SpringerBriefs in Computer Science

SpringerBriefs present concise summaries of cutting-edge research and practical applications across a wide spectrum of fields. Featuring compact volumes of 50 to 125 pages, the series covers a range of content from professional to academic.

Typical topics might include:

- A timely report of state-of-the art analytical techniques
- A bridge between new research results, as published in journal articles, and a contextual literature review
- A snapshot of a hot or emerging topic
- An in-depth case study or clinical example
- A presentation of core concepts that students must understand in order to make independent contributions

Briefs allow authors to present their ideas and readers to absorb them with minimal time investment. Briefs will be published as part of Springer's eBook collection, with millions of users worldwide. In addition, Briefs will be available for individual print and electronic purchase. Briefs are characterized by fast, global electronic dissemination, standard publishing contracts, easy-to-use manuscript preparation and formatting guidelines, and expedited production schedules. We aim for publication 8–12 weeks after acceptance. Both solicited and unsolicited manuscripts are considered for publication in this series.

**Indexing: This series is indexed in Scopus, Ei-Compendex, and zbMATH **

More information about this series at http://www.springer.com/series/10028

Ahmed Imteaj • M. Hadi Amini
Panos M. Pardalos

Foundations of Blockchain

Theory and Applications

Springer

Ahmed Imteaj
Florida International University
Miami, FL, USA

M. Hadi Amini
Florida International University
Miami, FL, USA

Panos M. Pardalos
University of Florida
Gainesville, FL, USA

ISSN 2191-5768 ISSN 2191-5776 (electronic)
SpringerBriefs in Computer Science
ISBN 978-3-030-75024-4 ISBN 978-3-030-75025-1 (eBook)
https://doi.org/10.1007/978-3-030-75025-1

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

This book provides a comprehensive analysis of fundamental topics related to blockchain. It explores different vital issues and specific application areas that can benefit from blockchain. The authors present the elementary description, visualize the working procedure of the blockchain paradigm, and highlight the areas it can be applied in real life. The main focus of this book is to explain blockchain and its application from a new perspective, that is, distributed Internet of Things (IoT) and interdependent networks.

Miami, FL, USA — Ahmed Imteaj

Miami, FL, USA — M. Hadi Amini

Gainesville, FL, USA — Panos M. Pardalos

Contents

Part I Blockchain Theory

1 Introduction to Blockchain Technology 3
1.1 What Is Blockchain Technology? 3
1.2 Blockchain Components 4
1.2.1 Cryptographic Hash Functions 4
1.2.2 Transactions 5
1.2.3 Asymmetric-Key Cryptography 5
1.2.4 Block 6
1.2.5 Chaining Blocks 7
1.3 How Blockchain Works 7
1.4 Key Characteristics of Blockchain 8
1.4.1 Decentralization 8
1.4.2 Immutability 9
1.4.3 Anonymity 9
1.4.4 Auditability 10
1.4.5 Non-repudiation 10
1.5 Taxonomy of Blockchain 10
1.5.1 Public Blockchain 10
1.5.2 Private Blockchain 11
1.5.3 Consortium Blockchain 11
1.6 Examples of Blockchain Applications 12
1.7 Advantage and Limitations of Blockchain 12
1.8 Discussion 13
References 13

2 Toward Smart Contract and Consensus Mechanisms of Blockchain ... 15
2.1 Smart Contract 15
2.1.1 Creation of a Smart Contract 16
2.1.2 Deployment of a Smart Contract 18
2.1.3 Execution of a Smart Contract 18
2.1.4 Completion of a Smart Contract 18

2.2 Blockchain Consensus Algorithms 19
2.2.1 Proof-of-Work (PoW) Consensus Model 19
2.2.2 Proof of Stake (PoS) 20
2.2.3 Practical Byzantine Fault Tolerance 22
2.2.4 Proof of Elapsed Time 23
2.2.5 Proof of Activity 23
2.2.6 Proof of Importance 24
2.2.7 Proof of Capacity 24
2.2.8 Proof of Burn 25
2.3 Comparison of Typical Consensus Algorithms 26
2.4 Discussion 26
References 27

3 Blockchain Interoperability from the Perspective of Interdependent Networks 29
3.1 Interoperability Definition 29
3.2 An Architecture of Interoperability 30
3.2.1 Data Generation in Data Layer 31
3.2.2 Cross-Chain Mechanism in Network Layer 31
3.2.3 Verification of Transaction in Consensus Layer 32
3.2.4 Smart Contract for Cross-Chain Mechanism in Contract Layer 32
3.2.5 Application Programming Interface (API) in Application Layer 32
3.3 How Blockchain Interoperability Concept Can Be Useful for Interdependent Networks? 32
3.4 Interoperability Challenges 33
3.4.1 Assurance of Atomicity 33
3.4.2 Improvement of Efficiency 34
3.4.3 Maintenance of Security 34
3.4.4 Handling of Diversification 34
3.5 A Comparison of Existing Interoperability Schemes 35
3.6 Open Issues and Challenges 35
3.7 Research Directions 36
3.8 Discussion 37
References 37

Part II Blockchain Applications

4 Blockchain Applicability in Internet-of-Things (IoT) Environment 41
4.1 Importance of Integrating Blockchain with IoT 41
4.2 Customized Application of Blockchain in an IoT Environment 42
4.3 Blockchain-Based IoT (BIoT) Applications 45
4.3.1 Smart Home 45
4.3.2 Smart Energy 45
4.3.3 Smart Healthcare 46
4.3.4 Supply Chain Management 46

4.4 Current Challenges of BIoT Application 47
4.5 Discussion 48
References 48

5 Leveraging Blockchain Technology for Artificial Intelligence 51
5.1 Importance of Integrating Blockchain with AI 51
5.1.1 Improved and Secured Decision Outcomes 52
5.1.2 Collaborative Decision and Decentralized Intelligence 52
5.1.3 Reliable and Trustworthy Intelligent Decisions 53
5.1.4 Higher Efficiency 53
5.2 Goals of Blockchain-Based AI Applications 53
5.2.1 Autonomous Computation 53
5.2.2 Planning 54
5.2.3 Discovering New Knowledge 54
5.2.4 Perceive Environment 54
5.2.5 Efficient Searching 54
5.2.6 Optimization of Decision-Making Process 55
5.3 Emerging Challenges and Research Gaps 55
5.3.1 Privacy 55
5.3.2 Security 56
5.3.3 Scalability 56
5.3.4 Consensus Protocol Design for AI Applications 56
5.3.5 Blockchain Regulations and Interoperability 56
5.3.6 Governance 57
5.4 Discussion 57
References 57

6 Coupling Blockchain with Emerging Real-Life Applications 59
6.1 Blockchain in Healthcare 59
6.2 Energy Market Trading 61
6.3 Banking and Finance 62
6.4 Agriculture and Food Supply Chain 62
6.5 Smart City 63
6.6 Smart Manufacturing 65
6.7 Voting 66
6.8 Personal Identity Management 66
6.9 Discussion 67
References 67

Index 71

About the Authors

Ahmed Imteaj is currently a PhD candidate and graduate assistant at the Knight Foundation School of Computing and Information Sciences, Florida International University, under the supervision of Professor M. Hadi Amini. He is also a research lab member of Sustainability, Optimization, and Learning for InterDependent networks laboratory (solid lab) at Florida International University. His research interests span federated learning, machine learning, internet of things (IoT), smart systems, and Blockchain. He holds a B.Sc. degree in Computer Science and Engineering from Chittagong University of Engineering and Technology (CUET), Bangladesh in 2015. From 2015 to 2018, he worked as a Lecturer at International Islamic University Chittagong (IIUC), Chittagong, Bangladesh. Ahmed's work on federated learning for IoT environments is the recipient of the best paper award from "2019 IEEE Conference on Computational Science & Computational Intelligence" and won the second place at 2021 Florida International University Graduate Student Appreciation Week. He has published more than 30 referred journals and conference papers.

M. Hadi Amini is an assistant professor in the Knight Foundation School of Computing and Information Sciences at Florida International University. He is the director of Sustainability, Optimization, and Learning for InterDependent networks laboratory (www.solidlab.network). He received both his Ph.D. in electrical and computer engineering in 2019 and M.Sc. degree in 2015 from Carnegie Mellon University. He also holds a doctoral degree in computer science and technology. Prior to that, he received an M.Sc. degree from Tarbiat Modares University in 2013 and a B.Sc. degree from Sharif University of Technology in 2011. His research interests include distributed optimization and learning algorithms, distributed computing and intelligence, sensor networks, interdependent networks, and cyber-physical-social resilience. Application domains include smart cities, energy systems, transportation electrification, and healthcare.

Hadi is a life member of IEEE-Eta Kappa Nu (IEEE-HKN), the honor society of IEEE. He served as the president of Carnegie Mellon University Energy Science and Innovation Club, as technical program committee of several IEEE and ACM conferences, and as the lead editor for a book series on sustainable interdependent networks since 2017. He also serves as associate editor of SN Operations Research Forum and International Transactions on Electrical Energy Systems. He has published in more than 100 refereed journals and conference papers and book chapters. He edited/authored six books. He is the recipient of the best paper award at the 2019 IEEE Conference on Computational Science & Computational Intelligence, 2020 Excellence in Teaching Award from the School of Computing and Information Sciences at Florida International University, best reviewer award from four IEEE Transactions, the best journal paper award by the Journal of Modern Power Systems and Clean Energy, and the dean's honorary award from the president of Sharif University of Technology. (Homepage: www.hadiamini.com)

Panos M. Pardalos is a distinguished professor and the Paul and Heidi Brown preeminent professor in the Departments of Industrial and Systems Engineering at the University of Florida, and a world-renowned leader in global optimization, mathematical modeling, and data sciences. He is a fellow of AAAS, AIMBE, and INFORMS and was awarded the 2013 Constantin Caratheodory Prize by the International Society of Global Optimization. In addition, Dr. Pardalos has been awarded the 2013 EURO Gold Medal prize bestowed by the Association for European Operational Research Societies. This medal is the preeminent European award given to operations research (OR) professionals for "scientific contributions that stand the test of time." Dr. Pardalos is also a member of the New York Academy of Sciences, the Lithuanian Academy of Sciences, the Royal Academy of Spain, and the National Academy of Sciences of Ukraine. He is the founding editor of Optimization Letters, Energy Systems, and co-founder of the International Journal of Global Optimization. He has published over 600 papers, edited/authored over 200 books, and organized over 80 conferences. He has about 57,000 citations on his work, an H-index of 95, an i10- index of 575 (Google Scholar), and has graduated 62 Ph.D. students so far.