CONTENTS

ACKNOWLEDGMENTS X

PRELUDE XIV

Who is this book for? XV
Who is this book not for? XVI
Online resources XVII
Requirements XVII
Goals and structure XIX

FOREWORD XX

INTRODUCTION 22

Why Rust and bitcoin are handsome together 23

ANALYZING THE WHITEPAPER 28

Brief history and overview of bitcoin 29
The whitepaper pulled apart 30
Introduction 30
Transactions 31
Timestamp Server 33
Proof-of-Work 33
Network 35
Incentive 37
Reclaiming Disk Space 38
Simplified Payment Verification 39
Combining and Splitting Value 40
Privacy 41
Calculations 41
Conclusion 46
Final evaluation and next steps 46

SETTING UP 50

Installing Rust 52
Rustup vs native packages 54
Installing VS Code and/or Rust Analyzer 58
Installing Rust Analyzer 58
Installing and setting up VS Code 60

Creating a workspace and starting with Rust 64
Crates 64
Dependency management 65
A tiny Cargo command reference 67
Workspace setup 70
Rust: The first contact 72
Hello world 73
Extended example 82
Referring to Rust documentation 94

TAMING RUST'S LEARNING CURVE 98

Memory model 99
Strings in Rust 107
Lifetimes of owned vs unowned values 110
Pattern matching 117
Global "variables" in Rust 118
Object-Oriented Programming in Rust 119
Visibility and privacy 119
User-defined types (structs and enums) 122
Static dispatch 124
Generic param bounds 126
Dynamic dispatch 127
Functional Programming in Rust 128
Immutability 129
The type system 133
Functions and closures 148
Iterators 151

KEEPING RUST CULTURED 156

Rustfmt 157
Clippy 161

IMPLEMENTING A BITCOIN LIBRARY 164

Data types 171
Error handling in Rust 200
Option<T> - Values might be absent 200
Result<T, E> - Recoverable errors 205
Panics - Errors we cannot recover from 208
Error handling in btclib 210
Difficulty 224
Mining 232

Blockchain methods 233
Splitting up the big file 259
Serialization into and deserialization out of files 264
Utility binaries 269

CREATING A CPU MINER 282

Networking 286
Miner that can talk to a node - Asynchronous Rust 291
Futures and promises 292
Tokio in miner 296

BUILDING A BITCOIN NODE 318

Organization 321
Node discovery 323
Fetching the blockchain from other nodes 326
Handling requests 332
Wrapping up 344

MAKING A CLI/TUI WALLET 348

Making a CLI wallet 350
The core of the wallet 365
The main() function 372
TUI wallet version 376
Logging and the util module 376
Core updates 380
Setting up tasks 392
Cursive user interface 397
The main file 417

CONCLUSION AND NEXT STEPS 424

Evaluating our project 425
Recommended reading from Braiins 426
Other resources for Rust and BTC 426
Rust 427
Bitcoin 428
Final words and opinions of Lukáš Hozda, Gentleman (not written by Laurence Stern) 429