1. Record Nr. UNINA9910770270303321

Autore	Pardalos Panos
Titolo	Mathematical Research for Blockchain Economy : 4th International Conference MARBLE 2023, London, United Kingdom / / edited by Panos Pardalos, Ilias Kotsireas, William J. Knottenbelt, Stefanos Leonardos
Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2023
ISBN	9783031487316 3031487311 9783031487309
Edizione	[1st ed. 2023.]
Descrizione fisica	1 online resource (193 pages)
Collana	Lecture Notes in Operations Research, , 2731-0418
Altri autori (Persone)	KotsireasIlias KnottenbeltWilliam J LeonardosStefanos
Disciplina	332
Soggetti	Finance Blockchains (Databases) Mathematical optimization Social sciences - Mathematics Business enterprises - Finance Econometrics Financial Economics Blockchain Optimization Mathematics in Business, Economics and Finance Corporate Finance Quantitative Economics
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Intro -- Preface -- Contents -- Deep Reinforcement Learning-Based Rebalancing Policies for Profit Maximization of Relay Nodes in Payment Channel Networks -- 1 Introduction -- 2 Background -- 2.1 Payment Channel Networks and the Need for Rebalancing -- 2.2 The Submarine Swap Rebalancing Mechanism -- 3 Problem Formulation -- 3.1 System

Evolution -- 3.2 Writing the Problem as a Markov Decision Process -- 4 Heuristic and Reinforcement Learning-Based Policies -- 4.1 Heuristic Policies -- 4.2 Deep Reinforcement Learning Algorithm Design -- 5 Evaluation -- 6 Related Work -- 7 Conclusion -- A Causes of Channel Depletion -- B The Submarine Swap Protocol -- C An Equivalent Objective -- D Deep Reinforcement Learning Algorithm Design Details -- D.1 Helping a Swap-In Succeed -- D.2 Design Choices -- D.3 Practical Applicability -- E Hyperparameters and Rewards -- F Additional Experimental Results -- F.1 The RebEL Policy Under Even Demand -- F.2 The Role of the Initial Conditions -- References -- Game-Theoretic Randomness for Proof-of-Stake -- 1 Introduction -- 2 Preliminaries -- 2.1 Games and Equilibria -- 2.2 Publicly-Verifiable Secret Sharing -- 2.3 Verifiable Delay Functions -- 3 Random Integer Generation Game (RIG) -- 3.1 Overview of RIG -- 3.2 Analysis of Alliance-Resistant Nash Equilibria -- 3.3 Dense RIG Bimatrix Game -- 4 Designing a Random Beacon Based on RIG -- 4.1 Commitment Scheme and VDF Approach -- 4.2 PVSS Approach -- 4.3 Further Details of the Approach -- 4.4 Assumptions and Limits to Applicability -- 5 RIG in Proof of Stake Protocols -- 5.1 RIG in Ouroboros Praos -- 5.2 RIG in Algorand -- 6 Conclusion -- References -- Incentive Schemes for Rollup Validators -- 1 Introduction -- 2 Model -- 2.1 Extension to n+1 Validators -- 2.2 Silent Validators -- 3 Protocol Level Incentives -- 4 Conclusions and Future Work -- References.
Characterizing Common Quarterly Behaviors in DeFi Lending Protocols -- 1 Introduction -- 2 Methods -- 2.1 Data Sources -- 2.2 Transaction-Level Data -- 2.3 Address-Level Summaries -- 2.4 Computation of Clusters -- 3 Results -- 3.1 Interpretations of Clusters -- 3.2 Insights Derived From Clusters -- 4 Related Work -- 5 Discussion and Future Work -- References -- Blockchain Transaction Censorship: (In)secure and (In)efficient? -- 1 Introduction -- 2 Background -- 2.1 Blockchain and Smart Contracts -- 2.2 Centralized Transaction Propagation Services -- 2.3 ZKP Mixers -- 2.4 Blockchain Regulation and Censorship -- 3 System Model -- 3.1 System Components -- 3.2 Blockchain Censoring -- 3.3 Threat Model -- 4 Censorship During Transaction Validation -- 4.1 Miners' Censorship on Tainted Transactions -- 4.2 DoS Censoring Miners Through Crafting Tainted Transactions -- 4.3 Attack Cost -- 5 Censorship During Transaction Propagation -- 5.1 FaaS Workflow -- 5.2 FaaS Censorship Mechanism -- 5.3 DoS Censoring FaaS Searchers and Builders -- 6 Censorship During Transaction Generation -- 6.1 Non-transparent Frontend-Level Censorship -- 6.2 Investigating DeFi Platforms' Censorship -- 6.3 Tainting Innocent Addresses -- 6.4 Bypassing Frontend-Level Censorship -- 7 Related Work -- 8 Conclusion -- References -- An Automated Market Maker Minimizing Loss-Versus-Rebalancing -- 1 Introduction -- 1.1 Our Contribution -- 1.2 Organization of the Paper -- 2 Related Work -- 3 Preliminaries -- 3.1 Constant Function Market Makers -- 3.2 Loss-Versus-Rebalancing -- 3.3 Auctions -- 4 Diamond -- 4.1 Model Assumptions -- 4.2 Core Protocol -- 4.3 Per-block Conversion Versus Future Contracts -- 4.4 Periodic Conversion Auction -- 5 Diamond Properties -- 6 Implementation -- 6.1 Core Protocol -- 6.2 Conversion Protocols -- 7 Experimental Analysis -- 8 Conclusion -- A Proofs -- References.
Profit Lag and Alternate Network Mining -- 1 Introduction -- 1.1 Nakamoto Consensus -- 1.2 Mining Process -- 1.3 Selfish Mining -- 1.4 Smart Mining -- 1.5 Intermittent Selfish Mining -- 1.6 Alternate Network Mining -- 1.7 Organization of This Article -- 2 Modelization -- 2.1 Mining and Difficulty Adjustment Formula -- 2.2 Notations -- 2.3 Profitability of a Mining Strategy -- 2.4 Attack Cycles -- 2.5

Performant Strategy and Profit Lag -- 3 Selfish Mining Revisited -- 3.1 Previous State-Machine Approach Revisited -- 3.2 Profit Lag -- 4 Intermittent Selfish Mining Strategy -- 4.1 Profit Lag -- 5 Alternate Network Mining Strategy -- 5.1 Profit Lag -- 6 Conclusion -- References -- Oracle Counterpoint: Relationships Between On-Chain and Off-Chain Market Data -- 1 Introduction -- 2 Methods -- 2.1 Fundamental Economic Features from On-Chain Markets -- 2.2 Data-Driven Feature Analysis -- 2.3 Modeling Off-Chain Prices -- 3 Results -- 3.1 Feature Analysis -- 3.2 Recovering Off-Chain Prices from On-Chain Data -- 3.3 Performance of Price Recovery -- 4 Discussion -- A More Details on Dataset Features -- A.1.1 Economic Features -- B Further Information on Ethereum Analysis -- B.1.1 Performance of Price Recovery -- C Analysis of Celo PoS Data -- References -- Exploring Decentralized Governance: A Framework Applied to Compound Finance -- 1 Introduction -- 1.1 Motivation -- 1.2 Contribution Summary -- 2 Compound -- 2.1 Governance -- 3 Relevant Work -- 3.1 Literature Discussion -- 4 Methodology and Data -- 4.1 Data -- 4.2 Methodology -- 4.3 Top 100 Leaderboard -- 4.4 Proposals -- 5 Discussion -- 6 Conclusions -- Appendix A Proof for Gini and Nakamoto Coefficients When n = 2 and u1 = u2 -- References -- A Mathematical Approach on the Use of Integer Partitions for Smurfing in Cryptocurrencies -- 1 Introduction -- 2 Related Work. 3 Using Integer Partitions to Create Patterns for Smurfing -- 3.1 Problem Formulation -- 3.2 Possible Implications of the Conceptualization of Smurfing via Integer Partitions -- 3.3 Examples for Integer Partitions and Smurfing -- 4 Conclusion and Future Work -- References -- Bigger Than We Thought: The Upbit Hack Gang -- 1 Introduction -- 2 Rough ML Network Construction -- 2.1 Crawling Tool and Event -- 2.2 Account and Transaction Data Crawling -- 2.3 Network Construction -- 3 ML Network Refinement -- 3.1 Design an ML Suspiciousness Indicator -- 3.2 Calculate ML Risks of Accounts -- 4 Results and Analysis -- 5 Conclusion -- References -- Staking Pools on Blockchains.

Sommario/riassunto

This book presents the best papers from the 4th International Conference on Mathematical Research for Blockchain Economy (MARBLE) 2023, held in London, UK. While most blockchain conferences and forums are dedicated to business applications, product development, or Initial Coin Offering (ICO) launches, this conference focused on the mathematics behind blockchain to bridge the gap between practice and theory. The book spans the divide between theoretical promise and practical reality in blockchain technology and explores the challenges hindering its real-world integration across diverse sectors, offering comprehensive insights into issues like scalability, security, and privacy. .