Introduction to the Special Issue on Mathematical Research for Blockchain Economy

Blockchain Technology has been considered as the most revolutionizing invention since the Internet. Because of its immutable nature and the associated security and privacy benefits, it has widely attracted the attention of banks, governments, techno-corporations and venture investors. Blockchain applications range from finance to healthcare, from education and media to logistics, NFTs and many more. However, the theoretical limitations and technical barriers to the adoption of blockchain such as scalability, latency, privacy and security need to be further studied and addressed in high-quality research.

This special issue of the *ACM Distributed Ledger Technologies: Research and Practice (ACM DLT)* journals contains selected and refereed papers on the topic of *Mathematical Research in Blockchain Economies.* Preliminary versions of some of the papers appeared in the 2022 edition of the International Conference on Mathematical Research for Blockchain Economy (MARBLE'22), which took place in Vilamoura, Portugal, from July 12 to 24, 2022. Following the paradigm of the conference, the current special issue provides a high-profile, cutting-edge platform for mathematicians, computer scientists and economists, from both industry and practice, to present the latest advances and innovations in key theories of blockchain. Having a broad international appeal, both the MARBLE conference and the current special issue focuses on the mathematics behind blockchain to bridge the gap between theory and practice.

The three selected article in this special issue were selected from 10 submitted manuscripts, following the standard, rigorous ACM DLT review procedures. The articles cover topics in decentralized finance, smart contracts and game-theoretic modelling of blockchains. The content of the articles is as follows.

Sylvain Carré (Universite Paris Dauphine), Franck Gabriel (ISFA, SAF), Clément Hongler (EPFL), Gustavo Lacerda and Gloria Capano in their article titled "Smart Proofs via Recursive Information Gathering: Decentralized Refereeing by Smart Contracts" introduce a **Smart Proofs via Recursive Information Gathering (SPRIG)** protocol that allows agents to propose, question and defend mathematical proofs in a decentralized fashion. The SPRIG protocol, which can run autonomously as a smart contract on a blockchain platform, utilises a complex structure of economic incentives and an oracle that are designed to promote succinct and informative proofs. The article offers insight into the game-theoretic properties of the protocol and dives deep into the possible attacks that the protocol's designers will need to take into account.

Lin Chen (Texas Tech University), Lei Xu (The University of Texas Rio Grande, Valley College of Sciences), Zhimin Gao (Auburn University at Montgomery), Ahmed Sunny (Texas Tech University, Computer Science), Keshav Kasichainula (University of Houston) and Weidong Shi (University of Houston System) in their article titled "A Game Theoretical Analysis of Non-linear Blockchain System" establish a formal framework and prove that, despite their impressive recent advances, no blockchain system can achieve a set of desirable properties related to partial verification, high scalability and low finality simultaneously. They then set out to analyse prominent

ACM Reference Format:
Stefanos Leonardos, William Knottenbelt, Elise Alfieri, Panos Pardalos, and Ilias Kotsireas. 2024. Introduction to the Special Issue on Mathematical Research for Blockchain Economy. *Distrib. Ledger Technol.* 3, 1, Article 1 (March 2024), 2 pages. https://doi.org/10.1145/3649882

© 2024 Copyright held by the owner/author(s).
ACM 2769-6472/2024/03-ART1
https://doi.org/10.1145/3649882

blockchain platforms, such as those that support Bitcoin and Ethereum, within the established framework and provide useful insights on the combinations of properties that these protocols can achieve in practice.

Finally, in their article titled "DeFi Survival Analysis: Insights into the Emerging Decentralized Financial Ecosystem," a group of researchers from Rensselaer Polytechnic Institute, USA, consisting of Aaron M. Green, Michael P. Giannattasio, John S. Erickson, Oshani Seneviratne and Kristing P. Bennett propose a novel survival analysis approach for discovering and characterizing user behavior and risks for lending protocols in **decentralized finance (DeFi)**. The approach utilises a wide range of statistical and visualisation methods to measure and quantify risks within the protocol. Through extensive evaluations and rich numerical results, the authors demonstrate how the established framework can be leveraged to answer critical questions regarding the stability and security of lending protocols and how it can be generalised to address similar queries in any other transaction handling cryptocurrency protocol.

We are most thankful to Editor-in-Chief Kim-Kwang Raymond Choo for giving us the opportunity to organize and edit this special issue. We also wish to think Editor-in-Chief Mohammad Hammoudeh for their contribution in editing this issue. We also thank Rebecca Malone, the journal's administrator, and the ACM staff for their support in all aspects of editing this issue. Finally, we would like to extend our special thanks to the reviewers of this special issue for all their invaluable contributions in ensuring a fair and detailed assessment of all submitted manuscripts and in improving the quality and presentation of the accepted articles.

Stefanos Leonardos
King's College London, London, United Kingdom
email: stefanos.leonardos@kcl.ac.uk

William Knottenbelt
Imperial College London, London, United Kingdom
email: w.knottenbelt@imperial.ac.uk

Elise Alfieri
Université Paris Est-Créteil, Paris, France
email: elise.alfieri@u-pec.fr

Panos Pardalos
University of Florida, Florida, United States of America
email: pardalos@ufl.edu

Ilias Kotsireas
Wilfried Laurier University, Waterloo, Canada
email: ikotsire@wlu.ca

Guest Editors