Indice generale

Prefazione ..... **xi**

Ringraziamenti ..... **xiii**

Parte I **Introduzione** **1**

Capitolo 1 **Introduzione alla blockchain** **3**

La blockchain 3
Il registro collaborativo 4
Criptovalute 5
Smart contract 6
Una rete trustless 6
Nuovi modi per collaborare 7
Un protocollo "grasso" 8
"In Code We Trust" 9
Conclusioni 9

Capitolo 2 **Raggiungere il consenso** **11**

Che cos'è il consenso sulla blockchain? 11
Proof-of-Work (PoW) 12
Proof-of-Stake (PoS) 13
Delegated Proof-of-Stake (DPoS) 14
Conclusioni 15

Capitolo 3 **Una prima app basata su blockchain** **17**

Lo smart contract 18
Front end HTML 21
JavaScript e web3.js 22
Il codice in azione 23

Condividere la DApp 24
Conclusioni 24

Parte II Introduzione a Ethereum 25

Capitolo 4 Per iniziare 27

Procedere con BUIDL 28
Il wallet Metamask 30
Remix 32
Web3 37
Conclusioni 40

Capitolo 5 Concetti e strumenti 41

Wallet Ethereum e concetti di base 41
EtherScan 43
TestRPC 44
Interagire con Ethereum tramite GETH 47
Interagire con Ethereum tramite web3 48
Gestione di un nodo Ethereum 49
Gestione di una rete privata Ethereum 50
Conclusioni 51

Capitolo 6 Smart contract 53

Di nuovo: Hello, World 54
Programmazione di smart contract 55
Codice a consenso e non 56
Strutture di dati 56
Parametri della funzione e valori restituiti dalla funzione 57
Funzioni "pagabili" 57
Richiamare altri contratti 57
Realizzazione e pubblicazione degli smart contract 58
Gli strumenti di Solidity 58
L'IDE di BUIDL 59
L'IDE di Remix 59
Il framework Truffle 60
Richiamare le funzioni dello smart contract 64
L'IDE di BUIDL 64
L'IDE di Remix 64
La console GETH 66
Un nuovo linguaggio 67
Altri linguaggi di programmazione per smart contract 70
Conclusioni 71

Capitolo 7 DApp: applicazioni decentralizzate 73
Lo stack di una DApp 74
La libreria web3 75
Servizi esterni 76
Alcuni esempi di DApp 76
Uniswap 76
Cryptokitties 78
Scommesse 78
DApp interattive 78
Conclusioni 79

Capitolo 8 Alternative alle DApp 81
JavaScript 82
Wallet a nodo completo 82
Transazioni grezze 83
Python e altri 85
Conclusioni 86

Parte III Approfondimenti su Ethereum 87

Capitolo 9 Dentro Ethereum 89
Che cos'è lo "stato" della blockchain? 89
Lo stato di Ethereum 91
Struttura dei dati 92
I trie (o tree) 93
Il trie standard 93
Il Patricia trie 94
Analogie fra il trie e il Patricia trie 96
Differenze principali fra il trie e il Patricia trie 96
Modified Merkle Patricia trie 97
La struttura del trie Ethereum 97
Trie degli stati: l'unico e il solo 97
Trie di memorizzazione: dove si trovano i dati del contratto 98
Trie delle transazioni: uno per blocco 99
Esempi concreti di trie in Ethereum 99
Analisi del database Ethereum 100
Ottenere i dati 101
Decodifica dei dati 102
Leggere e modificare lo stato levelDB 103
Conclusioni 103

Capitolo 10 Servizi di fornitura dati della blockchain 105
Explorer blockchain 106
Raccolta (harvesting) di dati 109
Transazioni e conti 111

Ricompense 111
Identità off-chain 112
Dentro gli smart contract 113
Interfaccia di query 116
Query SQL 116
Query JSON 116
GraphQL 117
BigQuery Google 119
Che cosa ci aspetta 120
Conclusioni 121

Capitolo 11 Un motore di ricerca per smart contract 123

Introduzione 124
Per iniziare 125
La DApp FairPlay 129
Un'architettura modulare 131
Il motore di ricerca per smart contract 131
Casi d'uso 133
Asset in criptovalute 133
DeFi (Decentralized Finance) 133
Giochi 133
Conclusioni 134

Capitolo 12 Sicurezza degli smart contract e best practice 135

Gravi problemi e vulnerabilità degli smart contract Ethereum 136
Attacco Decentralized Autonomous Organization 136
Attacco al token BEC 137
Attacco al wallet Parity 138
L'attacco alle DApp FOMO3D e LastWinner 139
Aspetti sconosciuti e futuro 141
Best practice per la sicurezza degli smart contract 142
Verifica manuale da parte di esperti 143
Verifica formale 143
Sandbox 143
Strumenti 144
Conclusioni 144

Capitolo 13 Il futuro di Ethereum 145

Ethereum 1.0 146
Privacy 146
Consenso 146
Scalabilità 149
Miglioramenti ai token 150
Oltre Ethereum 1.0 150

Lo sharding....151
Zero Knowledge Proof....151
Ethereum 2.0....153
La Beacon Chain....153
eWASM....154
Fasi attuative di Ethereum 2.0....155
Fase 0....155
Fase 1....155
Fase 2....155
Innovazioni post-Ethereum 2.0....156
Conclusioni....156

Parte IV Creazione di protocolli applicativi....157

Capitolo 14 Estensione del protocollo Ethereum....159

Pienamente compatibile, ma più veloce....160
Miglioramenti "smart" alla EVM....161
Oracoli fidati....162
Numeri casuali sicuri....163
Commissioni (gas fee) alternative....163
La sicurezza innanzitutto....164
Conclusioni....165

Capitolo 15 Estensione degli strumenti per Ethereum....167

Strumenti per smart contract....168
Il wallet Venus....168
L'IDE Europa....169
Il compilatore e lo strumento di analisi Lity....173
Strumenti per DApp....174
Web3-cmt....174
L'app CyberMiles....176
Conclusioni....178

Capitolo 16 Esempi di DApp....179

Caso di studio 1: Valentines....180
Lo smart contract Valentines....180
La DApp JavaScript....182
Caso di studio 2: WeBet....184
Lo smart contract WeBet....187
L'applicazione JavaScript WeBet....191
Operazioni off-chain della DApp....198
Conclusioni....199

Capitolo 17 Regole operative e contratti 201

Un esempio 202
Il linguaggio per definire le regole 204
L'algoritmo Rete 205
Gli attributi delle regole 205
I filtri per le regole 206
Le azioni per le regole 207
Ereditarietà delle regole 207
La memoria di lavoro 208
Altri esempi 208
Assicurazione sul volo 208
Tasse 209
Combinazioni di prodotti 211
Conclusioni 212

Capitolo 18 Creazione di una EVM specifica per l'applicazione 213

Uso delle funzioni libENI 214
Inversione della stringa 215
RSA 216
Scrypt 218
Scrivere una funzione libENI 220
Parsing degli argomenti 221
Stima delle commissioni 222
Esecuzione della funzione 222
Associazione al nome della funzione libENI 222
Pubblicazione della funzione libENI 223
Governance CyberMiles 223
Conclusioni 224

Parte V Creare una blockchain 225

Capitolo 19 Per iniziare 227

Il sistema 228
Come funziona 229
Configurazione di un nodo 229
Configurazione di una rete 232
Conclusioni 234

Capitolo 20 La logica operativa 235

Il protocollo 236
Consenso sul blocco 237
Consenso sulle transazioni 238
Ottenere informazioni 238

Un'applicazione d'esempio 239
Implementazione Java 240
Implementazione GO 245
Cosmos SDK 249
Conclusioni 250

Capitolo 21 Creazione di un client della blockchain 251

Panoramica dell'approccio 252
Applicazione di esempio 254
PHP 254
Java 256
Conclusioni 258

Parte VI Cripto-economia 259

Capitolo 22 Cripto-economia e struttura dei token 261

Token per servizi di rete 262
BTC (Bitcoin) 263
ETH (Ethereum) 263
ZEC (ZCash) 264
Token per servizi applicativi 264
Token per titoli (investimenti) 265
La DAO 265
Fondi d'investimento in token 266
Valutazione di mercato dei token 266
Token di servizio 266
Considerazioni progettuali 268
Un approccio alternativo 268
Argomenti avanzati 270
Pricing non monetario 270
Le stable coin 271
Conclusioni 273

Capitolo 23 Initial Coin Offering (ICO) 275

Una breve storia 275
L'utilità di una ICO 276
Facilitatori di un progetto blockchain 277
Fundraising 278
ICO contro finanziamenti di capitale tradizionali 279
Barriera d'ingresso come investimento 279
Barriera d'ingresso come fundraising 279
Leggi/documenti 279
Liquidità dopo il fundraising 280
Partecipazione della community 280
Rischi 280

Dimensioni del mercato....280
Valutazione di un progetto ICO....281
Progetto....281
Team....281
Struttura di fundraising....281
Tabella di distribuzione dei token....281
Community....282
Assetto legale....282
Rischi per la partecipazione a ICO....282
Rischio di hacking....282
Rischi nello sviluppo del progetto....283
Rischi legati al team....283
Conclusioni....283

Capitolo 24 Exchange di criptovalute....285

Tipi di exchange....285
Exchange in valute correnti....285
Exchange per token....286
Exchange per titoli in token....286
Decentralizzazione....287
Prodotti e servizi....289
Conclusioni....289

Appendice A Primi passi con CyberMiles....291

Pubblicazione di un nodo....291
Console interattiva nel nodo....292
Conclusioni....294

Indice analitico....295