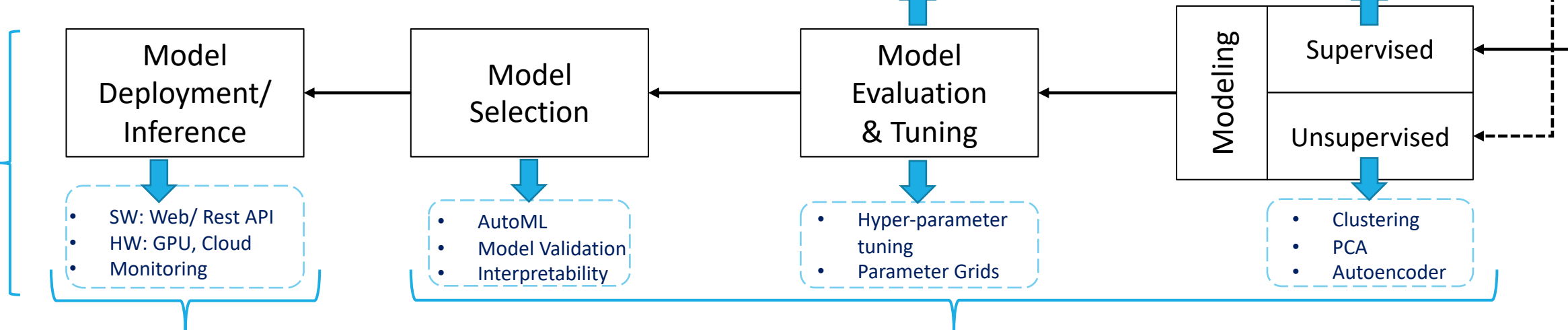


Risk Management/ Compliance(All stages)

Analysts & Decision Makers

- RMS
- MAPS
- MAE
- Confusion Matrix
- Precision/Recall
- ROC

- Regression
- KNN
- Decision Trees
- Naive Bayes
- Neural Networks
- Ensembles



Software/Web Engineer

Data Scientist/Quants

A Machine Learning Audit

Security

Performance

Data used and
profiles

Processing of
data

Data privacy

Algorithmic
performance,
selection

Explainability

Fairness and
Bias

Model
monitoring

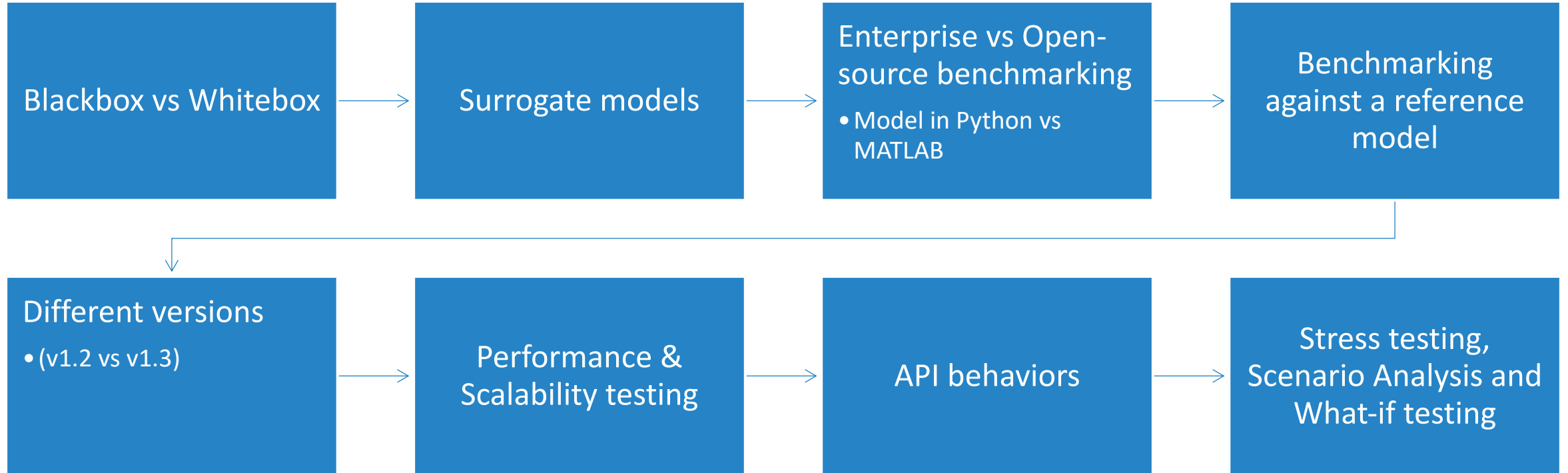
Model failures

Model
deployment

Metrics used
for evaluation











Considerations with auditing and benchmarking models















Demo



-  Sri Krishnamurthy ▲
-  QuProfile
-  Projects
-  QuApiVault
-  Log Out
-  QuToolBox ▼
-  QuModelStudio
-  QuAcademy

⋮ **Projects**

 Summary Summary card 	 Audit Checklist Audit Checklist card	 Data Data card	 Model Model card
 Environment Environment card	 Pipeline Pipeline card	 Explainability Explainability card	 Fairness Fairness and Bias
 Findings Findings card	 Recommendations Recommendations	 Report Report card	

Project Name: ML - Sklearn

Project Description: This model predicts whether breast cancer is benign or malignant based on image measurements.

Project ID: 0d371a9d315447d3af8e9c8adaac23e6

Experiment Name: ML - SKLearn Experiment

Experiment Description:

Experiment ID: 59b00d287b69428b8e6144df25c51d6d

QuSandbox

- QuToolBox
- Data
- Explore
- Data Processing
- Modeling Tools
- Models
- Explain**
- Fairness and Bias
- Report
- Case studies


⋮ **Explain** ⓘ

Search 🔍

CREATE PROJECT

UQ360

Version: 1.0.0




QuSandbox

Adversarial Robustness Toolbox

📄 🗑️

ART

Version: 1.7




QuSandbox

Adversarial Robustness Toolbox

📄 🗑️

H2O

Version: 1.0.0




QuSandbox

Run H2O on QuSandbox

📄 🗑️

AIX-360

Version: 1.0




QuSandbox

AIX-360 Explainability Toolkit

📄 🗑️

Shapash

Version: 1.0




QuSandbox

Make machine learning interpretable and understandable by everyone

📄 🗑️

Manifold

Version: 1.0.0



QuSandbox

Model-agnostic visual debugging tool

📄 🗑️



QuSandbox

Sri Krishnamurthy

QuProjects

QuToolBox

Data

Explore

Data Processing

Modeling Tools

Models

Explain

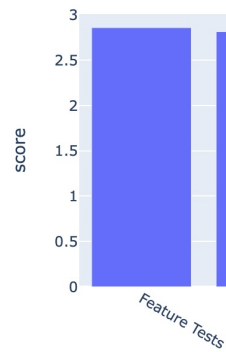
Fairness and Bias

QUReport Score Report credit risk

Id: 8cf00cf70ed9499a9b483362ad58eb4c
Version: 1.1
Date: 2021-05-14

Information
 Experiment: 8cf00cf70ed9499a9b483362ad58eb4c
 Owner: Sri Krishnamurthy
 Contact: info@qusandbox.com
 References: The ML Test Score: A Rubric for ML Production Readiness and Technical Debt Reduction

Final Score



QuSandbox

Sri Krishnamurthy

QuProjects

QuToolBox

QuAcademy

Findings Board

Recommendations Board

TESTPLAN

REPORTS

NOTES

ISSUES

Reports

Name *

Version *

Test Plan

1. Document the test plan for the report

2. How is the model tested (Full, sampled, regression tested)

3. Comment on the testing infrastructure (CI/CD, test suites)





QuantUniversity, LLC
www.quantuniversity.com

Request DEMO at
info@qusandbox.com

QuSandbox

EDUCATION
QUACADEMY

EXPERIMENTATION
QUTOOLBOX

ENABLEMENT
QUSANDBOX

QuantUniversity Course Catalog

- Just Enough Python for Data Science**
Understand the core Python constructs needed to build scalable data science and machine learning applications.
- Machine Learning and AI for Financial Professionals**
Learn how to build pragmatic AI and ML applications with case studies in finance.
- Model Risk Management for Machine Learning Models**
Address the key model risk management and validation challenges when deploying data science and machine learning models in the enterprise.
- The Fintech Bootcamp: The 8 Facets of FinTech**
- Algorithmic Auditing**
- RISK & ML MODELS: STRESS, TESTING & EVALUATION**

QuSandbox Qutoolbox interface showing service cards for:

- MATLAB (Version: 1.0.0)
- Microsoft (Version: 1.0.0)
- Jupyter (Version: 1.0.0)
- Google (Version: 1.0.0)
- NVIDIA RAPIDS (Version: 1.0.0)
- data (Version: 1.0.0)
- Julia (Version: 1.0.0)
- AWS (Version: 1.0.0)

QuSandbox Projects dashboard showing:

- Summary (Summary card)
- Audit Checklist (Audit Checklist card)
- Data (Data card)
- Model (Model card)
- Environment (Environment card)
- Pipeline (Pipeline card)
- Explainability (Explainability card)
- Fairness (Fairness and Bias)
- Findings (Findings card)
- Recommendations (Recommendations)
- Report (Report card)

Project Details:

- Project Name: M... Stream
- Project Description: This model predicts whether breast cancer is benign or malignant based on image measurements.
- Project ID: 3c371e9d31547b38f9e0b0a9c236e
- Experiment Name: ML... SMLearn Experiment
- Experiment Description:
- Experiment ID: 590062876942886e1449255186d

Speaker bio



Sri Krishnamurthy
Founder and CEO
QuantUniversity



- AI advisory focused on AI Risk, Governance and enablement
- Prior Experience at MathWorks, Citigroup and Endeca and 25+ financial services and energy customers.
- Columnist for the [Wilmott Magazine](#)
- Author of forthcoming book [“Pragmatic AI and ML in Finance”](#)
- Teaches AI/ML and Fintech Related topics in the MS and MBA programs at [Northeastern University, Boston](#)
- **Reviewer:** Journal of Asset Management



QuantUniversity, LLC

www.quantuniversity.com

Thank you!

Contact

Sri Krishnamurthy, CFA, CAP
Founder and CEO
QuantUniversity LLC.

LinkedIn [srikrishnamurthy](#)

www.QuantUniversity.com

