

1. Record Nr.	UNINA9910555252103321
Titolo	Wireless blockchain : principles, technologies and applications // editors, Bin Cao [et al.]
Pubbl/distr/stampa	Chichester, England : , : John Wiley & Sons, Inc., , [2022] ©2022
ISBN	1-119-79082-4 1-119-79083-2 1-119-79081-6
Descrizione fisica	1 online resource (331 pages)
Collana	IEEE Press Ser.
Disciplina	005.74
Soggetti	Wireless communication systems - Industrial applications Blockchains (Databases) Personal communication service systems Electronic books.
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Cover -- Title Page -- Copyright -- Contents -- List of Contributors -- Preface -- Abbreviations -- Chapter 1 What is Blockchain Radio Access Network? -- 1.1 Introduction -- 1.2 What is BRAN -- 1.2.1 BRAN Framework -- 1.2.2 Consensus Mechanism -- 1.2.3 Implementation -- 1.3 Mining Model -- 1.3.1 HashBased Mining -- 1.3.2 Modeling of Hash Trials -- 1.3.3 Threat Model -- 1.4 BRAN Queuing Model -- 1.5 Latency Analysis of BRAN -- 1.5.1 SteadyState Analysis -- 1.5.2 Average Service Latency -- 1.6 Security Considerations -- 1.6.1 Alternative History Attack -- 1.6.2 Probability of a Successful Attack -- 1.7 LatencySecurity Tradeoff -- 1.8 Conclusions and Future Works -- 1.8.1 Network Effect and Congest Effect -- 1.8.2 Chicken and Eggs -- 1.8.3 Decentralization and Centralization -- 1.8.4 Beyond Bitcoin Blockchain -- References -- Chapter 2 Consensus Algorithm Analysis in Blockchain: PoW and Raft -- 2.1 Introduction -- 2.2 Mining Strategy Analysis for the PoW ConsensusBased Blockchain -- 2.2.1 Blockchain Preliminaries -- 2.2.2 Proof of Work and Mining -- 2.2.3 Honest Mining Strategy -- 2.2.4 PoW Blockchain Mining Model -- 2.2.4.1 State --

2.2.4.2 Action -- 2.2.4.3 Transition and Reward -- 2.2.4.4 Objective Function -- 2.2.4.5 Honest Mining -- 2.2.4.6 Selfish Mining -- 2.2.4.7 Lead Stubborn Mining -- 2.2.4.8 Optimal Mining -- 2.2.5 Mining Through RL -- 2.2.5.1 Preliminaries for Original Reinforcement Learning Algorithm -- 2.2.5.2 New Reinforcement Learning Algorithm for Mining -- 2.2.6 Performance Evaluations -- 2.3 Performance Analysis of the Raft Consensus Algorithm -- 2.3.1 Review of Raft Algorithm -- 2.3.2 System Model -- 2.3.3 Network Model -- 2.3.4 Network Split Probability -- 2.3.5 Average Number of Replies -- 2.3.6 Expected Number of Received Heartbeats for a Follower -- 2.3.7 Time to Transition to Candidate. 2.3.8 Time to Elect a New Leader -- 2.3.9 Simulation Results -- 2.3.10 Discussion -- 2.3.10.1 Extended Model -- 2.3.10.2 System Availability and Consensus Efficiency -- 2.4 Conclusion -- References -- Chapter 3 A Low Communication Complexity Doublelayer PBFT Consensus -- 3.1 Introduction -- 3.1.1 PBFT Applied to Blockchain -- 3.1.2 From CFT to BFT -- 3.1.2.1 State Machine Replication -- 3.1.2.2 Primary Copy -- 3.1.2.3 Quorum Voting -- 3.1.3 Byzantine Generals Problem -- 3.1.4 Byzantine Consensus Protocols -- 3.1.4.1 TwoPhase Commit -- 3.1.4.2 View Stamp -- 3.1.4.3 PBFT Protocol -- 3.1.5 Motivations -- 3.1.6 Chapter Organizations -- 3.2 DoubleLayer PBFTBased Protocol -- 3.2.1 Consensus Flow -- 3.2.1.1 The Client -- 3.2.1.2 FirstLayer Protocol -- 3.2.1.3 SecondLayer Protocol -- 3.2.2 Faulty Primary Elimination -- 3.2.2.1 Faulty Primary Detection -- 3.2.2.2 View Change -- 3.2.3 Garbage Cleaning -- 3.3 Communication Reduction -- 3.3.1 Operation Synchronization -- 3.3.2 Safety and Liveness -- 3.4 Communication Complexity of DoubleLayer PBFT -- 3.5 Security Threshold Analysis -- 3.5.1 Faulty Probability Determined -- 3.5.2 Faulty Number Determined -- 3.6 Conclusion -- References -- Chapter 4 BlockchainDriven Internet of Things -- 4.1 Introduction -- 4.1.1 Challenges and Issues in IoT -- 4.1.2 Advantages of Blockchain for IoT -- 4.1.3 Integration of IoT and Blockchain -- 4.2 Consensus Mechanism in Blockchain -- 4.2.1 PoW -- 4.2.2 PoS -- 4.2.3 Limitations of PoW and PoS for IoT -- 4.2.3.1 Resource Consumption -- 4.2.3.2 Transaction Fee -- 4.2.3.3 Throughput Limitation -- 4.2.3.4 Confirmation Delay -- 4.2.4 PBFT -- 4.2.5 DAG -- 4.2.5.1 Tangle -- 4.2.5.2 Hashgraph -- 4.3 Applications of Blockchain in IoT -- 4.3.1 Supply Chain -- 4.3.1.1 Introduction -- 4.3.1.2 Modified Blockchain -- 4.3.1.3 Integrated Architecture -- 4.3.1.4 Security Analysis. 4.3.2 Smart City -- 4.3.2.1 Introduction -- 4.3.2.2 Smart Contract System -- 4.3.2.3 Main Functions of the Framework -- 4.3.2.4 Discussion -- 4.4 Issues and Challenges of Blockchain in IoT -- 4.4.1 Resource Constraints -- 4.4.2 Security Vulnerability -- 4.4.3 Privacy Leakage -- 4.4.4 Incentive Mechanism -- 4.5 Conclusion -- References -- Chapter 5 Hyperledger BlockchainBased Distributed Marketplaces for 5G Networks -- 5.1 Introduction -- 5.2 Marketplaces in Telecommunications -- 5.2.1 Wireless Spectrum Allocation -- 5.2.2 Network Slicing -- 5.2.3 Passive optical networks (PON) Sharing -- 5.2.4 Enterprise Blockchain: Hyperledger Fabric -- 5.2.4.1 Shared Ledger -- 5.2.4.2 Organizations -- 5.2.4.3 Consensus Protocol -- 5.2.4.4 Network Peers -- 5.2.4.5 Smart Contracts (chaincodes) -- 5.2.4.6 Channels -- 5.3 Distributed Resource Sharing Market -- 5.3.1 Market Mechanism (Auction) -- 5.3.2 Preliminaries -- 5.4 Experimental Design and Results -- 5.4.1 Experimental Blockchain Deployment -- 5.4.1.1 Cloud Infrastructure -- 5.4.1.2 Container Orchestration: Docker Swarm -- 5.4.2 Blockchain Performance Evaluation -- 5.4.3 Benchmark Apparatus -- 5.4.3.1 Hyperledger Caliper -- 5.4.3.2 Data Collection: Prometheus Monitor -- 5.4.4 Experimental Results -- 5.4.4.1

Maximum Transaction Throughput -- 5.4.4.2 Block Size -- 5.4.4.3
Network Size -- 5.5 Conclusions -- References -- Chapter 6
Blockchain for Spectrum Management in 6G Networks -- 6.1
Introduction -- 6.2 Background -- 6.2.1 Rise of Microoperators --
6.2.2 Case for Novel Spectrum Sharing Models -- 6.2.2.1 Blockchain for
Spectrum Sharing -- 6.2.2.2 Blockchain in 6G Networks -- 6.3
Architecture of an Integrated SDN and Blockchain Model -- 6.3.1 SDN
Platform Design -- 6.3.2 Blockchain Network Layer Design -- 6.3.3
Network Operation and Spectrum Management -- 6.4 Simulation
Design -- 6.5 Results and Analysis.
6.5.1 Radio Access Network and Throughput -- 6.5.2 Blockchain
Performance -- 6.5.3 Blockchain Scalability Performance -- 6.6
Conclusion -- Acknowledgments -- References -- Chapter 7
Integration of MEC and Blockchain -- 7.1 Introduction -- 7.2 Typical
Framework -- 7.2.1 BlockchainEnabled MEC -- 7.2.1.1 Background --
7.2.1.2 Framework Description -- 7.2.2 MECBased Blockchain --
7.2.2.1 Background -- 7.2.2.2 Framework Description -- 7.3 Use Cases
-- 7.3.1 Security Federated Learning via MECEnabled Blockchain
Network -- 7.3.1.1 Background -- 7.3.1.2 BlockchainDriven Federated
Learning -- 7.3.1.3 Experimental Results -- 7.3.2 BlockchainAssisted
Secure Authentication for CrossDomain Industrial IoT -- 7.3.2.1
Background -- 7.3.2.2 BlockchainDriven CrossDomain Authentication
-- 7.3.2.3 Experimental Results -- 7.4 Conclusion -- References --
Chapter 8 Performance Analysis on Wireless Blockchain IoT System --
8.1 Introduction -- 8.2 System Model -- 8.2.1 BlockchainEnabled IoT
Network Model -- 8.2.2 Wireless Communication Model -- 8.3
Performance Analysis in BlockchainEnabled Wireless IoT Networks --
8.3.1 Probability Density Function of SINR -- 8.3.2 TDP Transmission
Successful Rate -- 8.3.3 Overall Communication Throughput -- 8.4
Optimal FN Deployment -- 8.5 Security Performance Analysis -- 8.5.1
Eclipse Attacks -- 8.5.2 Random Link Attacks -- 8.5.3 Random FN
Attacks -- 8.6 Numerical Results and Discussion -- 8.6.1 Simulation
Settings -- 8.6.2 Performance Evaluation without Attacks -- 8.7
Chapter Summary -- References -- Chapter 9 Utilizing Blockchain as a
CitizenUtility for Future Smart Grids -- 9.1 Introduction -- 9.2 DET
Using CitizenUtilities -- 9.2.1 Prosumer Community Groups -- 9.2.1.1
Microgrids -- 9.2.1.2 Virtual Power Plants (VPP) -- 9.2.1.3 Vehicular
Energy Networks (VEN) -- 9.2.2 Demand Side Management -- 9.2.2.1
Energy Efficiency.
9.2.2.2 Demand Response -- 9.2.2.3 Spinning Reserves -- 9.2.3 Open
Research Challenges -- 9.2.3.1 Scalability and IoT Overhead Issues --
9.2.3.2 Privacy Leakage Issues -- 9.2.3.3 Standardization and
Interoperability Issues -- 9.3 Improved CitizenUtilities -- 9.3.1 Toward
Scalable CitizenUtilities -- 9.3.1.1 Challenges -- 9.3.1.2 HARB
FrameworkBased CitizenUtility -- 9.3.2 Toward PrivacyPreserving
CitizenUtilities -- 9.3.2.1 Threat Model -- 9.3.2.2 PDCH System -- 9.4
Conclusions -- References -- Chapter 10 Blockchainenabled COVID19
Contact Tracing Solutions -- 10.1 Introduction -- 10.2 Preliminaries of
BeepTrace -- 10.2.1 Motivation -- 10.2.1.1 Comprehensive Privacy
Protection -- 10.2.1.2 Performance is Uncompromising -- 10.2.1.3
Broad Community Participation -- 10.2.1.4 Inclusiveness and Openness
-- 10.2.2 Two Implementations are Based on Different Matching
Protocols -- 10.3 Modes of BeepTrace -- 10.3.1 BeepTraceActive --
10.3.1.1 Active Mode Workflow -- 10.3.1.2 Privacy Protection of
BeepTraceActive -- 10.3.2 BeepTracePassive -- 10.3.2.1 TwoChain
Architecture and Workflow -- 10.3.2.2 Privacy Protection in BeepTrace
Passive -- 10.4 Future Opportunity and Conclusions -- 10.4.1
Preliminary Approach -- 10.4.2 Future Directions -- 10.4.2.1 Network

Throughput and Scalability -- 10.4.2.2 Technology for Elders and
Minors -- 10.4.2.3 Battery Drainage and Storage Optimization --
10.4.2.4 Social and Economic Aspects -- 10.4.3 Concluding Remarks
-- References -- Chapter 11 Blockchain Medical Data Sharing -- 11.1
Introduction -- 11.1.1 General Overview -- 11.1.2 Defining Challenges
-- 11.1.2.1 Data Security -- 11.1.2.2 Data Privacy -- 11.1.2.3 Source
Identity -- 11.1.2.4 Data Utility -- 11.1.2.5 Data Interoperability --
11.1.2.6 Trust -- 11.1.2.7 Data Provenance -- 11.1.2.8 Authenticity --
11.1.3 Sharing Paradigms.
11.1.3.1 InstitutiontoInstitution Data Sharing.
