1. Record Nr. UNINA9910842493003321

Autore	Ruj Sushmita
Titolo	Blockchains [[electronic resource]] : A Handbook on Fundamentals, Platforms and Applications / / edited by Sushmita Ruj, Salil S. Kanhere, Mauro Conti
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2024
ISBN	3-031-32146-4
Edizione	[1st ed. 2024.]
Descrizione fisica	1 online resource (621 pages)
Collana	Advances in Information Security, , 2512-2193 ; ; 105
Altri autori (Persone)	KanhereSalil S ContiMauro
Disciplina	005.74
Soggetti	Cryptography Data encryption (Computer science) Data protection - Law and legislation Data protection Computer networks - Security measures Cryptology Privacy Security Services Mobile and Network Security Data and Information Security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Ten Myths About Blockchain Consensus -- Cryptographic Primitives in Blockchain -- Bitcoin Blockchain System: An Overview of Security and Privacy Aspects -- The Ethereum Blockchain: Implementation and Security Aspects -- The Future Ring Confidential Transaction Protocols for Privacy-Preserving Blockchain -- Algorand Blockchain -- Tendermint -- The Security of Delegated Proof of Stake Wallet and Stake Pools -- Layer-2 Scalability Solutions for Blockchains -- Illicit Blockchain Content – Its Different Shapes, Consequences, and Remedies -- Blockchain-based Distributed and Secure Digital Forensic Investigation Systems -- Supply Chain Management Using Blockchain -- Blockchain Technology for E-Governance Applications -- When

Blockchain meets Smart Cities: Opportunities, Security and Future Research -- Decentralised Identity Management and Blockchains: Design Patterns and Architectures -- From Centralized to Decentralized Remote Electronic Voting -- Blockchain Technology Accelerating Industry 4.0 -- Blockchain for Health Data Management -- Supporting Secure Trusted Manufacturing via Blockchain -- Blockchain for Data Sharing.

Sommario/riassunto

This handbook is a selection of foundational aspects, security analysis, platforms, and applications of blockchains that consists of four parts. The first part introduces the basic building blocks such as distributed computing and cryptography. Consensus algorithms that form the basic backbone of blockchain protocols are presented. Various cryptographic tools like hash functions, digital signatures and commitment schemes are also introduced. Advanced cryptographic techniques such as zero knowledge protocols, secret sharing, verifiable random functions that are used for privacy-preserving and secure design are discussed. The second part of this handbook consists of popular blockchain designs and platforms. Architecture of Bitcoin, Ethereum, Monero, Tendermint and Algorand have been presented. Various important issues like scalability and security are discussed in the third part. Security design challenges, security vulnerabilities and their analysis are discussed. The final part of this handbook discusses various applications of blockchains. These include supply-chain, identity and credential management, Internet of Things (IoT), data-sharing, e-voting, e-governance, e-health, smart cities, and Industry 4.0. Research challenges and directions of future work are included in this handbook. This comprehensive reference targets students and researchers, who are starting to explore blockchain. Professionals working in blockchain security and applications will find this handbook to be a valuable reference.