
Table of Contents

Preface.....	ix
1. Why Build a Blockchain Truth Machine for AI?.....	1
Dissecting AI's Trust Deficit	1
Machine Learning Concerns	4
Opaque Box Algorithms	5
Genetic Algorithms	8
Data Quality, Outliers, and Edge Cases	8
Supervised Versus Unsupervised ML	10
Reinforcement Learning and Deep Learning	11
Program Synthesis	12
Superintelligent Agents	16
Technological Singularity	17
Attacks and Failures	17
Model/Data Drift	18
Adversarial Data Attacks	19
Risk and Liability	21
Blockchain as an AI Tether	21
Enterprise Blockchain	23
Distributed, Linked Blocks	24
Trust and Transparency	27
Defining Your Use Case	31
Audit Trail	36
Local Memory Bank	36
Shared Memory Bank	37
Four Controls	37
Case Study: Oracle AIoT and Blockchain	38
What's Next?	39

2. Blockchain Controls for AI.....	41
Four Blockchain Controls	41
Blockchain Control 1: Pre-establishing Identity and Workflow Criteria for People and Systems	42
Establishing Identity	42
Predetermining Workflow Among Participants	49
Blockchain Control 2: Distributing Tamper-Evident Verification	57
Using Crypto Anchors to Verify Data Sets, Models, and Pipelines	57
Using Blockchain to Detect Common AI Hacks	58
Understanding Federated Learning and Blockchain	59
Understanding Model Marketplaces	60
Blockchain Control 3: Governing, Instructing, and Inhibiting Intelligent Agents	61
Establishing a Governance Group	63
Implementing On-Chain Governance	64
Developing Compliant Intelligent Agents	66
Blockchain Control 4: Showing Authenticity Through User-Viewable Provenance	69
Deciding Whether to Trust AI	69
Summary	70
3. User Interfaces.....	73
Design Thinking	73
Web Interfaces	75
Blockchain Tethered AI User Interfaces	76
BTA User Mockups	78
Functionality	88
Traceability and Transparency	92
Smartphone and Tablet Apps	95
Email and Text Notifications	96
Spreadsheets	96
Third-Party Systems	96
Working with APIs	98
Integrated Hardware	99
Third-Party Services and Tools	102
System Security	104
AI Security	104
Database Security	105
Blockchain Security	105
Additional Security	105
Summary	106

4. Planning Your BTA.....	107
BTA Architecture	107
Sample Model	108
AI Factsheet: Traffic Signs Detection Model	109
How the Model Works	109
Tethering the Model	110
Subscribing	118
Controlling Access	119
Organization Units	119
Staffings	119
Users	120
Analyzing the Use Case	127
Participants	128
Assets	128
Transactions	129
Smart Contracts	129
Audit Trail	130
Summary	132
5. Running Your Model.....	133
Exercise: Oracle Cloud Setup	133
Creating a Cloud Provider Account	134
Creating a Compartment	135
Creating a Bucket	135
Creating a Pre-authenticated Request	136
Creating Oracle Groups	137
Creating IDCS Groups	138
Mapping Oracle Groups	138
Creating a Policy	139
Generating a Secret Key	140
Exercise: Building and Training a Model	141
Exploring the Model Repository	142
Installing Python and PyTorch	144
Starting the Notebook	145
Configuring Boto3	145
Running Your Notebook	146
Checking the Bucket	147
Optimizing Hyperparameters	149
Learning Rate for Training a Neural Network	149
Number of Training Epochs Used	150
Size of the Training Batches	150
Size of the Hidden Layers	151

Understanding Metrics	151
Accuracy	151
Loss	151
Precision	152
Recall	152
F1 Score	152
Summary	153
6. Instantiating Your Blockchain.....	155
Exercise: Setting Up Hyperledger Fabric	155
Installing Node.js, npm, and NestJS	157
Understanding Hyperledger Fabric 2.0 Required Nodes	157
Installing, Configuring, and Launching the Blockchain	158
Creating and Joining Channels	164
Creating Channels	164
Joining Channels	165
Configuring Anchor Peers	165
Using Chaincodes	165
Understanding Response Struct	168
Using GetTxDateTime	168
Project (project)	168
Model Version (model-version)	171
Model Review (model-review)	173
Model Artifact (model-artifact)	176
Model Experiment (model-experiment)	178
Setting Up the Blockchain Connector	180
Creating Multiple Blockchain Connectors	181
Setting Up the Oracle Connector	182
Configuring Your env File with Your OCI Variables	184
Starting the Oracle Connector	188
More About Integrating Blockchain and the Application Layer	188
Blockchain Connector	194
query	196
OC User Service	196
OC Group	198
Summary	200
7. Preparing Your BTA.....	201
Exercise: Installing and Launching Your BTA	201
Installing the BTA Backend	201
Understanding Your BTA Backend's env File	202
Understanding Your environment.ts File	206

Launching the BTA Frontend	206
Exercise: Creating Users and Permissions	207
Using MailCatcher	207
Configuring the Super Admin	207
Creating a New Subscription Account in Your BTA	210
Configuring Organization Admin's Node	212
Configuring Organization Admin's Channel	213
Verifying the Subscription	213
Activating Your Organization Admin	214
Configuring Access for Your AI Team	214
Summary	229
8. Using Your BTA.....	231
Exercise: Recording Critical AI Touchpoints to Blockchain	231
Adding a New Project	231
Adding a New Version	232
Understanding How Training and Testing Data Use Blockchain	234
Understanding How Models and Algorithms Use Blockchain	235
Understanding How Inputs and Outputs Use Blockchain	235
Understanding How Performance Metrics Use Blockchain	236
Understanding How New Model Versions Use Blockchain	237
Understanding How the Uploads Work	237
Reviewing and Approving the Model	240
Adding AI's Purpose and Intended Domain	246
Exercise: Auditing Your BTA	248
Tracking Your Model's Training and Test Data Sets	248
Tracing Your Inputs and Outputs	249
Verifying Performance Metrics	250
Tracing Identity of People and AI Systems	251
Tracking and Tracing Model Development	251
Identifying Tampering	256
Reversing Your Blockchain Tethered Model	256
Checking the Training Data Sets	258
Checking the Algorithms	258
Retraining the Model	258
Summary	258
Index.....	259

