1. Record Nr. UNISA996503565903316

Titolo	Blockchain and trustworthy systems : 4th International Conference, BlockSys 2022, Chengdu, China, August 4-5, 2022, revised selected papers / / edited by Davor Svetinovic [and four others]
Pubbl/distr/stampa	Singapore : , : Springer, , [2023] ©2023
ISBN	981-19-8043-8
Descrizione fisica	1 online resource (386 pages)
Collana	Communications in Computer and Information Science ; ; v.1679
Disciplina	016.403
Soggetti	Artificial intelligence
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	Intro -- Preface -- Organization -- Contents -- Trustworthy Systems -- Secure and Efficient Agreement Signing Atop Blockchain and Decentralized Identity -- 1 Introduction -- 2 Background -- 3 System and Security Models -- 3.1 System Model -- 3.2 Security Model -- 4 System Design -- 4.1 Identity System -- 4.2 Agreement Signing System -- 4.3 Security Sketch -- 5 Experiments -- 6 Conclusion -- References -- A Privacy-Preserving Credit Bank Supervision Framework Based on Redactable Blockchain -- 1 Introduction -- 1.1 Related Works -- 1.2 Our Contributions -- 1.3 Paper Organization -- 2 Preliminaries -- 2.1 Chameleon Hash -- 2.2 Smart Contract -- 2.3 Threshold Signature -- 2.4 Bilinear Mapping -- 3 System Model and Requirements -- 3.1 System Model -- 3.2 Security Requirements -- 4 PCR Construction -- 4.1 Initialization Phase -- 4.2 Storage Phase -- 4.3 Delete Phase -- 5 Security Analysis -- 6 Evaluation -- 7 Conclusion -- References -- A Trusted Storage System for Digital Object in the Human-Cyber-Physical Environment -- 1 Introduction -- 2 Related Work -- 2.1 Digital Object Architecture's Application -- 2.2 Trusted Storage Technology Based on Blockchain -- 3 Trusted Storage System -- 3.1 System Description -- 3.2 Block Generation -- 3.3 Block Consensus -- 4 Experiment and Analysis -- 4.1 The Experiment Setting -- 4.2 The Performance in the Block Generation Stage -- 4.3 The Performance in the Block Consensus Stage -- 4.4 The Performance of the Trusted

Storage System -- 5 Conclusion -- References -- The Role of Absorptive Capacity in the Blockchain Enabled Traceability Alignment: An Empirical Investigation -- 1 Introduction -- 2 Literature Review -- 3 Research Setting and Method -- 4 Data Interpretation -- 5 Discussion and Implications -- 6 Conclusion and Limitation -- References -- DataAttest: A Framework to Attest Off-Chain Data Authenticity.
1 Introduction -- 2 Motivating Example and Goals -- 3 DataAttest Design -- 3.1 DAP Construction and Verification -- 3.2 Attestation Optimization -- 4 Case Study -- 4.1 Experimental Setup -- 4.2 Effectiveness Evaluation -- 4.3 Performance Evaluation -- 5 Discussion -- 6 Related Work -- 6.1 Blockchain Oracle -- 6.2 Control-Flow Attestation -- 7 Conclusion -- References -- Blockchain-Based Healthcare and Medicine Data Sharing and Service System -- 1 Introduction -- 2 Related Work -- 3 HMChain Architecture -- 4 Data Extraction and Storage Layer -- 4.1 Data Extraction -- 4.2 Data Storage -- 5 Data Management Layer -- 5.1 Peer-to-Peer Network -- 5.2 Consensus Mechanism -- 5.3 Smart Contract -- 6 Data Application Layer -- 6.1 Clinical Research and Development -- 6.2 Medicine Traceability -- 7 Conclusions -- References -- BCSChain: Blockchain-Based Ceramic Supply Chain -- 1 Introduction -- 2 Background -- 2.1 Conventional Ceramic Supply Chains -- 2.2 Blockchain -- 2.3 Related Works -- 3 BCSChain: Blockchain-Based Ceramic Supply Chain -- 3.1 System Architecture of BCSChain -- 3.2 Advantages of BCSChain -- 4 Application Scenarios of BCSChain -- 4.1 Application in Logistics Traceability Management -- 4.2 Application in Supply Chains Finance -- 4.3 Application in Automatic Trading -- 5 Conclusion -- References -- Blockchain -- A Highly Scalable Blockchain-Enabled DNS Architecture -- 1 Background -- 1.1 Challenges -- 1.2 Related Work -- 1.3 Contribution -- 2 Architecture and Procedures -- 2.1 Design Principles -- 2.2 Architecture Overview -- 2.3 Procedures -- 2.4 Data Structure -- 3 Scalabiity -- 3.1 Limitless Capacity -- 3.2 Overload -- 3.3 Lookup Latency -- 3.4 On-Demand Spanning -- 3.5 Reasonable Lookup Latency -- 4 Security -- 4.1 Intra-node Security -- 4.2 Inter-node Security -- 5 Assessment -- 5.1 Lookup-Latency (LO) and Branch Number (k).
5.2 Amount of De-centralized Services (TN) and TREE'S Depth (D) -- 5.3 Round-Trip Time (RTT) -- 5.4 Total Latency (LA) -- 6 Discussion -- 6.1 Merits -- 6.2 Further Discussion -- 6.3 Future Work -- 7 Conclusion -- References -- Traceable Ring Signature Schemes Based on SM2 Digital Signature Algorithm and Its Applications in the Evidence-Storage System -- 1 Introduction -- 1.1 Application Case -- 1.2 Our Contributions -- 1.3 Layout -- 2 Preliminaries -- 2.1 Notions -- 2.2 SM2 Signature Algorithm -- 3 The Proposed SM2 Traceable Ring Signature -- 3.1 Definition -- 3.2 Constructions -- 3.3 Discussion -- 4 Evaluation and Analysis -- 4.1 Communication Cost -- 4.2 Computation Cost -- 5 STRS-Based Blockchain Evidence-Storage System -- 5.1 System Model -- 5.2 Our Protocol -- 6 Security Analysis -- 7 Conclusion -- References -- Blockchain-Enabled Techniques for Energy Internet of Things: A Review -- 1 Introduction -- 2 Blockchain-Enabled Key Techniques in EIoT -- 2.1 Smart Contracts to Achieve EIoT Access Control -- 2.2 Consensus Protocol in EIoT Network -- 2.3 Cross-Chain Communication in Distributed Energy Transactions -- 3 Performance Evaluation Methods of Blockchain-Based EIoT -- 4 Challenges and Future Research Opportunities -- 5 Conclusion -- References -- Blockchain-Based Social Network Access Control Mechanism -- 1 Introduction -- 2 Preliminaries -- 2.1 Blockchain and Smart Contract -- 2.2 Role-Based Access Control -- 3 General

Process and Design Model of Blockchain-Based Social Network Access Control Mechanism -- 3.1 Procedure of Blockchain-Based Social Network Access Control -- 3.2 Design Model of Social Network Access Control Based on Blockchain -- 4 Specific Scheme of Blockchain-Based Social Network Access Control Mechanism -- 4.1 User and Role -- 4.2 Upload Data -- 4.3 The Public Role of Feature Extraction -- 4.4 Role Application.
5 Realization of Social Network Access Control Based on Smart Contracts -- 5.1 Contract Description -- 5.2 Access Control Algorithm -- 6 Verification of Social Network Access Control Mechanism Scheme Based on Blockchain -- 6.1 Experimental Environment -- 6.2 Experimental Details -- 6.3 Interpretation of Result -- 7 Conclusion -- References -- Latency Analysis for Raft Consensus on Hyperledger Fabric -- 1 Introduction -- 2 Related Work -- 3 Theoretical Modeling -- 3.1 A Transaction Block Size Modeling -- 3.2 Raft Consensus Latency Modeling -- 4 Experiments and Analysis -- 5 Conclusion -- References -- A Survey of Blockchain-Based Stablecoin: Cryptocurrencies and Central Bank Digital Currencies -- 1 Introduction -- 2 Background -- 2.1 Blockchain Technology -- 2.2 Blockchain-Based Stablecoins -- 3 Project Review on Blockchain-Based Stablecoins -- 3.1 Wholesale CBDC Stablecoins -- 3.2 Retail CBDC Stablecoins -- 3.3 Fiat Asset-Backed Stablecoins -- 3.4 Crypto Asset-Backed Stablecoins -- 3.5 Algorithmic Stablecoins -- 4 Regulation Towards Blockchain-Based Stablecoins -- 4.1 Regulation Towards Stablecoins in CBDC -- 4.2 Regulation Towards Cryptocurrencies Stablecoins -- 5 Discussions -- 5.1 Regulation Issues -- 5.2 Technology Issues -- 5.3 Stability Issues -- 6 Conclusion -- References -- Collusion Attack Analysis and Detection of DPoS Consensus Mechanism -- 1 Introduction -- 2 Related Work -- 3 Preliminaries -- 3.1 DPoS: Delegated Proof of Stake -- 3.2 Weighted Voting Games -- 3.3 Collusion Attack -- 4 Model and Definitions -- 4.1 Coalitional Games in DPoS -- 4.2 SSI: Shapley-Shubik Power Index -- 4.3 PBI: Banzhaf Power Index or Penrose Index -- 4.4 The Weighted Voting Game in DPoS -- 5 Experiment and Analysis -- 5.1 Analysis of Collusion Attack in DPoS -- 5.2 Detection of Collusion Attack in DPoS -- 6 Conclusion -- References.
Decentralized Blockchain Transaction Scheme Based on Digital Commitment -- 1 Introduction -- 2 Preliminaries -- 2.1 Digital Commitment -- 2.2 Homomorphic Encryption -- 2.3 Multi-key Fully Homomorphic Encryption -- 2.4 Zero-Knowledge Proof -- 3 Blockchain Transaction Scheme Based on Digital Commitment -- 3.1 Transaction Scene -- 3.2 Scheme Design -- 4 Scheme Analysis -- 4.1 Positive Analysis -- 4.2 Security Analysis -- 4.3 Performance Analysis -- 5 Conclusion -- References -- Private Computing -- Research on Abnormal Transaction Detection Method for Blockchain -- 1 Introduction -- 2 Related Work -- 3 Model -- 3.1 System Model -- 3.2 Building Transaction Topology -- 4 Blockchain Anomaly Detection Based on GNN-FiLM -- 5 Experiment -- 5.1 Method Comparison -- 5.2 Feature Preprocessing and Sample Equalization -- 6 Conclusion -- References -- Cross Cryptocurrency Relationship Mining for Bitcoin Price Prediction -- 1 Introduction -- 2 Related Work -- 2.1 External Factors -- 2.2 Machine Learning Methods -- 2.3 Graph Analytics -- 3 Methodology -- 3.1 Data Preprocessing -- 3.2 Lead-Lag Variance Kernel -- 3.3 Deep Learning Models -- 4 Experiments -- 4.1 Dataset -- 4.2 Baselines -- 4.3 Evaluation Metric -- 4.4 Results and Analysis -- 5 Conclusion -- References -- Blockchain-Based UAV-Assisted Forest Supervision and Data Sharing -- 1 Introduction -- 1.1 Related Works -- 1.2 Our Contributions -- 2 Preliminaries -- 2.1 Blockchain -- 2.2

Smart Contract -- 2.3 Interplanetary File System -- 2.4 Physical Unclonable Functions -- 3 System Model and Security Requirements -- 3.1 System Model -- 3.2 Security Requirements -- 4 BSR Construction -- 4.1 System Initialization -- 4.2 Forest Information Initialization -- 4.3 Data Collection -- 4.4 Data Processing -- 5 Security Analysis -- 6 Performance Analysis -- 7 Conclusion -- References.
Suspicious Customer Detection on the Blockchain Network for Cryptocurrency Exchanges.