Table of Contents

Foreword ................................................................. xv
Preface ................................................................. xvii

1. Business Cases for Corda ............................................. 1
   What Is Blockchain? .................................................. 2
   Solving Double Spend ............................................... 3
   What Is Corda? ...................................................... 4
   Business Cases ...................................................... 5
      Decentralized Finance and Digital Assets .................. 5
      Tokenization .................................................... 6
      Capital Raising ................................................ 7
      Traceability and Provenance .................................. 8
      Reconciliation Cost Reduction .............................. 8
      Reconciliation Revenue Streams ............................ 12
      Better AI ....................................................... 13
   Enterprise Requirements ......................................... 14
      Privacy ......................................................... 15
      Know Your Counterparty ................................. 15
      Permissioning ............................................... 15
      Scalability and Performance ................................ 15
      Integration and Developer Adoption .................... 16
   A Brief History of Corda ........................................... 16
   On-Ledger Versus Off-Ledger Data ............................ 21
   Challenges to Adoption ......................................... 22
      The Critical Mass Challenge ............................ 24
      Alternatives to Corda ...................................... 25
      Portability ................................................ 25
Corda Enterprise
Corda Business Networks Toolkit
Wrap-Up

2. Essential Corda and Blockchain Cryptography ................................................................. 27
   Understanding Hashes
      The SHA-256 Hash Algorithm
      Hashes in Corda
   Asymmetric Cryptography
      Symmetric Key Cryptography
      Modern Cryptography
   The Encryption Process
      Combining Encryption with Hashes
      Proof of Origin
      Combining Encryption with Proof of Origin
      Proof of Ownership of a Public Key
   Key Generation Algorithms: Elliptical Curves
   Corda and Keys
   Digital Signatures
      Corda Digital Signatures
   Digital Certificates
      The X.509 Digital Certificate Structure
      Corda Digital Certificates
   Merkle Trees
      Corda Merkle Trees
   Wrap-Up

3. Your First Corda Smart Contract ................................................................. 70
   The Echo CorDapp
      Flow Basics
   High-Level Overview of the Echo CorDapp
   Creating a New CorDapp Project
      Loading the Template Code into IntelliJ
   Overview of Scaffolding Code
      The Initiator
      The Responder
      The Gradle Build File
      Gradle Wrapper Scripts
   Underlying Mechanics of the Echo CorDapp
   Coding the Echo CorDapp
      Coding the Responder Flow
      Completing the EchoInitiatorFlow
Step 2: Create a Grouping Marker for the Versions 215
Step 3: Define a Schema Version of the Model 215
Step 4: Refactor TaskModel as an Inner Class in ToDoSchemaV1 215
Step 5: Implement the QueryableState Interface 216
Inspecting a Queryable State 217
Schedulable States 220
Requiring Signatures by a Certain Time 225
Corda TimeWindows 225
Creating To-Do Time Windows 227
Attaching a File to a To-Do 229
ToDoDist Attachment 230
Running AttachDocToDoInitiator 233
Wrap-Up 236

8. State Linking, Fungibility, Coin Selection, and Observers. 237
   Complex States 238
   Linking States 240
      Locating States on the Ledger 246
      Linking States via StateRef 247
      Linking States via linearId 248
   Reference States 254
      Publishing and Using a Reference State 255
      Example: Stock Symbol 256
   Fungibility 260
      Non-fungible States 261
      Fungible States 262
   Coin Selection 264
      Soft Locking 265
   Fungible Stablecoin Cash on Ledger 268
      Refactoring for Multiple Coin Selection and Fractional Amounts 272
      Redemption: Burning a State 273
   Propagating States to Observers 274
   State Design 277
   Wrap-Up 278

9. Tokens and the Token SDK. 279
   What Are Tokens? 279
   Why Do We Use Tokens? 280
      The Era of Tokens Is Upon Us 281
   A Brief History of Tokens on Blockchain 282
      Bitcoin as a Rigidly Defined Token 283
      Ethereum: Programmable Tokens with Rigid Transactions 284
Corda: Coming Full Circle 287
Illustrating Token Fundamentals with Code 288
Token Ownership 289
Token with Owner 292
Types of Tokens 292
Controlling the Volume 294
Transferring Tokens Out 295
Transferring Tokens In 296
Using the Kotlin infix Operator 297
Non-fungible Tokens 298
Coding a Non-fungible Token 300
The Token SDK 308
Corda Settler and Redemption 310
Wrap-Up 311

10. Oracles and Corda Services .......................................................... 312
Corda Oracles 313
Prime: The Example Corda Oracle CorDapp 313
The Oracle Node 315
The Client Node 320
Filtered Transactions 323
Running the Prime Oracle 325
Corda Oracles with Java: The SDR Oracle 326
Obtaining SDR Data 329
Project Setup 330
Coding the Command Object 332
Coding the SDR Corda Service 332
The sign Method 333
The Client’s Initiator Flow 335
Running the SDR Oracle 338
The Economics of Oracles 338
Wrap-Up 339

11. Node Internals and Analytics ......................................................... 340
Why Python? 341
Quick Start 342
Installing PyCorda 343
The Python REPL 343
Programmatically Downloading the H2 DB Drivers 344
Exploring a Node 345
Reading the Java Keystore for a Node 349
Node and Vault Snapshot to File 350

xii | Table of Contents
Exploring the Vault and CorDapp
   Analyzing a Transaction
   Invoking the Obligation CorDapp’s API Directly from Python
   Generating Tons of Transactions
   Time-Series Charts
   Piping Monitoring Data to Plotly
   Building a Simple Monitoring Web App with PyCorda and Flask
   PyCorda’s Future

12. Corda RPC and Vault Queries

CordaIQ
Obtaining a CordaRPCOps Instance
   RPC Client Setup
RPC Methods
   Network
   Party and Public Key Query
   Flows
   Querying and Managing the Vault
   Transaction Notes
   Attachment Management
   Node Management
   Notary
   State Machine Management
Monitoring RPC Calls
   Using Jolokia
   Using Hawtio
   Pause and Resume via Browser
Wrap-Up

A. The Obligation CorDapp

B. Kotlin Cheat Sheet

C. Comparison Tables

D. DAML for Corda

Index