1. Record Nr. UNISA996546822203316

Titolo	Principles and practice of blockchains / / edited by Kevin Daimi, Ioanna Dionysiou, and Nour El Madhoun
Pubbl/distr/stampa	Cham, Switzerland : , : Springer, , [2023] ©2023
ISBN	3-031-10507-9
Descrizione fisica	1 online resource (398 pages)
Disciplina	005.74
Soggetti	Blockchains (Databases)
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Intro -- Preface -- Acknowledgments -- Contents -- About the Editors -- Part I Blockchain Fundamentals -- Fundamentals of Blockchain Technology -- 1 Introduction -- 2 Blockchain Features and Architecture -- 2.1 Proof of Work (PoW) -- 2.2 Proof of Stake (PoS) -- 2.3 Proof of Burn (PoB) -- 2.4 Proof of Capacity (PoC) -- 2.5 Proof of Elapsed Time (PoET) -- 3 Smart Contracts -- 4 Security Features -- 4.1 Security on Infrastructure -- 4.1.1 Decentralisation -- 4.1.2 Transparency -- 4.1.3 Immutability -- 4.1.4 Consistency -- 4.2 Security on Transactions -- 5 Applications -- 5.1 Electronic Voting -- 5.2 Healthcare Services -- 5.3 Identity Management -- 5.4 Access Control -- 5.5 Decentralised Notaries -- 5.6 Supply Chain Management -- 6 Conclusion and Future Works -- References -- Identification of Illicit Blockchain Transactions Using Hyperparameters Auto-tuning -- 1 Introduction -- 2 Related Work -- 3 Experimental Dataset -- 4 Experimental Setup and Evaluation -- 4.1 Offline Learning -- 4.2 Online Learning -- 4.3 PCA Analysis -- 5 Conclusions -- References -- Multidimensional Blockchain: Construction and Security Analysis -- 1 Introduction -- 2 Robust Distributed Ledgers -- 3 Multidimensional Blockchain -- 4 Multidimensional Blockchain Security Analysis -- 4.1 Security Analysis of Underlying Robust Distributed Ledgers -- 4.2 Intersystem Exchange Security Analysis -- 4.3 Scaling Security Analysis -- 5 Search and Verification Protocol -- 6 Theoretical and Experimental Analysis -- 7 Conclusion -- References -- Blockchain Project Workflow

Execution for Trustless Operation -- 1 Introduction -- 2 Literature Review -- 2.1 Blockchain and Workflow Operations -- 2.2 Salient Features of Blockchain -- 2.3 Blockchain Structure -- 2.4 Project Workflow Trustless Operation -- 2.5 Smart Contract and Workflow Project Dynamics.
2.6 Structure of the Smart Contract in Workflow -- 2.7 Smart Contracts and Traditional Contracts -- 2.8 Smart Contract Applications -- 2.9 Advantages of Smart Contracts -- 2.10 Information and Sharing in Inter-organizational Workflows -- 2.11 Blockchain-Smart Contract Workflow Solutions -- 2.12 Project Workflow Execution Layers -- 3 Proposed Methodology -- 4 Results and Discussions -- 4.1 Smart Contracts: Ethereum Platform -- 4.2 Concept of Cryptocurrency -- 4.3 Decentralized Applications (DApps) -- 5 Survey Research on Blockchain Applications -- 5.1 Smart Contract and Blockchain in Food Tracing -- 5.2 Blockchain in Food Traceability: A Systematic Literature Review -- 5.3 Blockchain Technology in Supply Chain -- 5.4 Towards Automated Migration for Blockchain-Based Decentralized Application -- 5.5 Ensure Traceability in European Food Supply Chain by Using a Blockchain System -- 5.6 A Proof-of-Concept of Farmer-to-Consumer Food Traceability on Blockchain for Local Communities -- 5.7 Blockchain and IoT-Based Food Traceability for Smart Agriculture -- 5.8 A Trustworthy Food Resume Traceability System Based on Blockchain Technology -- 5.9 Smart Contract and Blockchain in Food Tracing -- 5.10 Blockchain Technologies and Their Applications in Data Science and Cyber Security -- 5.11 Towards Automated Migration for Blockchain-Based Decentralized Application -- 5.12 Rebuilding Food Supply Chain with the Introduction of Decentralized Credit Mechanism -- 6 Conclusion -- References -- Part II Blockchains in Internet of Things and Mobile Phones -- Protecting Location Privacy in Blockchain-Based Mobile Internet of Things -- 1 Introduction -- 2 Related Work -- 3 System Overview and Design Goals -- 3.1 Blockchain System Model -- 3.2 Malicious Entities -- 3.3 Attacker's Goal and Strategies -- 3.4 Problem Formulation and Design Goals -- 4 The BlockPriv Approach.
5 Scheme Analysis -- 5.1 Privacy Analysis -- 5.1.1 Privacy Bound -- 5.1.2 Obfuscating Paths -- 5.2 Utility Analysis -- 5.2.1 Loss of Utility Bound -- 5.3 Security Analysis -- 5.3.1 Collusion Attack -- 5.3.2 Map Matching Attack -- 5.3.3 Time Reachability-Based Path Reconstruction Attack -- 5.3.4 Transaction Dropping Attack -- 5.3.5 Security Limitations -- 6 Experimental Evaluation -- 6.1 Experimental Settings -- 6.1.1 Dataset Description -- 6.1.2 Simulation Setup -- 6.2 Experiment Results -- 6.2.1 Utility Versus Privacy Level -- 6.2.2 Utility Versus Number of Sensitive Location Types -- 6.2.3 User-Level Correlation Analysis -- 7 Conclusion and Future Direction -- References -- A Blockchain-Based Machine Learning Intrusion Detection System for Internet of Things -- 1 Introduction -- 2 IoT Security Attacks and Their Solutions -- 3 Blockchain of Things (Blockchain with IoT) -- 3.1 Advantages of Blockchain of Things -- 3.2 Disadvantages of Blockchain of Things -- 3.3 Some Related Work of Blockchain of Things -- 4 ML and DL Algorithms in IoT Security -- 5 Combining Technologies (Blockchain, IoT, and ML/DL) for IoT Security -- 5.1 Brief Summary of Our Problem Statement -- 5.2 Our Proposed Approach -- 6 Experimentation and Results -- 7 Conclusions and Future Directions -- References -- ECOM: Epoch Randomness-Based Consensus Committee Configuration for IoT Blockchains -- 1 Introduction -- 2 An Overview of Scaling Blockchain Solutions -- 2.1 Off-Chain Blockchain Solutions -- 2.2 On-Chain Blockchain -- 3 Epoch Randomness and Configuration -- 3.1 Verifiable Random Function (VRF) -- 3.2 Verifiable Secret Sharing (VSS) -- 3.3 Publicly Verifiable

Secret Sharing (PVSS) -- 4 Network Traffic Model in Blockchain -- 4.1 Unstructured P2P Network Model -- 4.2 Structured P2P Network Model -- 5 ECOM: An Epoch Randomness-Based Committee Configuration for IoT Blockchains.
5.1 ECOM System Design -- 5.2 Prototype Implementation -- 5.3 Performance Evaluation -- 5.4 Security Analysis -- 6 Conclusions -- References -- Customer Outcome Framework for Blockchain-Based Mobile Phone Applications -- 1 Introduction -- 2 Literature Review -- 2.1 Singapore's Electronic Payment Journey -- 2.2 Blockchain and AI Combination in the Metaverse -- 2.3 Mobile Payment Applications -- 2.4 Personalized Recommendation Systems -- 2.5 Shopping Motivation Using BMPAs -- 2.6 Means-End Chain Theory -- 2.7 Social Identity Theory -- 2.8 Prospect Theory -- 2.9 Utilitarian Value, Hedonic Value, and BMPA Identification -- 2.10 BMPA Trustworthiness, BMPA Identification, and Repeat Customers' BMPA Usage -- 2.11 Perceived Risk -- 2.12 Control Variables and the Research Model -- 3 Discussions -- 3.1 Theoretical Implications -- 3.2 Practical Implications -- 3.3 Limitation -- 4 Conclusions and Future Research -- References -- Part III Blockchains and Healthcare -- A Secure Decentralized Privacy-Preserving Healthcare System Using Blockchain -- 1 Introduction -- 2 Overview and Related Work -- 2.1 Consensus Protocols -- 2.1.1 Proof-of-Work (PoW) -- 2.1.2 Proof-of-Stake (PoS) -- 2.1.3 Delegated Proof-of-Stake (DPoS) -- 2.1.4 Proof-of-Authority (PoA) -- 2.1.5 Access Control Mechanism with Smart Contract for Data Sharing -- 2.2 Smart Contract -- 3 Methodology -- 3.1 System Design -- 3.2 Content Extraction Signature -- 3.2.1 Key Generation GK(k) -- 3.2.2 Signature Generation Algorithm Sig (SK, M, CEAS) -- 3.2.3 Signature Extraction Algorithm Ext(pk,M,F,X) -- 3.2.4 Signature Verification Algorithm Ver(pk,M,E) -- 4 Implementation -- 4.1 Front End -- 4.2 EHR Manager -- 4.3 Ethereum Proof-of-Authority -- 4.4 Storing EHR -- 4.5 Sharing of EHR -- 5 Evaluation -- 5.1 Security Assessment -- 5.1.1 Privacy and Sharing -- 5.1.2 Storage Management -- 5.1.3 Data Audit.
6 Conclusion -- References -- An Investigation of Blockchain Technology and Smart Contracts Deployment in Smart Medicine 4.0 -- 1 Introduction -- 1.1 Smart Life -- 1.2 Smart Contracts -- 2 Current Blockchain Technology and Smart Contracts Issues and Challenges -- 2.1 Blockchain and Smart Contracts in a Nutshell -- 2.2 Advantages in Comparison with Non-blockchain Systems -- 2.2.1 Generic Blockchain Advantages -- 2.2.2 Blockchain Advantages for Healthcare Industry -- 2.2.3 Blockchain and Smart Contracts Challenges -- 2.2.4 Security of IoT and IoHT Critical Infrastructure: Blockchain as a Solution -- 2.2.5 Summary -- 2.3 Legislation and Legislative Initiatives Related to Blockchain and Smart Contracts in Different Jurisdictions -- 2.3.1 General Legal Regulation Provisions of Blockchain and Smart Contracts -- 2.3.2 Health Insurance Portability and Accountability Act of 1996 (HIPAA) -- 2.3.3 General Data Protection Regulation (GDPR) -- 2.3.4 Smart Medicine as a Target: The European Union Agency for Cybersecurity (ENISA) Recommendations -- 3 Internet of Health Things Blockchain and Smart Contracts -- 3.1 Attacks on the Healthcare Sector: Defense on the Base of the Blockchain -- 3.2 IoT-Blockchain-Based Monitoring Model and Smart Contract as a Verification Link for Smart Healthcare Purposes -- 3.3 Successful Implementation of the Blockchain and Smart Contracts for Secure HER Sharing in E-Healthcare -- 3.4 Health Records Authorization Process with the Implementation of the Permissioned Blockchain and Smart Contracts: ABAC as an Important Tool for Smart Healthcare -- 3.5 Extended Usage of the Smart Contracts: Functionalities of Smart Contracts -- 3.6 GDPR

Insight: Combination of GDPR and Blockchain -- 3.7 Healthcare Data-Trading Market Based on Blockchain -- 3.8 Blockchain-Based Healthcare Monitoring Architecture.
3.9 IoT-Blockchain Ecosystem: Combination of Blockchain and Swarm Exchange Techniques.