1. Record Nr. UNINA9910676564003321

Titolo	Blockchain for distributed systems security / / edited by Sachin S. Shetty, Charles A. Kamhoua, Laurent L. Njilla
Pubbl/distr/stampa	Hoboken, New Jersey : , : Wiley-IEEE, , [2019] [Piscataqay, New Jersey] : , : IEEE Xplore, , [2019]
ISBN	1-119-51958-6 1-119-51962-4 1-119-51959-4
Descrizione fisica	1 online resource (347 pages) : illustrations
Disciplina	005.824
Soggetti	Blockchains (Databases) Internet auctions - Security measures
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Foreword xiii -- Preface xv -- List of Contributors xix -- Part I Introduction to Blockchain 1 -- 1 Introduction 3 /Sachin S. Shetty, Laurent Njilla, and Charles A. Kamhoua -- 1.1 Blockchain Overview 3 -- 1.1.1 Blockchain Building Blocks 5 -- 1.1.2 Blockchain Commercial Use Cases 6 -- 1.1.3 Blockchain Military Cyber Operations Use Cases 11 -- 1.1.4 Blockchain Challenges 13 -- 1.2 Overview of the Book 16 -- 1.2.1 Chapter 2: Distributed Consensus Protocols and Algorithms 16 -- 1.2.2 Chapter 3: Overview of Attack Surfaces in Blockchain 17 -- 1.2.3 Chapter 4: Data Provenance in Cloud Storage with Blockchain 17 -- 1.2.4 Chapter 5: Blockchain-based Solution to Automotive Security and Privacy 18 -- 1.2.5 Chapter 6: Blockchain-based Dynamic Key Management for IoT-Transportation Security Protection 19 -- 1.2.6 Chapter 7: Blockchain-enabled Information Sharing Framework for Cybersecurity 19 -- 1.2.7 Chapter 8: Blockcloud Security Analysis 20 -- 1.2.8 Chapter 9: Security and Privacy of Permissioned and Permissionless Blockchain 20 -- 1.2.9 Chapter 10: Shocking Public Blockchains’ Memory with Unconfirmed Transactions-New DDoS Attacks and Countermeasures 21 -- 1.2.10 Chapter 11: Preventing Digital Currency Miners From Launching Attacks Against Mining Pools

by a Reputation-Based Paradigm 21 -- 1.2.11 Chapter 12: Private Blockchain Configurations for Improved IoT Security 22 -- 1.2.12 Chapter 13: Blockchain Evaluation Platform 22 -- References 23 -- 2 Distributed Consensus Protocols and Algorithms 25 /Yang Xiao, Ning Zhang, Jin Li, Wenjing Lou, and Y. Thomas Hou -- 2.1 Introduction 25 -- 2.2 Fault-tolerant Consensus in a Distributed System 26 -- 2.2.1 The System Model 26 -- 2.2.2 BFT Consensus 28 -- 2.2.3 The OM Algorithm 29 -- 2.2.4 Practical Consensus Protocols in Distributed Computing 30 -- 2.3 The Nakamoto Consensus 37 -- 2.3.1 The Consensus Problem 38 -- 2.3.2 Network Model 38 -- 2.3.3 The Consensus Protocol 39 -- 2.4 Emerging Blockchain Consensus Algorithms 40 -- 2.4.1 Proof of Stake 41.
2.4.2 BFT-based Consensus 42 -- 2.4.3 Proof of Elapsed Time (PoET) 44 -- 2.4.4 Ripple 45 -- 2.5 Evaluation and Comparison 47 -- 2.6 Summary 47 -- Acknowledgment 49 -- References 49 -- 3 Overview of Attack Surfaces in Blockchain 51 /Muhammad Saad, Jeffrey Spaulding, Laurent Njilla, Charles A. Kamhoua, DaeHun Nyang, and Aziz Mohaisen -- 3.1 Introduction 51 -- 3.2 Overview of Blockchain and its Operations 53 -- 3.3 Blockchain Attacks 54 -- 3.3.1 Blockchain Fork 54 -- 3.3.2 Stale Blocks and Orphaned Blocks 54 -- 3.3.3 Countering Blockchain Structure Attacks 55 -- 3.4 Blockchain’s Peer-to-Peer System 55 -- 3.4.1 Selfish Mining 56 -- 3.4.2 The 51% Attack 57 -- 3.4.3 DNS Attacks 57 -- 3.4.4 DDoS Attacks 58 -- 3.4.5 Consensus Delay 59 -- 3.4.6 Countering Peer-to-Peer Attacks 59 -- 3.5 Application Oriented Attacks 60 -- 3.5.1 Blockchain Ingestion 60 -- 3.5.2 Double Spending 60 -- 3.5.3 Wallet Theft 61 -- 3.5.4 Countering Application Oriented Attacks 61 -- 3.6 Related Work 61 -- 3.7 Conclusion and Future Work 62 -- References 62 -- Part II Blockchain Solutions for Distributed System Security 67 -- 4 ProvChain: Blockchain-based Cloud Data Provenance 69 /Xueping Liang, Sachin S. Shetty, Deepak Tosh, Laurent Njilla, Charles A. Kamhoua, and Kevin Kwiat -- 4.1 Introduction 69 -- 4.2 Background and Related Work 70 -- 4.2.1 Data Provenance 70 -- 4.2.2 Data Provenance in the Cloud 71 -- 4.2.3 Blockchain 73 -- 4.2.4 Blockchain and Data Provenance 74 -- 4.3 ProvChain Architecture 75 -- 4.3.1 Architecture Overview 76 -- 4.3.2 Preliminaries and Concepts 77 -- 4.3.3 Threat Model 78 -- 4.3.4 Key Establishment 78 -- 4.4 ProvChain Implementation 79 -- 4.4.1 Provenance Data Collection and Storage 80 -- 4.4.2 Provenance Data Validation 83 -- 4.5 Evaluation 85 -- 4.5.1 Summary of ProvChain’s Capabilities 85 -- 4.5.2 Performance and Overhead 86 -- 4.6 Conclusions and Future Work 90 -- Acknowledgment 91 -- References 92 -- 5 A Blockchain-based Solution to Automotive Security and Privacy 95 /Ali Dorri, Marco Steger, Salil S. Kanhere, and Raja Jurdak.
5.1 Introduction 95 -- 5.2 An Introduction to Blockchain 98 -- 5.3 The Proposed Framework 101 -- 5.4 Applications 103 -- 5.4.1 Remote Software Updates 103 -- 5.4.2 Insurance 105 -- 5.4.3 Electric Vehicles and Smart Charging Services 105 -- 5.4.4 Car-sharing Services 106 -- 5.4.5 Supply Chain 106 -- 5.4.6 Liability 107 -- 5.5 Evaluation and Discussion 108 -- 5.5.1 Security and Privacy Analysis 108 -- 5.5.2 Performance Evaluation 109 -- 5.6 Related Works 112 -- 5.7 Conclusion 113 -- References 114 -- 6 Blockchain-based Dynamic Key Management for IoT-Transportation Security Protection 117 /Ao Lei, Yue Cao, Shihan Bao, Philip Asuquom, Haitham Cruickshank, and Zhili Sun -- 6.1 Introduction 117 -- 6.2 Use Case 119 -- 6.2.1 Message Handover in VCS 120 -- 6.3 Blockchain-based Dynamic Key Management Scheme 124 -- 6.4 Dynamic Transaction Collection Algorithm 125 -- 6.4.1 Transaction Format 125 -- 6.4.2 Block Format

127 -- 6.5 Time Composition 128 -- 6.5.1 Dynamic Transaction Collection Algorithm 129 -- 6.6 Performance Evaluation 130 -- 6.6.1 Experimental Assumptions and Setup 130 -- 6.6.2 Processing Time of Cryptographic Schemes 132 -- 6.6.3 Handover Time 133 -- 6.6.4 Performance of the Dynamic Transaction Collection Algorithm 135 -- 6.7 Conclusion and Future Work 138 -- References 140 -- 7 Blockchain-enabled Information Sharing Framework for Cybersecurity 143 /Abdulhamid Adebayo, Danda B. Rawat, Laurent Njilla, and Charles A. Kamhoua -- 7.1 Introduction 143 -- 7.2 The BIS Framework 145 -- 7.3 Transactions on BIS 146 -- 7.4 Cyberattack Detection and Information Sharing 147 -- 7.5 Cross-group Attack Game in Blockchain-based BIS Framework: One-way Attack 149 -- 7.6 Cross-group Attack Game in Blockchain-based BIS Framework: Two-way Attack 151 -- 7.7 Stackelberg Game for Cyberattack and Defense Analysis 152 -- 7.8 Conclusion 156 -- References 157 -- Part III Blockchain Security 159 -- 8 Blockcloud Security Analysis 161 /Deepak Tosh, Sachin S. Shetty, Xueping Liang, Laurent Njilla, Charles A. Kamhoua, and Kevin Kwiat.
8.1 Introduction 161 -- 8.2 Blockchain Consensus Mechanisms 163 -- 8.2.1 Proof-of-Work (PoW) Consensus 164 -- 8.2.2 Proof-of-Stake (PoS) Consensus 165 -- 8.2.3 Proof-of-Activity (PoA) Consensus 167 -- 8.2.4 Practical Byzantine Fault Tolerance (PBFT) Consensus 168 -- 8.2.5 Proof-of-Elapsed-Time (PoET) Consensus 169 -- 8.2.6 Proof-of-Luck (PoL) Consensus 170 -- 8.2.7 Proof-of-Space (PoSpace) Consensus 170 -- 8.3 Blockchain Cloud and Associated Vulnerabilities 171 -- 8.3.1 Blockchain and Cloud Security 171 -- 8.3.2 Blockchain Cloud Vulnerabilities 174 -- 8.4 System Model 179 -- 8.5 Augmenting with Extra Hash Power 180 -- 8.6 Disruptive Attack Strategy Analysis 181 -- 8.6.1 Proportional Reward 181 -- 8.6.2 Pay-per-last N-shares (PPLNS) Reward 184 -- 8.7 Simulation Results and Discussion 187 -- 8.8 Conclusions and Future Directions 188 -- Acknowledgment 190 -- References 190 -- 9 Permissioned and Permissionless Blockchains 193 /Andrew Miller -- 9.1 Introduction 193 -- 9.2 On Choosing Your Peers Wisely 194 -- 9.3 Committee Election Mechanisms 196 -- 9.4 Privacy in Permissioned and Permissionless Blockchains 199 -- 9.5 Conclusion 201 -- References 202 -- 10 Shocking Blockchain’s Memory with Unconfirmed Transactions: New DDoS Attacks and Countermeasures 205 /Muhammad Saad, Laurent Njilla, Charles A. Kamhoua, Kevin Kwiat, and Aziz Mohaisen -- 10.1 Introduction 205 -- 10.2 Related Work 207 -- 10.3 An Overview of Blockchain and Lifecycle 208 -- 10.3.1 DDoS Attack on Mempools 210 -- 10.3.2 Data Collection for Evaluation 210 -- 10.4 Threat Model 211 -- 10.5 Attack Procedure 212 -- 10.5.1 The Distribution Phase 214 -- 10.5.2 The Attack Phase 214 -- 10.5.3 Attack Cost 214 -- 10.6 Countering the Mempool Attack 215 -- 10.6.1 Fee-based Mempool Design 216 -- 10.6.2 Age-based Countermeasures 221 -- 10.7 Experiment and Results 224 -- 10.8 Conclusion 227 -- References 227 -- 11 Preventing Digital Currency Miners from Launching Attacks Against Mining Pools Using a Reputation-based Paradigm 233 /Mehrdad Nojoumian, Arash Golchubian, Laurent Njilla, Kevin Kwiat, and Charles A. Kamhoua.
11.1 Introduction 233 -- 11.2 Preliminaries 234 -- 11.2.1 Digital Currencies: Terminologies and Mechanics 234 -- 11.2.2 Game Theory: Basic Notions and Definitions 235 -- 11.3 Literature Review 236 -- 11.4 Reputation-based Mining Model and Setting 238 -- 11.5 Mining in a Reputation-based Model 240 -- 11.5.1 Prevention of the Re-entry Attack 240 -- 11.5.2 Technical Discussion on Detection Mechanisms 241 -- 11.5.3 Colluding Miner’s Dilemma 243 -- 11.5.4 Repeated Mining Game 244 -- 11.5.5 Colluding Miners’

Preferences 245 -- 11.5.6 Colluding Miners’ Utilities 245 -- 11.6 Evaluation of Our Model Using Game-theoretical Analyses 246 -- 11.7 Concluding Remarks 248 -- Acknowledgment 249 -- References 249 -- Part IV Blockchain Implementation 253 -- 12 Private Blockchain Configurations for Improved IoT Security 255 /Adriaan Larmuseau and Devu Manikantan Shila -- 12.1 Introduction 255 -- 12.2 Blockchain-enabled Gateway 257 -- 12.2.1 Advantages 257 -- 12.2.2 Limitations 258 -- 12.2.3 Private Ethereum Gateways for Access Control 259 -- 12.2.4 Evaluation 262 -- 12.3 Blockchain-enabled Smart End Devices 263 -- 12.3.1 Advantages 263 -- 12.3.2 Limitations 264 -- 12.3.3 Private Hyperledger Blockchain-enabled Smart Sensor Devices 264 -- 12.3.4 Evaluation 269 -- 12.4 Related Work 270 -- 12.5 Conclusion 271 -- References 271 -- 13 Blockchain Evaluation Platform 275 /Peter Foytik and Sachin S. Shetty -- 13.1 Introduction 275 -- 13.1.1 Architecture 276 -- 13.1.2 Distributed Ledger 276 -- 13.1.3 Participating Nodes 277 -- 13.1.4 Communication 277 -- 13.1.5 Consensus 278 -- 13.2 Hyperledger Fabric 279 -- 13.2.1 Node Types 279 -- 13.2.2 Docker 280 -- 13.2.3 Hyperledger Fabric Example Exercise 281 -- 13.2.4 Running the First Network 281 -- 13.2.5 Running the Kafka Network 286 -- 13.3 Measures of Performance 291 -- 13.3.1 Performance Metrics With the Proof-of-Stake Simulation 293 -- 13.3.2 Performance Measures With the Hyperledger Fabric Example 296 -- 13.4 Simple Blockchain Simulation 300.
13.5 Blockchain Simulation Introduction 303 -- 13.5.1 Methodology 304 -- 13.5.2 Simulation Integration With Live Blockchain 304 -- 13.5.3 Simulation Integration With Simulated Blockchain 306 -- 13.5.4 Verification and Validation 306 -- 13.5.5 Example 307 -- 13.6 Conclusion and Future Work 309 -- References 310 -- 14 Summary and Future Work 311 /Sachin S. Shetty, Laurent Njilla, and Charles A. Kamhoua -- 14.1 Introduction 311 -- 14.2 Blockchain and Cloud Security 312 -- 14.3 Blockchain and IoT Security 312 -- 14.4 Blockchain Security and Privacy 314 -- 14.5 Experimental Testbed and Performance Evaluation 316 -- 14.6 The Future 316 -- Index 319.

Sommario/riassunto

Blockchain for Distributed Systems Security contains a description of the properties that underpin the formal foundations of Blockchain technologies and explores the practical issues for deployment in cloud and Internet of Things "IoT" platforms. The authors - noted experts in the field - present security and privacy issues that must be addressed for Blockchain technologies to be adopted for civilian and military domains. The book covers a range of topics including data provenance in cloud storage, secure IoT models, auditing architecture, and empirical validation of permissioned Blockchain platforms. The book's security and privacy analysis helps with an understanding of the basics of Blockchain and it explores the quantifying impact of the new attack surfaces introduced by Blockchain technologies and platforms. In addition, the book contains relevant and current updates on the topic. This important resource: . Provides an overview of Blockchain-based secure data management and storage for cloud and IoT. Covers cutting-edge research findings on topics including invariant-based supply chain protection, information sharing framework, and trust worthy information federation. Addresses security and privacy concerns in Blockchain in key areas, such as preventing digital currency miners from launching attacks against mining pools, empirical analysis of the attack surface of Blockchain, and more Written for researchers and experts in computer science and engineering, Blockchain for Distributed Systems Security contains the most recent information and academic research to provide an understanding of the application of Blockchain technology.