1. Record Nr. UNINA9910629292103321

Titolo	Handbook on blockchain / / Duc A. Tran, My T. Thai, Bhaskar Krishnamachari, editors
Pubbl/distr/stampa	Cham, Switzerland : , : Springer, , [2022] ©2022
ISBN	3-031-07535-8
Descrizione fisica	1 online resource (707 pages)
Collana	Springer optimization and its applications ; ; 194
Disciplina	005.74
Soggetti	Blockchains (Databases) Digital currency Cadena de blocs (Bases de dades) Llibres electrònics
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references.
Nota di contenuto	Intro -- Preface -- Contents -- Foundation -- Blockchain in a Nutshell -- 1 Introduction -- 2 What is Blockchain -- 2.1 The Blockchain Computer -- 2.2 The Blockchain State -- 2.3 The Chain Structure -- 2.4 Use of Cryptography -- 2.5 Where is Blockchain Stored -- 2.6 How to Process a Transaction -- 2.7 How to Achieve Consensus -- 3 The Bitcoin Network -- 3.1 Addresses -- 3.2 Elliptic Curve Cryptography -- 3.3 Transactions -- 3.4 Blocks -- 3.5 Mining Difficulty -- 3.6 Mining (Un)Fairness -- 3.7 Block Finality -- 4 Smart-Contract Blockchains -- 4.1 Smart Contract -- 4.2 Token Creation -- 4.3 Transaction Processing -- 4.4 Block Validation -- 4.5 Contract Interoperability -- 5 Blockchain Scalability -- 5.1 The Blockchain Trilemma -- 5.2 Layer-2 Scalability -- 6 Blockchain Interoperability -- 6.1 Atomic Swap -- 6.2 Chain Bridge -- 6.3 Chain Hub -- 7 Conclusions -- References -- Blockchain Peer-to-Peer Network: Performance and Security -- 1 Introduction -- 1.1 Related Work -- 2 Overview -- 3 Network Topology -- 3.1 Bitcoin P2P Network -- 3.2 Ethereum's P2P Network -- 3.3 Data Forwarding -- 4 Attacks on Blockchain P2P Networks -- 4.1 Eclipse Attacks -- 4.2 Network Partitioning Attacks -- 4.3 DDoS Attacks -- 4.4 Man-in-the-Middle Attacks -- 4.5 Deanonymization Attacks -- 5

Performance -- 5.1 Throughput -- 5.2 Latency -- 6 Performance Improvement as an Optimization Problem -- 6.1 Optimization Problem -- 6.2 Throughput-Optimal Propagation Scheme for Single-Source Problem -- 6.3 Throughput-Optimal Propagation Scheme for Blockchain Data Forwarding Problem -- 7 Conclusion -- References -- Consensus Algorithms for Blockchain -- 1 Introduction -- 2 Evaluation Criteria -- 2.1 Related Works -- 2.2 Evaluation Framework -- 3 Consensus Algorithms -- 3.1 Proof-Based Consensus Algorithms -- 3.2 Proof of Work (PoW) -- 3.3 Proof of Stake (PoS).
3.4 Vote-Based Consensus Algorithms -- 4 Evaluation -- 5 Conclusion -- References -- Blockchain Incentive Design and Analysis -- 1 Introduction -- 2 Incentive Design and Analysis in Bitcoin -- 2.1 Overview of Bitcoin -- 2.2 Selfish Mining in Bitcoin -- 2.3 Theoretical Results on Selfish Mining in Bitcoin -- 3 Incentive Design and Analysis in Ethereum -- 3.1 Overview of Ethereum -- 3.2 Reward Design and Its Impact on Selfish Mining -- 3.3 Theoretical Results on Selfish Mining in Ethereum -- 4 Incentive Design and Analysis in Bitcoin-NG -- 4.1 Overview of Bitcoin-NG -- 4.2 Microblocks and Its Incentive-Based Attacks -- 4.3 Theoretical Results on Microblocks Mining -- 4.4 Theoretical Results on Microblocks and Key-Block Mining in Bitcoin-NG -- 5 Further Reading -- 6 Conclusion -- References -- Cross-Blockchain Transactions: Systems, Protocols, and Topological Theory -- 1 Introduction -- 2 Internet-of-Blockchains Systems -- 2.1 Background -- 2.2 Architecture -- 2.3 Consensus Protocol -- 2.4 Communication Model -- 2.5 Programming Interface -- 2.6 Limitation -- 3 Protocols of Chain-to-Chain Federation -- 3.1 C2C Blockchain Transactions Through Time Locks -- 3.2 CBT Protocols Through Two-Phase Commits -- 3.3 Atomicity of Forked Blockchains: A Taxonomy of Protocols -- 3.4 Limitation -- 4 A Topological Theory of Cross-Blockchain Transactions -- 4.1 Topological Preliminaries -- 4.2 Assumptions and Notations -- 4.3 Topological Space of No-Fork Blockchains -- 4.4 Topological Space of Static-Fork Complexes -- 4.5 Topological Space of Growing Fork Blockchains -- 4.6 Analyzing Blockchains Through Algebraic Topology -- 5 Bibliographic Notes -- References -- Scalability -- Scaling Blockchains and the Case for Ethereum -- 1 Introduction to the Scaling Problem -- 1.1 Considerations -- 1.2 Naive Scaling Solutions -- 1.3 Types of Scaling Solutions.
2 Layer-1 Scaling Solutions -- 2.1 Sharding -- 2.2 Ethereum 2.0 -- 3 Layer-2 Scaling Solutions -- 3.1 Side Chains -- 3.2 Rollups -- 4 Conclusion -- References -- Building Protocols for Scalable Decentralized Applications -- 1 Introduction -- 2 Decentralized Ledger Abstraction -- 2.1 Consistency -- 2.2 Immutability -- 2.3 Auditability -- 3 Decentralized Ledger Technologies -- 3.1 Assumptions and Attack Model -- 3.2 Data and Transaction Models -- 3.3 Smart Contracts -- 3.4 Committee-Based Consensus -- 3.5 Sybil Detection -- 3.6 Nakamoto Consensus -- 3.7 Bottlenecks -- 4 Improved and Novel Consensus Mechanisms -- 4.1 Improved Committee-Based Consensus Protocols -- 4.2 Minor Changes to Nakamoto Consensus -- 4.3 Decoupling Mining from Transaction Serialization -- 4.4 Novel Proof-of-Stake Protocols -- 4.5 Summary -- 5 Sharding Blockchains -- 5.1 Challenges in Sharding Blockchains -- 5.2 Foundations -- 5.3 Public Blockchain Sharding Protocols -- 5.4 Summary -- 6 Layer-2 Solutions -- 6.1 Building Blocks -- 6.2 Payment Channels -- 6.3 State Channels -- 6.4 Watchtowers -- 6.5 Subchains -- 6.6 Optimistic Rollups -- 6.7 Summary -- 7 Federated Chains -- 7.1 Cross-Chain Swaps -- 7.2 Polkadot -- 7.3 Avalanche Subnetworks and Cosmos Zones -- 7.4 Summary -- 8 Conclusion -- References -- Information-Theoretic

Approaches to Blockchain Scalability -- 1 Introduction -- 2 Blockchain System Primer -- 2.1 The Blockchain Network -- 2.2 Ledger Construction -- 2.3 Costs of Maintaining Blockchain Ledger -- 3 The Storage Problem with Blockchain Systems -- 4 Dynamic Distributed Storage-On Blockchain Storage Cost Reduction -- 4.1 Problem Description -- 4.2 Coding Data Block -- 4.3 Recovery Scheme -- 4.4 Feasible Encryption Scheme -- 4.5 Dynamic Zone Allocation -- 4.6 Security Enhancement -- 5 Application-Based Scalable Blockchain Methods -- 5.1 Problem Statement.
5.2 Computation Model -- 5.3 Validation Protocol -- 5.4 Client Operations -- 5.5 Endorser and Orderer Operations -- 5.6 Parameter Agnostic Design -- 5.7 Computations with External Randomness -- 5.8 Iterative Experiments with MNIST Training -- 5.9 Extensions of Distributed Trust Protocol -- 6 Future Work -- 7 Conclusion -- References -- Trust and Security -- On Trust, Blockchain, and Reputation Systems -- 1 Introduction -- 2 Definitions and Fundamentals -- 2.1 Definitions of Trust -- 2.2 Blockchains as a Trust Enabler Platform -- 2.3 Taxonomy of Reputation -- 2.4 Discussion of Trust and Reputation in Blockchains and Distributed Ledgers -- 3 Tools and Methods for Blockchain Reputation Tracking -- 3.1 Reputation Tokens -- 3.2 Event Reputation Factors -- 3.3 Reputation Thresholds -- 3.4 Multi Signature Transaction (Multi-Sig) -- 3.5 Optimistic Fair Exchange -- 3.6 Anonymous Feedback -- 3.7 Insurance Models -- 3.8 Reputation Engines -- 3.9 Reaction and Service Differentiation -- 3.10 Graph and Flow Engines -- 4 Case Study of Blockchain-Based Reputation in a Cooperative Defense -- 4.1 Analysis of Reputation Properties -- 4.2 Analysis of Reputation Threats -- 5 Chapter Considerations -- References -- Blockchain for Trust and Reputation Management in Cyber-Physical Systems -- 1 Introduction -- 2 Blockchain-Based Trust and Reputation Management Systems -- 2.1 Trust and Reputation Management Systems for CPS -- 2.2 Adopting Blockchain for TRMS -- 3 Use Cases -- 3.1 Generic CPS Trust Architecture -- 3.2 Supply Chain Management -- 3.3 Crowdsourcing -- 3.4 Robotic and Autonomous Systems -- 3.5 Vehicular Ad Hoc Networks -- 3.6 IoT Data Marketplace -- 3.7 Distributed Energy Trading -- 4 Challenges and Future Directions -- 4.1 Scalability -- 4.2 Privacy -- 4.3 Resource Consumption -- 4.4 Security -- 4.5 Interoperability -- 5 Conclusion -- References.
Advances in Blockchain Security -- 1 Introduction -- 2 Background -- 2.1 Cryptographic Primitives -- 2.2 Blockchain Primer -- 3 Blockchain Security: Attacks and Counter-measures -- 3.1 Blockchain Network -- 3.2 Smart Contracts -- 3.3 Other Security Issues -- 4 Other Significant Advances in Blockchain -- 4.1 Anonymous Transactions -- 4.2 Consensus Protocols -- 4.3 Trusted Execution Environments (TEE) in Blockchain -- 5 Conclusions -- References -- Formal Verification of Blockchain Byzantine Fault Tolerance -- 1 Introduction -- 2 The Problem of Proving Blockchain Consensus Algorithms by Hand -- 2.1 The HoneyBadger and Its Randomized Binary Consensus -- 2.2 The Ethereum Blockchain and Its Upcoming Casper Consensus -- 2.3 Known Problems in Blockchain Byzantine Consensus Algorithms -- 3 A Methodology for Verifying Blockchain Components -- 3.1 Preliminaries on ByMC and BV-Broadcast -- 3.2 Automated Verification of a Blockchain Byzantine Broadcast -- 4 Verifying a Blockchain Byzantine Consensus Algorithm -- 4.1 Experimental Results -- 5 Related Work -- 6 Discussion and Conclusion -- References -- Decentralized Finance -- Constant Function Market Makers: Multi-asset Trades via Convex Optimization -- 1 Introduction -- 1.1 Background and Related Work -- 1.2 Convex Analysis and Optimization -- 2 Constant Function Market

Makers -- 2.1 CFMM State -- 2.2 Proposed Trade -- 2.3 Trading Function -- 2.4 Trading Function Examples -- 2.5 Prices and Exchange Rates -- 2.6 Adding and Removing Liquidity -- 2.7 Agents Interacting with CFMMs -- 3 Properties -- 3.1 Properties of Trades -- 3.2 Properties of Liquidity Changes -- 4 Two-Asset Trades -- 4.1 Exchange Functions -- 4.2 Exchanging Multiples of Two Baskets -- 5 Multi-asset Trades -- 5.1 The General Trade Choice Problem -- 5.2 Special Cases -- 5.3 Numerical Examples -- 6 Conclusion -- References.
Stablecoins: Reducing the Volatility of Cryptocurrencies.