1. Record Nr. UNINA9911018826003321

Autore	Al-Dulaimi Anwer
Titolo	Blockchains : empowering technologies and industrial applications
Pubbl/distr/stampa	Newark : , : John Wiley & Sons, Incorporated, , 2023 ©2024
ISBN	9781119781042 1119781043 9781119781028 1119781027
Edizione	[1st ed.]
Descrizione fisica	1 online resource (419 pages)
Collana	IEEE Series on Digital and Mobile Communication Series
Altri autori (Persone)	DobreOctavia A YiZhilin
Disciplina	005.74
Soggetti	Blockchains (Databases) Distributed databases
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Cover -- Title Page -- Copyright -- Contents -- About the Editors -- About the Contributors -- Foreword -- Preface -- Chapter 1 Introduction -- 1.1 Exploring Blockchain Technology -- 1.2 Developing and Testing Blockchains: Software Development Approach -- 1.3 Blockchains and Cloud Integration -- 1.4 Blockchain and Mobile Networking -- 1.5 Open Architecture and Blockchains -- 1.6 Open API and Monetization of Mobile Network Infrastructure -- 1.6.1 Using Blockchain Technology to Tokenize API Access -- 1.6.2 Monetize Mobile Network Infrastructure -- 1.7 Resiliency of Current Blockchain Models -- 1.8 Next Evolution in Blockchain Functions -- 1.9 Book Objectives and Organization -- References -- Chapter 2 Enabling Technologies and Distributed Storage -- 2.1 Introduction -- 2.2 Data Storage -- 2.2.1 Distributed File Systems -- 2.2.2 Cloud Storage Systems -- 2.3 Blockchains -- 2.3.1 Building Elements of Blockchains -- 2.3.2 Mining in Blockchains -- 2.3.3 BlockchainBased Data Storage -- 2.3.4 Blockchain Types -- 2.4 Distributed Storage Systems -- 2.4.1 DSS Layers -- 2.4.2 Distributed Storage Challenges -- 2.4.2.1 Security -- 2.4.2.2 Reliability -- 2.4.2.3 Economic Incentives -- 2.4.2.4

Coordination -- 2.4.2.5 Monetization -- 2.4.3 DSS Implementations -- 2.4.4 DSS Use Cases -- 2.4.4.1 SCT dApps -- 2.4.4.2 SCT dApp Food Chain Example -- 2.4.5 Performance Evaluation of DSSs -- 2.5 The Future of DSS -- 2.6 Concluding Considerations -- Acronyms -- References -- Chapter 3 Managing Consensus in Distributed Transaction Systems -- 3.1 Ledgers and Consensus -- 3.1.1 Distributed Ledgers -- 3.1.2 Consensus -- 3.1.2.1 Consensus for Consistent Data Storage -- 3.1.2.2 Consensus for Transaction Ordering -- 3.1.2.3 Consensus as a Defense Against Bad Actors -- 3.1.3 Industrial Case Study -- 3.2 Consensus Protocols, Then and Now -- 3.2.1 State Machine Replication.
3.2.2 Byzantine Fault Tolerance -- 3.2.3 Nakamoto Consensus -- 3.2.4 Hybrid Consensus -- 3.3 Cryptographic Nakamoto Proofs -- 3.3.1 Proof of Work -- 3.3.2 Proof of Stake -- 3.3.2.1 ChainBased Proof of Stake -- 3.3.3 Proof of Capacity -- 3.3.4 Proof of Time -- 3.4 Challenges to Scalability -- 3.4.1 Communication Complexity -- 3.4.2 Asynchronous Context -- 3.4.3 Participant Churn -- 3.4.4 The Blockchain Scalability Problem -- 3.5 Block Size and Propagation -- 3.5.1 Larger Blocks -- 3.5.2 Shorter Rounds -- 3.6 Committees, Groups, and Sharding -- 3.6.1 Committees -- 3.6.2 Groups -- 3.6.3 Sharding -- 3.7 Transaction Channels -- 3.7.1 TrustWeighted Agreement -- 3.7.2 OffChain Transactions -- 3.7.3 Lightning Network -- 3.8 Checkpointing and Finality Gadgets -- 3.8.1 Probabilistic Finality -- 3.8.2 Checkpointing -- 3.8.3 Finality Gadgets -- 3.9 Bootstrapping -- 3.9.1 Networking -- 3.9.2 Data -- 3.10 Future Trends -- 3.10.1 Private Consensus -- 3.10.2 Improved Oracles -- 3.10.3 Streaming Consensus -- 3.11 Conclusion -- References -- Chapter 4 Security, Privacy, and Trust of Distributed Ledgers Technology -- 4.1 CAP Theorem and DLT -- 4.1.1 Distributed Database System (DDBS) -- 4.1.2 Evolution of DDBS to the Blockchain -- 4.1.3 Public vs Permissioned Blockchains -- 4.1.4 Evolution of Blockchain to the DLTs -- 4.2 CAP Theorem -- 4.2.1 CAP Theorem and Consensus Algorithms -- 4.2.2 Availability and Partition Tolerance (AP) Through PoW -- 4.2.3 Consistency and Partition Tolerance (CP) Through PBFT -- 4.2.4 Consistency and Availability (CA) -- 4.3 Security and Privacy of DLT -- 4.3.1 Security Differs by DLT -- 4.3.2 Security and Requirements for Transactions -- 4.3.3 Security Properties of DLT -- 4.3.4 Challenges and Trends in DLT Security -- 4.4 Security in DLT -- 4.4.1 Governance Scenario Security -- 4.4.2 DLT Application Security -- 4.4.3 DLT Data Security.
4.4.4 Transactions Security -- 4.4.5 DLT Infrastructure Security -- 4.5 Privacy Issues in DLT -- 4.6 Cyberattacks and Fraud -- 4.6.1 Challenges -- 4.6.2 Key Privacy and Security Techniques in DLT -- 4.7 DLT Implementation and Blockchain -- 4.7.1 Cryptocurrencies and Bitcoin -- 4.7.1.1 Origin of Blockchain -- 4.7.1.2 Bitcoin -- 4.7.1.3 Monero -- 4.7.2 Blockchain and Smart Contracts -- 4.7.3 Typical Blockchain Systems -- 4.7.3.1 Ethereum Classic (ETC) -- 4.7.3.2 Ethereum (ETH) -- 4.7.3.3 Extensibility of Blockchain and DLT -- 4.7.4 Origin of Blockchain 3.0 -- 4.7.5 Overview of Hyperledger Fabric -- 4.8 DLT of IOTA Tangle -- 4.9 Trilemma of Security, Scalability, and Decentralization -- 4.9.1 FirstGeneration Solutions: BTC/BCH -- 4.9.2 SecondGeneration Solutions: ETH/BSC -- 4.9.3 Threats in DLT and Blockchain Networks -- 4.10 Security Architecture in DLT and Blockchain -- 4.10.1 Threat Model in LDT -- 4.11 Research Trends and Challenges -- References -- Chapter 5 Blockchains for Business-Permissioned Blockchains# -- 5.1 Introduction -- 5.2 Major Architectures of Permissioned Blockchains -- 5.2.1 Order-Execute -- 5.2.2 Simulate-Order-Validate -- 5.2.2.1 Simulation Phase -- 5.2.2.2

Ordering Phase -- 5.2.2.3 Validation Phase -- 5.2.3 Comparison and Analysis -- 5.3 Improving Order-Execute Using Deterministic Concurrency Control -- 5.3.1 Calvin -- 5.3.2 BOHM -- 5.3.3 BCDB -- 5.3.3.1 Simulation Phase -- 5.3.3.2 Commit Phase -- 5.3.4 Aria -- 5.3.4.1 Simulation Phase -- 5.3.4.2 Analysis Phase -- 5.3.4.3 Commit Phase -- 5.3.5 Comparison and Analysis -- 5.4 Improving Execute-Order-Validate -- 5.4.1 Transaction Reordering -- 5.4.2 Early Abort -- 5.4.3 FastFabric -- 5.5 ScaleOut by Sharding -- 5.6 Trends of Development -- 5.6.1 Trusted Hardware -- 5.6.2 Chainify DBMSs -- Acronyms -- References.
Chapter 6 Attestation Infrastructures for Automotive Cybersecurity and Vehicular Applications of Blockchains -- 6.1 Introduction -- 6.2 Cybersecurity of Automotive and IoT Systems -- 6.2.1 Protecting Assets in Smart Cars -- 6.2.2 Reported Cases -- 6.2.3 Trusted Computing Base for Automotive Cybersecurity -- 6.2.4 Special Hardware for Security -- 6.2.5 Truthful Reporting: The Challenge of Attestations -- 6.3 The TCB and Development of Trusted Hardware -- 6.3.1 The Trusted Computing Base -- 6.3.2 The Trusted Platform Module (TPM) -- 6.3.3 ResourceConstrained Automotive Systems: Thin TPMs -- 6.3.4 Virtualized TPMs for ECUs -- 6.3.5 The DICE Model and CyberResilient Systems -- 6.4 Attestations in Automotive Systems -- 6.4.1 A Reference Framework for Attestations -- 6.4.2 Entities, Roles, and Actors -- 6.4.3 Variations in Evidence Collations and Deliveries -- 6.4.4 Composite Attestations for Automotive Systems -- 6.4.5 Appraisal Policies -- 6.5 Vehicle Wallets for Blockchain Applications -- 6.5.1 Vehicular Application Scenarios -- 6.5.2 Protection of Keys in Automotive Wallets -- 6.5.3 Types of Evidence from Wallets -- 6.6 Blockchain Technology for Future Attestation Infrastructures -- 6.6.1 Challenges in the SupplyChain of Endorsements -- 6.6.2 Decentralized Infrastructures -- 6.6.3 Example of Verifier Tasks -- 6.6.4 Notarization Records and Location Records -- 6.6.5 Desirable Properties of BlockchainBased Approaches -- 6.6.6 Information within the Notarization Record -- 6.6.7 Information in the Location Record -- 6.6.8 The Compliance Certifications Record -- 6.7 Areas for Innovation and Future Research -- 6.8 Conclusion -- Acknowledgments -- References -- Chapter 7 Blockchain for Mobile Networks -- 7.1 Introduction -- 7.2 NextGeneration Mobile Networks: Technology Enablers and Challenges -- 7.2.1 Mobile Networks: Technology Enablers.
7.2.1.1 SoftwareDefined Networking (SDN) -- 7.2.1.2 Network Function Virtualization (NFV) -- 7.2.1.3 Cloud Computing (CC) -- 7.2.1.4 Multiaccess Edge Computing (MEC) -- 7.2.1.5 5GNew Radio (5GNR) and Millimeter Wave (mmWave) -- 7.2.2 Mobile Networks: Technology Challenges -- 7.2.2.1 Scalability in Massive Communication Scenarios -- 7.2.2.2 Efficient Resource Sharing -- 7.2.2.3 Network Slicing and Multitenancy -- 7.2.2.4 Security -- 7.3 Blockchain Applicability to Mobile Networks and Services -- 7.3.1 Background and Definitions -- 7.3.2 Blockchain for Radio Access Networks -- 7.3.3 Blockchain for Core, Cloud, and Edge Computing -- 7.3.3.1 Data Provenance -- 7.3.3.2 Encrypted Data Indexing -- 7.3.3.3 Mobile Network Orchestration -- 7.3.3.4 Mobile Task Offloading -- 7.3.3.5 Service Automation -- 7.4 Blockchain for Network Slicing -- 7.4.1 The Network Slice Broker (NSB) -- 7.4.2 NSB Blockchain Architecture (NSBchain) -- 7.4.2.1 Technical Challenges -- 7.4.3 NSBchain Modeling -- 7.4.3.1 System Setup -- 7.4.3.2 Message Exchange -- 7.4.3.3 Billing Management -- 7.4.4 NSBchain Evaluation -- 7.4.4.1 Experimental Setup -- 7.4.4.2 FullScale Evaluation -- 7.4.4.3 Brokering Scenario Evaluation -- 7.5 Concluding Remarks and Future

Work -- Acronyms -- References -- Chapter 8 Blockchains for Cybersecurity and AI Systems -- 8.1 Introduction -- 8.2 Securing Blockchains and Traditional IT Architectures -- 8.2.1 On Securing a Blockchain Platform -- 8.3 Public Blockchains Cybersecurity -- 8.3.1 Vulnerabilities Categorization -- 8.3.1.1 Technical Limitations, Legal Liabilities, and Connected 3rdParty Applications -- 8.3.1.2 Cybersecurity Issues -- 8.3.1.3 Public Blockchain 1.0: PoW and PoS -- 8.3.1.4 Public Blockchain 1.0: DPoS -- 8.3.1.5 Public Blockchain 2.0: Ethereum Smart Contracts -- 8.3.1.6 Public Blockchain 2.0-Privacy Issues.
8.4 Private Blockchains Cybersecurity.

Sommario/riassunto

This book, 'Blockchains: Empowering Technologies and Industrial Applications,' explores various aspects of blockchain technology and its applications across multiple industries. Edited by Anwer Al-Dulaimi, Octavia A. Dobre, and Chih-Lin I, the book delves into the technical foundations of blockchains, including distributed storage, consensus mechanisms, security, privacy, and trust in distributed ledger technology. It also examines specific applications such as permissioned blockchains for business, automotive cybersecurity, blockchain integration in mobile networks, and smart healthcare systems. The work aims to provide a comprehensive understanding of blockchain as a transformative technology and is intended for professionals and researchers in the fields of telecommunications, computer science, and engineering.