

# Contents

Acknowledgments .....	xiii
Introduction .....	xv
<b>CHAPTER 1 Introduction to Blockchain .....</b>	<b>1</b>
Blockchain: An Information Technology .....	6
A Distributed Trusted Information Technology .....	6
Implementation Trends .....	7
Trust: The Byzantine Generals Problem .....	8
The Byzantine Generals Problem Explained: Why Trust Is So Important .....	8
Byzantine Fault Tolerance in Use Today: Why Airplanes Are Safe .....	10
Satoshi Nakamoto's Blockchain Breakthrough .....	11
Satoshi Nakamoto: The Man, the Myth, the Mystery .....	11
Satoshi Nakamoto: Timing Is Everything .....	12
Blockchain: Underpinning of Cryptocurrency .....	13
Types of Blockchain .....	13
Public Blockchains .....	13
Consortium Blockchains .....	14
Private Blockchains .....	14
Comparing Blockchains .....	14
Blockchain Implementations .....	15
Bitcoin .....	16
Namecoin .....	22
Ripple .....	22
Ethereum .....	23
Blockchain Collaborative Implementations .....	24
Hyperledger .....	24
Corda .....	25
Blockchain in Practical Use Today .....	26
Blockchain in the Financial Technology Space .....	27
Blockchain in the Sharing Economy .....	27
Blockchain and Real Estate .....	28
Blockchain and Identity .....	28

## viii Contents

Blockchain and the Practice of Law .....	29
Blockchain Decentralized File Storage .....	30
Decentralized Autonomous Organizations .....	30
Blockchain and Cloud Computing .....	31
Blockchain Gambling and Betting .....	31
Summary .....	31
<b>CHAPTER 2 Business Use Cases.....</b>	<b>33</b>
Currency and Tokens .....	33
Cryptocurrency .....	33
Digital Tokens .....	36
Financial Services Use Cases .....	37
Know Your Customer (KYC) Use Case .....	37
Asset Management Settlement Use Case .....	38
Insurance Claims Processing Use Case .....	38
Trade Finance (Supply Chain) Use Case .....	40
Global Payments Use Case .....	41
Smart Property .....	42
Transferring Ownership of Smart Property .....	43
Using Smart Property as Collateral .....	45
Smart Contracts on the Blockchain .....	46
The Trust Problem .....	46
Blockchain Details .....	48
Blockchain IoT Protocol Projects .....	52
Summary .....	53
<b>CHAPTER 3 Technology Use Cases.....</b>	<b>55</b>
Web Versions 1 and 2 .....	56
Web 3.0 .....	57
Distributed Storage Systems .....	59
InterPlanetary File System .....	59
Swarm .....	62
Storj .....	65
Distributed Computation .....	66
Golem .....	67
Zennet .....	68
Decentralized Communications .....	69
Existing Decentralized Communications .....	70
Whisper .....	70
Summary .....	72
<b>CHAPTER 4 Legal and Governance Use Cases.....</b>	<b>75</b>
Blockchain Changes the Legal Landscape .....	76
Cryptocurrencies as Legal Tender .....	76
Blockchain and Privacy Laws .....	79
Legal Ramifications of Blockchain Records .....	81

The Beginning of Autonomous Law: Smart Contract .....	82
Smart Contract Evolution.....	83
Smart Contract Components.....	83
Smart Contract Benefits .....	84
Smart Contract Challenges.....	85
Smart Contract Risks.....	85
Smart Contract Legal Challenges .....	85
Blockchain as Evidence and Digital Signature.....	87
Smart Contract Design Example .....	88
Is an Advertising Payment Application a Blockchain Fit?.....	89
Defining Contract Data Structures.....	92
Smart Contract Events .....	93
Smart Contract Functions .....	93
Smart Contracts in Practice .....	95
Decentralized Autonomous Organizations .....	96
DAO and Jurisdiction .....	97
DAO Service-Level Liability.....	99
DAO Liability for Contract Breach.....	99
DAO and Intellectual Property .....	99
DAO and Who or What Is Responsible.....	100
DAO Compliance with Financial Services Regulation .....	100
The DAO and Exiting a Contract .....	100
DAO Data as Property.....	100
DAO and Due Diligence .....	101
Summary .....	101
<b>CHAPTER 5 Technology on Ethereum .....</b>	<b>103</b>
Ethereum Accounts .....	105
Ether the Cryptocurrency.....	105
Obtaining Ether .....	106
Mining in Ethereum.....	107
Ethereum Work.....	110
Transactions .....	110
Network Fuel (Gas) .....	111
Messages .....	111
The Ethereum Block .....	115
State Transition Function (STF) .....	116
Code Execution .....	117
Turing Complete .....	118
Scalability.....	119
Infrastructure: Storage and Communication .....	120
Decentralized Applications.....	122
Profile of a Dapp.....	122
Decentralized Autonomous Organizations .....	123
Summary .....	124

<b>CHAPTER 6 Fast-Track Application Tutorial</b>	<b>125</b>
Introducing Solidity	125
Solidity Basics	126
Solidity Functions and Parameters	134
Layout of Storage	137
Run Ethereum Dapps in Your Browser	138
Installing MetaMask	139
Developing a Contract Using MetaMask	139
Remix/Browser Solidity	140
Develop a Simple Smart Contract	140
Deploy the Smart Contract	141
Validate the Smart Contract	142
Next Step: Try Truffle	143
Summary	143
<b>CHAPTER 7 Ethereum Application Best Practices</b>	<b>145</b>
Ethereum Blockchain Development	145
Setting Up the Development Environment for Truffle	145
Set Up a Truffle Project	146
Truffle Directory Structure	146
Ethereum Blockchain Development: Best Practices	146
Blockchain Technologies	147
Solidity Basics Continued	148
Calling Contracts from Contracts	149
Handling Events	151
Smart Contract Design	154
Modules and Interfaces	154
Security and Roles	155
Single Contract Design	156
Linked Contracts	156
User-Specific Contracts	158
Handling Persistent Contract Addresses	160
Halting a Contract	162
Smart Contract Life Cycle: Migration	163
Smart Contract Interaction with Users and Enterprise Applications	164
Debugging Your Smart Contract	164
Debugging Using Remix	164
Debugging Using Events	165
Smart Contract Validation	165
Types of Tests	165
Dry Run Using Private Nets	167
Autopsy of a Wallet Bug	169
The Future	171
Summary	172

<b>CHAPTER 8 Private Blockchain Platforms and Use Cases .....</b>	<b>173</b>
Categories of Blockchain .....	174
Private Blockchain Use Cases .....	175
Private Blockchain Technology .....	176
AlphaPoint Distributed Ledger Platform .....	176
Chain Core .....	177
Corda .....	177
Domus Tower .....	177
The Elements Project .....	178
HydraChain .....	179
Hyperledger .....	179
Interbit .....	197
Monax .....	197
MultiChain .....	213
Openchain .....	214
Quorum .....	214
Stellar .....	215
Symbiont Assembly .....	215
Summary .....	215
<b>CHAPTER 9 Challenges .....</b>	<b>217</b>
Blockchain Governance Challenges .....	218
Bitcoin Blocksize Debate .....	218
The Ethereum DAO Fork .....	220
Ethereum's Move to PoS and Scaling Challenges .....	221
Blockchain Technical Challenges .....	221
Bugs in the Core Code .....	221
Denial-of-Service Attacks .....	222
Security in Smart Contracts .....	223
Scaling .....	228
Sharding .....	229
Summary .....	231
<b>CHAPTER 10 Sample Application: Blockchain and Betting .....</b>	<b>233</b>
What Is a Dapp? .....	233
Introduction to Lotteries, Betting, and Gambling on the Blockchain .....	234
Setting Up a Development Environment .....	236
Syncing an Ethereum Node .....	236
Creating and Configuring a Private Development Chain .....	237
Creating a Killable Contract .....	238
Compiling the Contract .....	240
Deploying a Contract .....	240
Contract Debugging and Interaction .....	243
Defining Data Structures .....	245
Enumerables .....	247

## **xii** Contents

Storage Variables . . . . .	247
Events . . . . .	248
Functions . . . . .	248
Creating a Game . . . . .	249
Bidding . . . . .	250
Scoring Games and Payouts . . . . .	259
Withdrawing . . . . .	260
Reading Games . . . . .	261
Reading Bids . . . . .	261
Summary . . . . .	263
<b>CHAPTER 11 Deploying the Sample Application: Blockchain and Betting . . . . .</b>	<b>265</b>
Deploying Full Contract . . . . .	265
Deploying to the Mainnet . . . . .	266
Seeding Data . . . . .	266
Front-End User Interface . . . . .	271
Pages in the User Interface . . . . .	271
Displaying Games . . . . .	271
Bet Page Markup . . . . .	277
Displaying Game Information . . . . .	280
Displaying Open Bids . . . . .	281
Displaying Bets . . . . .	282
Placing Bids/Bets . . . . .	283
Scoring Games . . . . .	287
Withdrawing Money . . . . .	288
Deploying to AWS . . . . .	290
Summary . . . . .	290
<b>Index . . . . .</b>	<b>291</b>