

Lecture Notes in Networks and Systems 595

Javier Prieto

Francisco Luis Benitez Martínez

Stefano Ferretti

David Arroyo Guardeso

Pedro Tomás Nevado-Batalla *Editors*

# Blockchain and Applications, 4th International Congress

 Springer

# Lecture Notes in Networks and Systems

Volume 595

## Series Editor

Janusz Kacprzyk, Systems Research Institute, Polish Academy of Sciences,  
Warsaw, Poland

## Advisory Editors

Fernando Gomide, Department of Computer Engineering and Automation—DCA,  
School of Electrical and Computer Engineering—FEEC, University of  
Campinas—UNICAMP, São Paulo, Brazil

Okay Kaynak, Department of Electrical and Electronic Engineering,  
Bogazici University, Istanbul, Turkey

Derong Liu, Department of Electrical and Computer Engineering, University of  
Illinois at Chicago, Chicago, USA

Institute of Automation, Chinese Academy of Sciences, Beijing, China

Witold Pedrycz, Department of Electrical and Computer Engineering, University of  
Alberta, Alberta, Canada

Systems Research Institute, Polish Academy of Sciences, Warsaw, Poland

Marios M. Polycarpou, Department of Electrical and Computer Engineering,  
KIOS Research Center for Intelligent Systems and Networks, University of Cyprus,  
Nicosia, Cyprus

Imre J. Rudas, Óbuda University, Budapest, Hungary

Jun Wang, Department of Computer Science, City University of Hong Kong,  
Kowloon, Hong Kong

The series “Lecture Notes in Networks and Systems” publishes the latest developments in Networks and Systems—quickly, informally and with high quality. Original research reported in proceedings and post-proceedings represents the core of LNNS.

Volumes published in LNNS embrace all aspects and subfields of, as well as new challenges in, Networks and Systems.

The series contains proceedings and edited volumes in systems and networks, spanning the areas of Cyber-Physical Systems, Autonomous Systems, Sensor Networks, Control Systems, Energy Systems, Automotive Systems, Biological Systems, Vehicular Networking and Connected Vehicles, Aerospace Systems, Automation, Manufacturing, Smart Grids, Nonlinear Systems, Power Systems, Robotics, Social Systems, Economic Systems and other. Of particular value to both the contributors and the readership are the short publication timeframe and the world-wide distribution and exposure which enable both a wide and rapid dissemination of research output.

The series covers the theory, applications, and perspectives on the state of the art and future developments relevant to systems and networks, decision making, control, complex processes and related areas, as embedded in the fields of interdisciplinary and applied sciences, engineering, computer science, physics, economics, social, and life sciences, as well as the paradigms and methodologies behind them.

Indexed by SCOPUS, INSPEC, WTI Frankfurt eG, zbMATH, SCImago.

All books published in the series are submitted for consideration in Web of Science.

For proposals from Asia please contact Aninda Bose ([aninda.bose@springer.com](mailto:aninda.bose@springer.com)).

Javier Prieto · Francisco Luis Benítez Martínez ·  
Stefano Ferretti · David Arroyo Guardado ·  
Pedro Tomás Nevado-Batalla  
Editors

# Blockchain and Applications, 4th International Congress

 Springer

*Editors*

Javier Prieto  
Departamento de Informática y Automática  
University of Salamanca  
Salamanca, Spain

Francisco Luis Benítez Martínez  
Parque Tecnológico de la Salud (PTS)  
Granada, Spain

Stefano Ferretti  
University of Urbino Carlo Bo  
Urbino, Italy

David Arroyo Guardado  
Spanish National Research Council (CSIC)  
Madrid, Spain

Pedro Tomás Nevado-Batalla  
Facultad de Derecho  
University of Salamanca  
Salamanca, Spain

ISSN 2367-3370

ISSN 2367-3389 (electronic)

Lecture Notes in Networks and Systems

ISBN 978-3-031-21228-4

ISBN 978-3-031-21229-1 (eBook)

<https://doi.org/10.1007/978-3-031-21229-1>

© The Editor(s) (if applicable) and The Author(s), under exclusive license to Springer Nature Switzerland AG 2023

This work is subject to copyright. All rights are solely and exclusively licensed by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors, and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

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

# Organization

## General Chair

Javier Prieto Tejedor University of Salamanca, (Spain) and AIR Institute, Spain

## Advisory Board

Abdelhakim Hafid Université de Montréal, Canada  
Ashok Kumar Das IIIT Hyderabad, India  
António Pinto Instituto Politécnico do Porto, Portugal  
Paulo Leitao Technical Institute of Bragança, Portugal

## Program Committee Chair

Francisco Luis Benitez Martínez Fidesol, Spain

## Local Chair

Stefano Ferretti University of Bologna, Italy

## Organizing Committee Chair

Pedro Nevado University of Salamanca, Spain

## Local Organizing Committee

Pierpaolo Vittorini (Co-chair)	University of L'Aquila, Italy
Tania Di Mascio (Co-chair)	University of L'Aquila, Italy
Federica Caruso	University of L'Aquila, Italy
Anna Maria Angelone	University of L'Aquila, Italy

## Organizing Committee

Juan M. Corchado Rodríguez	University of Salamanca, Spain, AIR Institute, Spain
Fernando De la Prieta	University of Salamanca, Spain
Sara Rodríguez González	University of Salamanca, Spain
Javier Prieto Tejedor	University of Salamanca, Spain, AIR Institute, Spain
Pablo Chamoso Santos	University of Salamanca, Spain
Liliana Durón	University of Salamanca, Spain
Belén Pérez Lancho	University of Salamanca, Spain
Ana Belén Gil González	University of Salamanca, Spain
Ana De Luis Reboredo	University of Salamanca, Spain
Angélica González Arrieta	University of Salamanca, Spain
Emilio S. Corchado Rodríguez	University of Salamanca, Spain
Alfonso González Briones	University of Salamanca, Spain
Yeray Mezquita Martín	University of Salamanca, Spain
Beatriz Bellido	University of Salamanca, Spain
María Alonso	University of Salamanca, Spain
Sergio Marquez	University of Salamanca, Spain
Marta Plaza Hernández	University of Salamanca, Spain
Guillermo Hernández González	AIR Institute, Spain
Ricardo S. Alonso Rincón	University of Salamanca, Spain
Raúl López	University of Salamanca, Spain
Sergio Alonso	University of Salamanca, Spain
Andrea Gil	University of Salamanca, Spain
Javier Parra	University of Salamanca, Spain

## Program Committee

Mahmoud Abbasi	University of Salamanca, Salamanca
Ermyas Abebe	ConsenSys R&D, USA
Iván Abellán	Outpost24, Sweden

Mo Adda	University of Portsmouth, UK
Imtiaz Ahmad Akhtar	XLENT Link, Sweden
Sami Albouq	Islamic University of Madenah, Saudi Arabia
Ricardo S. Alonso	AIR Institute, Valladolid
Onur Ascigil	University College London, UK
Anusha Avyukt	University of Southern California, USA
Syed Badruddoja	University of North Texas, USA
Richard Banach	The University of Manchester, UK
Aritra Banerjee	Trinity College Dublin, Ireland
Badr Bellaj	Mchain, Morocco
Yahya Benkaouz	Mohammed V University in Rabat, Morocco
José Vicente Berná Martínez	University of Alicante—Computer Science Department, Spain
Cyrille Bertelle	Le Havre University, France
Andrea Bondavalli	University of Florence, Italy
Carlos Bordons	University of Seville, Spain
William J. Buchanan	Napier University, UK
Arnaud Castellort	Université de Montpellier, France
Bishakh Chandra Ghosh	Indian Institute of Technology Kharagpur, India
Sang-Yoon Chang	University of Colorado Colorado Springs, USA
Mohammad Jabed Morshed Chowdhury	La Trobe University, Australia
Giovanni Ciatto	University of Bologna, Italy
Victor Cook	University of Central Florida, USA
Manuel E. Correia	CRACS/INESC TEC; DCC/FCUP, Portugal
Gaby G. Dagher	Boise State University, USA
Sankarshan Damle	IIIT Hyderabad, India
Ashok Kumar Das	International Institute of Information Technology, India
Giovanni De Gasperis	DISIM, Università degli Studi dell'Aquila, Italy
Josep Lluís De La Rosa	TECNIO Centre EASY Innovation, UdG, Spain
Volkan Dedeoglu	CSIRO, Australia
Roberto Di Pietro	Hamad Bin Khalifa University—College of Science and Engineering, Qatar
Ba-Lam Do	Hanoi University of Science and Technology, Vietnam
Katerina Doka	National Technical University of Athens, Greece
Claude Duvallet	LITIS—Université Le Havre Normandie, France
Joshua Ellul	University of Malta, Malta
Sante Dino Facchini	Università degli Studi dell'Aquila, Italy
Tooba Faisal	King's College London, UK
Wenjun Fan	Xi'an Jiaotong-Liverpool University, China
Xinxin Fan	IoTeX, USA
Manuel J. Fernandez	University of Seville, Spain



Christof Ferreira Torres	University of Luxembourg, Luxembourg
Ernestas Filatovas	Vilnius University, Lithuania
Nikos Fotiou	AUEB, Greece
Miguel Frade	Instituto Politécnico de Leiria, Portugal
Paula Fraga-Lamas	University of A Coruña, CITIC, Spain
Muriel Franco	University of Zurich, Switzerland
Felix Freitag	Universitat Politècnica de Catalunya, Spain
Shahin Gheitanchi	IEEE, UK
Radu Godina	NOVA University Lisbon, Portugal
Seep Goel	IBM Indian Research Labs, India
Mongetro Goint	Université Le Havre Normandie, France
Hélder Gomes	Escola Superior de Tecnologia e Gestão de Águeda, Universidade de Aveiro, Portugal
Dhrubajyoti Goswami	Concordia University, Canada
Volker Gruhn	Universität Duisburg-Essen, Germany
Susana Gutiérrez	Fundación CARTIF, Spain
Abdelatif Hafid	University of Montreal, Canada
Christopher G. Harris	University of Northern Colorado, USA
Yahya Hassanzadeh-Nazarabadi	Ferdowsi University of Mashhad, Turkey
Pham Hoai Luan	NAIST, Japan
Tim Hoiss	Universität der Bundeswehr München, Germany
Hsiang-Jen Hong	University of Colorado Colorado Springs, USA
Qin Hu	George Washington University, USA
Yining Hu	IBM Australia, Australia
Maria Visitación Hurtado	University of Granada, Spain
Shahid Hussain	National University of Ireland, Ireland
Fredrick Ishengoma	The University of Dodoma, Tanzania
Hans-Arno Jacobsen	University of Toronto, Canada
Marc Jansen	University of Applied Sciences Ruhr West, Germany
Zakwan Jaroucheh	Edinburgh Napier University, UK
Eder John Scheid	University of Zurich, Switzerland
Christina Joseph	National Institute of Technology Karnataka, India
Taeho Jung	University of Notre Dame, USA
Raja Jurdak	QUT, Australia
K. Chandrasekaran	NITK, India
Ayten Betul Kahya	University of Southern California, USA
Dimitris Karakostas	University of Edinburgh, UK
Christos Karapapas	Athens University of Economics and Business, Greece
Samuel Karumba	UNSW, Australia
Shoji Kasahara	Nara Institute of Science and Technology, Japan
Latifur Khan	UTD, USA
Nectarios Koziris	National Technical University of Athens, Greece

Renata Kramberger	Zagreb University of Applied Sciences, Croatia
Mohamed Laarabi	Mohammadia School of Engineering Rabat, Morocco
Oscar Lage	TECNALIA, Spain
Chhagan Lal	University of Padova, Italy
Anne Laurent	LIRMMUM, France
Ulrike Lechner	Universität der Bundeswehr München, Germany
Paulo Leitao	Polythecnic Institute of Braganca, Portugal
Boyang Li	University of Notre Dame, USA
Sotirios Liaskos	School of IT, York University, Canada
Roben Lunardi	IFRS, Brazil
Fengji Luo	The University of Sydney, Australia
João Paulo Magalhaes	ESTGF, Porto Polytechnic Institute, Portugal
Aanchal Malhotra	Ripple, USA
Yacov Manevich	IBM, Israel
Stefano Mariani	Università degli Studi di Modena e Reggio Emilia, Italy
Luis Martínez	University of Jaén, Spain
Collin Meese	University of Delaware, USA
Gerard Memmi	Telecom Paris, France
Imran Memon	Zhejiang University, China
Suat Mercan	Florida International University, USA
Yeray Mezquita	Universidad de Salamanca, Spain
Saraju Mohanty	University of North Texas, USA
Juan Jose Morillas Guerrero	Universidad Politécnica de Madrid, Spain
Vaikunth Mugunthan	Massachusetts Institute of Technology, USA
Daniel-Jesus Munoz	ITIS Software, Universidad de Malaga, Spain
Mikhail Nesterenko	Kent State University, USA
Binh Minh Nguyen	Hanoi University of Science and Technology, Vietnam
Joseph Oglio	Kent State University, USA
Andrea Omicini	Alma Mater Studiorum–Università di Bologna, Italy
Kazumasa Omote	University of Tsukuba, Japan
Arindam Pal	Data61, CSIRO, Australia
Andreea-Elena Panait	University of Bucharest, Romania
Gaurav Panwar	New Mexico State University, USA
Nohpill Park	Oklahoma State University, USA
Alberto Partida	URJC, Spain
Rafael Pastor Vargas	UNED, Spain
Remigijus Paulavičius	Institute of Data Science and Digital Technologies, Lithuania
Miguel Pincheira	Fondazione Bruno Kessler, Italy
Karl Pinter	TU Vienna (INSO), Austria

António Pinto	ESTG, P.Porto, Portugal
Pedro Pinto	ESTG Polytechnic Institute of Viana do Castelo, Portugal
Steven Platt	Universitat Pompeu Fabra, Spain
Matthias Pohl	Otto-von-Guericke-Universität Magdeburg, Germany
Hauke Precht	University Oldenburg, Germany
Wolfgang Prinz	Fraunhofer, Germany
Guntur Dharma Putra	The University of New South Wales, Australia
Yuansong Qiao	Athlone Institute of Technology, Ireland
Venkatraman Ramakrishna	IBM Research—India, India
Emanuel Regnath	Technical University of Munich, Germany
Cristina Regueiro	TECNALIA Research and Innovation, Spain
Denisa Reshef Kera	Tel Aviv University, Israel
Richard Richard	Bina Nusantara University, Indonesia
Peter Robinson	School of Information Technology and Electrical Engineering, University of Queensland, Australia
Bruno Rodrigues	University of Zurich, Switzerland
Ivan Rodriguez-Conde	University of Arkansas at Little Rock, USA
Thomas Rose	Fraunhofer, Germany
Maria Saiz Santos	University of the Basque Country UPV/EHU, Spain
Abiola Salau	University of North Texas, USA
Gernot Salzer	Vienna University of Technology, Austria
Georgios Samakovitis	University of Greenwich, UK
Altino Sampaio	Instituto Politécnico do Porto, Escola Superior de Tecnologia e Gestão de Felgueiras, Portugal
Elio San Cristóbal Ruiz	UNED, Spain
Ricardo Santos	ESTG/IPP, Portugal
Vishal Saraswat	Robert Bosch Engineering and Business Solutions Pvt. Ltd. (RBEI/ESY), India
Dominik Schmelz	Research Group for Industrial Software (INSO), Austria
Karl Seidenfad	Universität der Bundeswehr München, Germany
Jongho Seol	Middle Georgia State University, USA
Gokarna Sharma	Kent State University, USA
Wazen Shbair	University of Luxembourg-SnT, Luxembourg
Chien-Chung Shen	University of Delaware, USA
Ajay Shrestha	University of Saskatchewan, Canada
Mirza Kamrul Bashar Shuhan	Bkash Limited, Bangladesh
Saurabh Shukla	National University of Ireland Galway, Ireland
Ram Govind Singh	Indian Computer Emergency Response Team, Ministry of Electronics and IT, India
Manuel Sivianes	Universidad de Sevilla, Spain

Benfano Soewito	Bina Nusantara University, Indonesia
Mark Staples	CSIRO, Australia
Denis Stefanescu	Ikerlan, Spain
Marko Suvajdzic	University of Florida, USA
Stefan Tai	TU Berlin, Germany
Chamseddine Talhi	École de Technologie Supérieure, Canada
Teik Guan Tan	Singapore University of Technology and Design, Singapore
Keisuke Tanaka	Tokyo Institute of Technology, Japan
Subhasis Thakur	National University of Ireland, Galway, Ireland
Llanos Tobarra	UNED, Spain
Natkamon Tovanich	IRT SystemX, France
Tuan Tran	CMPS232, USA
Florian Tschorsch	TU Berlin, Germany
Kritagya Upadhyay	University of North Texas, USA
Aitor Urbieto	IK4-Ikerlan Technology Research Centre, Spain
Julita Vassileva	University of Saskatchewan, Canada
Massimo Vecchio	FBK, Spain
Andreas Veneris	University of Toronto, Canada
Paulo Vieira	Instituto Politécnico da Guarda, Portugal
Luigi Vigneri	IOTA Foundation, Germany
Marco Vitale	Foodchain Spa, Italy
Chenggang Wang	University of Cincinnati, USA
Alexander Weinert	German Aerospace Center (DLR), Germany
Tatjana Welzer	University of Maribor, Faculty of Electrical Engi- neering and Computer Science, Slovenia
Lei Xu	University of Texas Rio Grande Valley, USA
Yury Yanovich	Skoltech, Russia
Kosala Yapa Bandara	NUI Galway, Ireland
Amr Youssef	Concordia University, Canada
Jiangshan Yu	Monash University, Australia
Uwe Zdun	University of Vienna, Austria
Kaiwen Zhang	École de Technologie Supérieure de Montréal, Canada
Chen Zhao	UTDallas, USA
Haofan Zheng	UC Santa Cruz, USA
Mirko Zichichi	Universidad Politécnica de Madrid, Spain
Avelino F. Zorzo	PUCRS, Brazil
André Zúquete	University of Aveiro, Portugal

## **Workshop on Beyond the Promises of Web3.0: Foundations and Challenges of Trust Decentralization (WEB3-TRUST)**


















Web 3.0 has arisen as the next step into the configuration of a more secure and trustworthy Internet. This new stage in the deployment of web technologies is based on the implementation of new architectures for trust decentralization. Distributed ledger technologies and, in specific, blockchain are used as the main components to manage trust without any central authority. Nonetheless, the deployment of such technologies in real and practical scenarios is of problematic nature, and in many occasions this leads to the re-centralization of decision taking. This being the case, governance and the supposed equality provided by blockchain and DLT are hindered, which eventually determine cybersecurity risks of major impact than those in web 2.0. This workshop is devoted to discuss these shortcomings and the associated cyber-risks, taking into account the current state of maturity of blockchain, smart contracts, and the new governance schemes in the blockchain era.

### **Organizing Committee Chairs**




David Arroyo    CSIC, Spain  
Jesús Díaz Vico    IOHK, EE.UU.

### **Program Committee**

Luca Nizzardo    Protocol Labs, Spain  
Antonio Nappa    Universidad Carlos III de Madrid, Spain  
Andrés Marín López    Universidad Carlos III de Madrid, Spain  
Andrea Vesco    Head of cybersecurity at LINKS Foundation, Italy  
Pedro López    CSIC, Spain  
Mayank Dhiman    Dropbox, USA

Sponsors	Organizers
 	   
 	 Instituto Superior de Engenharia do Porto  
 	
 	
 	

Support from National Associations

		
---	---	---

© Copyright 2022

**BLOCKCHAIN'22 Sponsors**

# Preface

The 4th International Congress on Blockchain and Applications 2022 was held in L'Aquila from 13th to 15th of July. This annual congress reunites blockchain and artificial intelligence (AI) researchers who share ideas, projects, lectures, and advances associated with those technologies and their application domains.

Among the scientific community, blockchain and AI are seen as a promising combination that will transform the production and manufacturing industry, media, finance, insurance, e-government, etc. Nevertheless, there is no consensus with schemes or best practices that would specify how blockchain and AI should be used together. Combining blockchain mechanisms and artificial intelligence is still a particularly challenging task.

The BLOCKCHAIN'22 congress has been devoted to promoting the investigation of cutting-edge blockchain technology, to exploring the latest ideas, innovations, guidelines, theories, models, technologies, applications, and tools of blockchain and AI for the industry, and to identifying critical issues and challenges those researchers and practitioner must deal with in future research. BLOCKCHAIN'22 wants to offer researchers and practitioners the opportunity to work on promising lines of research and to publish their developments in this area.

In this 4th edition of the congress, the technical program has been diverse and of high quality, focused on contributions to both well-established and evolving areas of research. The congress has had an acceptance rate close to 50%. More than 75 papers were submitted, and 37 full papers were accepted. The volume also includes three papers from the WEB3-TRUST workshop and two papers from the Doctoral Consortium.

Shipments came from more than 35 different countries (Spain, USA, Sweden, UK, Saudi Arabia, Ireland, Morocco, France, Italy, India, Australia, Portugal, Qatar, Greece, Vietnam, Malta, China, Luxembourg, Lithuania, Switzerland, Canada, Germany, Turkey, Japan, Tanzania, Croatia, Brazil, Israel, Romania, Indonesia, Bangladesh, Singapore, Slovenia, Russia, and Austria).

We would like to thank all the contributing authors, the members of the program committee, the sponsors (IBM, Indra, DISIM, MESVA, Armundia, Reply White Hall, Technologies and Communication, LCL, MDPI, AEPIA, APPIA, and AIR Institute),

and the Organizing Committee for their hard and highly valuable work. Their work contributed to the success of the BLOCKCHAIN'22 event. And finally, special thanks to the local organization members and the program committee members for their hard work, which was essential for the success of BLOCKCHAIN'22.

Javier Prieto  
Francisco Luis Benítez Martínez  
Stefano Ferretti  
David Arroyo Guardañó  
Pedro Tomás Nevado-Batalla



# Contents

## **BLOCKCHAIN 2022 Main Track**

<b>Modelling of the Internet Computer Protocol Architecture: The Next Generation Blockchain</b> .....	3
AoXuan Li, Luca Serena, Mirko Zichichi, Su-Kit Tang, Gabriele D’Angelo, and Stefano Ferretti	
<b>Assessing Blockchain Challenges in the Maritime Sector</b> .....	13
Rim Abdallah, Jérôme Besancenot, Cyrille Bertelle, Claude Duvallet, and Frédéric Gilletta	
<b>A Model of Decentralised Distribution Line Using Layer 2 Blockchains</b> .....	23
Subhasis Thakur and John Breslin	
<b>ChronoEOS: Configuration Control System Based on EOSIO Blockchain for On-Running Forensic Analysis</b> .....	37
Jose Alvaro Fernandez-Carrasco, Telmo Egues-Arregui, Francesco Zola, and Raul Orduna-Urrutia	
<b>Sharding-Based Proof-of-Stake Blockchain Protocol: Security Analysis</b> .....	48
Abdelatif Hafid, Abdelhakim Hafid, and Adil Senhaji	
<b>Cryptocurrencies, Survey on Legal Frameworks and Regulation Around the World</b> .....	58
Yeray Mezquita, Dévika Pérez, Alfonso González-Briones, and Javier Prieto	
<b>SmartTwin: A Blockchain-Based Software Framework for Digital Twins Using IoT</b> .....	67
Miguel Pincheira, Massimo Vecchio, and Fabio Antonelli	
<b>Proofs and Limitations of the Pathway Protocol</b> .....	78
Marc Jansen, Ilya Sapranidi, and Aleksei Pupyshev	

**Profitable Fee Controller for Payment Channel Networks** ..... 88  
 Anupa De Silva, Subhasis Thakur, and John Breslin

**Riddle: A Fully Decentralized Mobile Game for Fun and Profit** ..... 100  
 Athanasia Maria Papatthanasidou, Chalima Dimitra Nassar Kyriakidou,  
 Iakovos Pittaras, and George C. Polyzos

**Mitigation of Scaling Effects in NTF-Based Ticketing Systems** ..... 110  
 Dan Heilmann, Daniel Muschiol, Lars Karbach, Moritz Korte,  
 Nils Orbat, Vincenzo Schulte am Hülse, and Marc Jansen

**Digital Content Verification Using Hyperledger BESU** ..... 120  
 Carmen María Alba, Francisco Luis Benítez-Martínez,  
 Manuel Ventura-Duque, and Rafael Muñoz-Román

**Prototyping a Smart Contract Application for Fair Reward  
 Distribution in Software Development Projects** ..... 131  
 Agostino Di Dia, Tim Riebner, Alexander Arntz, and Marc Jansen

**Blockchain in the Public Sector: An Umbrella Review of Literature** .... 142  
 Fernando Escobar, Henrique Santos, and Teresa Pereira

**Digital Identity Using Hyperledger Fabric as a Private  
 Blockchain-Based System** ..... 153  
 Suhail Odeh, Anas Samara, Ramiz Rizqallah, and Lara Shaheen

**Cryptocurrencies, Systematic Literature Review on Their Current  
 Context and Challenges** ..... 162  
 Yeray Mezquita, Marta Plaza-Hernández, Mahmoud Abbasi,  
 and Javier Prieto

**Blockchain Assisted Voting in Academic Councils** ..... 173  
 João Alves and António Pinto

**Scalable and Transparent Blockchain Multi-layer Approach  
 for Smart Energy Communities** ..... 183  
 Marta Chinnici, Luigi Telesca, Mahfuzul Islam,  
 and Jean-Philippe Georges

**Blockchain Consensus Algorithms: A Survey** ..... 198  
 Pooja Khobragade and Ashok Kumar Turuk

**Decentralised Argumentation for Data Vetting in Blockchains** ..... 211  
 Subhasis Thakur and John Breslin

**Designing the Chain of Custody Process for Blockchain-Based  
 Digital Evidences** ..... 225  
 Pablo Santamaría, Llanos Tobarra, Rafael Pastor-Vargas,  
 and Antonio Robles-Gómez

**The Devil Hides in the Model: Reviewing Blockchain and BFT Protocols** ..... 237  
 Antoine Durand and Gérard Memmi

**Blockchain-Based Business Process Management (BPM) for Finance: The Case of Loan-Application** ..... 249  
 Galena Pisoni, Meriem Kherbouche, and Bálint Molnár

**Objective-Aware Reputation-Enabled Blockchain-Based Federated Learning** ..... 259  
 Samaneh Miri Rostami, Saeed Samet, and Ziad Kobti

**Enhancing Smart Contract Quality by Introducing a Continuous Integration Pipeline for Solidity Based Smart Contracts** ..... 269  
 Hauke Precht, Florian Schwarm, and Jorge Marx Gómez

**“Are You What You Claim to Be?” Attribute Validation with IOTA for Multi Authority CP-ABE** ..... 279  
 Aintzane Mosteiro-Sanchez, Marc Barcelo, Jasone Astorga, and Aitor Urbieto

**Privacy-Preserving Energy Trade Using Double Auction in Blockchain Offline Channels** ..... 289  
 Subhasis Thakur, John Breslin, and Sweta Malik

**Interoperable Industry 4.0 Plant Blockchain and Data Homogenization via Decentralized Oracles** ..... 303  
 Denis Stefanescu, Leticia Montalvillo, Patxi Galán-García, Juanjo Unzilla, and Aitor Urbieto

**Towards Cost-Efficient Management for Power Purchase Agreements Using Blockchain Technology** ..... 314  
 Ivan Gutierrez-Aguero, Yesnier Bravo, Daniel Landa, Oscar Lage, Iñaki Seco, and Aitor Castillo

**Tokenizing the Portuguese Accounting Standards System** ..... 324  
 Paulo Vieira and Helena Saraiva

**Bibliometric Analysis on the Convergence of Artificial Intelligence and Blockchain** ..... 334  
 Maryam Hajizadeh, Morteza Alaeddini, and Paul Reaidy

**Towards an Infrastructure Cost Model for Blockchain-Based Applications** ..... 345  
 Miguel Pincheira, Elena Donini, Massimo Vecchio, and Raffaele Giaffreda

**A Benchmarking Study of Blockchain-Based Technology Implementation Cost: Public and Private Blockchain for Enterprise Level Organization Using Benchmarking Model** ..... 356  
Richard, Vera Angelina, Felix, and Michael Wangsa Mulia

**SSI4Web: A Self-sovereign Identity (SSI) Framework for the Web** ..... 366  
Md Sadek Ferdous, Andrei Ionita, and Wolfgang Prinz

**The Communicational Universe of Cryptocurrencies. An Approach to the Current Scientific Importance** ..... 380  
Sergio Manzano, Javier Parra-Domínguez, Francisco Pinto, Alfonso González-Briones, and Guillermo Hernández

**Evaluation and Comparison of a Private and a Public Blockchain Solution for Use in Supply Chains of SMEs Based on a QOC Analysis** ..... 388  
Vanessa Carls, Lambert Schmidt, and Marc Jansen

**Identification of False Stealthy Data Injection Attacks in Smart Meters Using Machine Learning and Blockchain** ..... 398  
Saurabh Shukla, Subhasis Thakur, Shahid Hussain, John G. Breslin, and Syed Muslim Jameel

**Workshop on Beyond the Promises of Web3.0: Foundations and Challenges of Trust Decentralization (WEB3-TRUST)**

**Enhancing the Anonymity and Auditability of Whistleblowers Protection** ..... 413  
Sergio Chica, Andrés Marín, David Arroyo, Jesús Díaz, Florina Almenares, and Daniel Díaz

**Bottom-Up Trust Registry in Self Sovereign Identity** ..... 423  
Kai Jun Eer, Jesus Diaz, and Markulf Kohlweiss

**Integrating Web3 Features into Moodle** ..... 434  
Urban Vidovič, Vid Keršič, and Muhamed Turkanović

**Doctoral Consortium**

**Overview of Multiple User Encryption for Exchange of Private Data via Blockchains** ..... 447  
Vanessa Carls, Lambert Schmidt, and Marc Jansen

**Blockchain Adoption in the Energy Sector: A Comprehensive Regulatory Readiness Assessment Framework to Assess the Regulatory Readiness Levels of Countries** ..... 454  
Karisma Karisma and Pardis Moslemzadeh Tehrani

**Author Index** ..... 461

# **BLOCKCHAIN 2022 Main Track**



# Modelling of the Internet Computer Protocol Architecture: The Next Generation Blockchain

AoXuan Li<sup>1</sup>(✉), Luca Serena<sup>2</sup>, Mirko Zichichi<sup>3</sup>, Su-Kit Tang<sup>1</sup>,  
Gabriele D'Angelo<sup>2</sup>, and Stefano Ferretti<sup>4</sup>

<sup>1</sup> Faculty of Applied Sciences, Macao Polytechnic University, Macao SAR, China  
aoxuan.li@mpu.edu.mo sktang@ipm.edu.mo

<sup>2</sup> Department of Computer Science and Engineering,  
University of Bologna, Bologna, Italy  
luca.serena2@unibo.it g.dangelo@unibo.it

<sup>3</sup> Ontology Engineering Group, Universidad Politécnica de Madrid, Madrid, Spain  
mirko.zichichi@upm.es

<sup>4</sup> Department of Pure and Applied Sciences, University of Urbino “Carlo Bo”,  
Urbino, Italy  
stefano.ferretti@uniurb.it

**Abstract.** The Internet Computer Protocol is described as a third-generation blockchain system that aims to provide secure and scalable distributed systems through blockchains and smart contracts. In this position paper, this innovative architecture is introduced and then discussed in view of its modeling and simulation aspects. In fact, a properly defined digital twin of the Internet Computer Protocol could help its design, development, and evaluation in terms of performance and resilience to specific security attacks. To this extent, we propose a multi-level simulation model that follows an agent-based paradigm. The main issues of the modeling and simulation, and the main expected outcomes, are described and discussed.

**Keywords:** Internet Computer · Distributed Ledger Technology · Modelling and simulation · Blockchain

## 1 Introduction

Cloud computing has undoubtedly been the fastest growing and most successful in delivering technical and economic benefits for application and system development in recent years [26, 30]. Starting from startups up to large companies, everyone is adopting cloud computing to get rid of the risk of capital

---

This work has received funding from the EU H2020 research and innovation programme under the MSCA ITN grant agreement No 814177 LAST-JD-RIoE; and the research grant (No.: RP/ESCA-04/2020) offered by Macao Polytechnic University.

© The Author(s): under exclusive license to Springer Nature Switzerland AG 2023  
J. Prieto et al. (Eds.): BLOCKCHAIN 2022, LNNS 595, pp. 3–12, 2023.  
[https://doi.org/10.1007/978-3-031-21229-1\\_1](https://doi.org/10.1007/978-3-031-21229-1_1)

investment, cutting the cost of hardware and software infrastructure, and availing themselves of services according to their demand. This is why paradigms such as ‘Infrastructure-as-a-Service (IaaS)’, ‘Platform-as-a-Service (PaaS)’, and ‘Software-as-a-Service (SaaS)’ have emerged. In general, however, cloud service providers maintain their customers with an opaque knowledge about the location and storage of data, the privacy offered to users, and the type of hardware infrastructure used. This leads firstly to a problem of trust by users [19]. Secondly, security and privacy are undermined by the centrality of these solutions, which more easily attracts cyber-attacks, i.e. single points of failure [30]. In addition, it should not be forgotten that centralized solutions will not be able to support the huge amount of data generated globally by users and Internet-of-Things devices for much longer [26]. Finally, it is commonly difficult to assess if Quality of Service (QoS) guarantees are met and Service Level Agreements (SLA) negotiated between users and the cloud provider are satisfied, due to the absence of trusted logs [7]. All this motivates the transition towards a completely decentralized approach. The benefits of this solution are many. In fact, the decentralization of the system removes the presence of a single point of failure, allows for inherently increasing scalability, curbs illicit activities of malicious nodes, and can also provide for accountability guarantees. Clearly, in order to realize a similar kind of system, it becomes necessary to encourage node participation that can be somehow rewarded through incentive mechanisms [33].

The Internet Computer Protocol (ICP) architecture<sup>1</sup> aims to establish a network of networks by defining a protocol for combining the resources of several decentralized computers into the reading, replication, modification, and procurement of an application state. A network of nodes runs the protocol through independently-operated data centers to provide general-purpose (largely) transparent computations for end-users. On the other hand, the development of applications on top of the ICP is facilitated by reliable message delivery, transparent accountability, and resilience. The typical use-case would involve users interacting with a decentralized application as is on a public or private cloud. This is enabled by the use of Canisters, i.e. tamper-proof and autonomous smart contracts hosted on-chain, that can be run concurrently and interact with each other. With respect to other smart contract implementations, such as Ethereum’s ones, the Canisters enable applications, systems, and services to be created and accessed by users without incorporating websites running on centralized cloud hosting, e.g. a canister can directly serve HTTP requests created by end-users through their browser. All of this paves the way for the creation of decentralized services where the user is constantly at the center of the process.

However, the design of the ICP requires a complete understanding of the technologies involved and the interactions among these building blocks. There is a need for viable modeling and simulation strategies that allow for what-if analyses and manageable evaluation studies. In this paper, we describe the rationale behind the design of an ICP digital twin that could serve this purpose.

---

<sup>1</sup> Authors are not sponsored or affiliated in any way with the DFINITY Foundation which is the not-for-profit organization that develops the Internet Computer.

Due to the complexity of the system, high levels of detail should be kept only when needed, while coarse simulations should be exploited when dealing with a high number of involved nodes. This leads to a multi-level simulator design [6].

This paper is structured as follows. Section 2 provides the necessary background about the technologies used in the ICP and a discussion of the related work. Section 3 presents a specific introduction of the ICP; while in Sect. 4, the main modelling and simulation issues of the ICP are discussed. Finally, Sect. 5 provides the concluding remarks.

## 2 Background and Related Work

### 2.1 Related Technologies

In this section, we briefly describe the background technologies and methodologies that are necessary for understanding the ICP architecture and evaluating the main problems that are related to its modelling and simulation.

**Blockchains** Informally, a blockchain is a public ledger that may hold any data, e.g., transactions between different parties, email records, or even daily grocery records. The ledger is distributed among all network participants, and it is immutable once written down. As the name suggests, a blockchain is a chain of blocks while each block contains a set of records. Moreover, a block also contains a timestamp and the hash value of the previous block. If any adversary user tries to change intermediate blocks, he/she has to change all following blocks. However, this is impossible since the ledger is decentralized. For any new block, it will not automatically join the chain until the majority of parties agree so. Blockchains have made impacts on various areas [20].

**Consensus Algorithms** Consensus algorithms allow (the majority of) nodes to agree on the status of the ledger. That is, they agree on the validity of transactions in a block, the validity of the block itself, and if there is more than one proposed block, on which block is appended to the chain. There are different types of consensus algorithms. Among them, two are worthy of mention here, i.e. proof-based algorithm and vote-based algorithm [24]. In a proof-based algorithm, parties need to solve a cryptography puzzle, and the first successful one gets the right to append the block. In a vote-based algorithm, if a party wants to append a block, there must be more than  $T$  parties appending the same block where  $T$  is a threshold number.

**Smart Contracts** Smart contracts are a set of instructions (or the source code from which such instructions were compiled from) stored in the blockchain and automatically triggered once the default condition is met [2]. This execution is triggered via a transaction and will produce a change in the blockchain state. Each node executing the instructions receives the same inputs and produces the



same outputs, thanks to a shared protocol. Smart contracts enable the execution of a service without a trusted human third party validator to check the terms of an agreement, however the smart contract issuer must be sure that the behaviour implemented is correct [2]. For instance, the creation of smart contract-based services may enable users to interact with devices/vehicles or favor interoperability in smart cities [14, 32].

## 2.2 Related Work

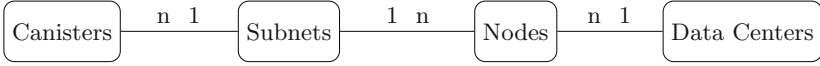
While there are no specific simulations of the ICP architecture, some simulators have been proposed for modelling blockchains and distributed ledgers technologies. The main difference between the simulators is the level of detail (and the corresponding simulation methodology) that has been chosen for modelling the system to be represented. For example, in [27], some of the authors of this paper have proposed an agent-based simulation to investigate some well-known network attacks on blockchains and distributed ledgers. In [1], the authors present BlockSim which is a discrete-event simulator of blockchain systems (implemented in Python) that specifically considers the modeling and simulation of block creation through the proof-of-work consensus algorithm. A totally different approach is introduced in [22], in which the queuing theory is used for modelling blockchain systems. In [29], the authors propose VIBES which is another blockchain simulator but specifically designed and implemented for large-scale peer-to-peer networks and able to simulate blockchain systems beyond Bitcoin and support large-scale simulations with thousands of nodes. Finally, in [25], the authors propose an approach that is based on stochastic blockchain models (i.e. Monte Carlo simulations).

## 3 The Internet Computer Protocol (ICP)

The ICP is defined as the third generation of the blockchain systems [31], where the first generation is Bitcoin [23], and the second generation is Ethereum [4]. The ICP provides an infinite blockchain where we may hold everything. Unlike previous blockchain systems, it aims to be scalable and to run at web speed. The main technical components of the Internet Computer are the Canister [8] and the Network Nervous System (NNS) [9]. The canister is a special type of smart contract. Users may interact with a canister directly as long as they know the identity of the canister. In the ICP, communication between the different nodes is demanded to the Network Nervous System (NNS, see Sect. 3.1).

The ICP has a four-layer structure. From bottom to top, there are data centers, nodes, subnets, and canisters. Data centers are hardware devices for holding nodes, and each node is a physical computer providing computational power. Each data center may have many nodes, and nodes from different data centers could build up a subnet. Each subnet hosts many canisters, which is the application program on the ICP. Figure 1 reports a high-level representation of this design structure. Each subnet handles the trust and immutability of the

Canister with a blockchain. The blockchain grows in rounds, and, in each round, a randomly selected node proposes a block containing the canister inputs and the hash of the previous block. If the majority of nodes agree on the subnet’s state and the validity of the new block, this new block is appended to the blockchain.



**Fig. 1.** The ICP high-level design architecture.

The ICP design guarantees the availability of canisters in subnets. In fact, by implementing a replication approach, the canisters do not suddenly stop running in case of localised failures. As long as more than two-thirds of replicas are online, the canister is available. A critical requirement for this approach is that all replicas must catch up with the latest state. In previous blockchains, like Bitcoin and Ethereum, this would require downloading the whole blockchain. The ICP provides a CatchUp Package (CUP) [10] so that a node only needs to download a limited amount of data to catch up with the current state of the blockchain. The CUP contains an intermediate replica state and a subsequent of the blockchain. With the replica state, the node can compute the next state on itself, and with the sub-blockchain, it can verify the replica states.

The ICP community claims that their blockchain could scale out to billions of users [11]. Since each canister can only support up to 4 GB of memory (i.e. due to the limitations of WebAssembly) then the Internet Computer uses a multi-canister architecture. For example, for a video-sharing application, it would be possible to split the user-uploaded content into multiple chunks and store them into multiple canisters. When a user wants to retrieve a video, the user makes a query call to the front-end canister, which in turn will make cross-canisters requests to multiple storage canisters. It is worth noticing that all these operations are transparent to users. Table 1 summarizes the main terms used to describe the ICP architecture.

**Table 1.** Main terms used in the ICP architecture.

Term	Definition
Canister	A special type of smart contract
Catch Up Packages (CUP)	A schema for state synchronization
Data center	The decentralized hardware of the ICP architecture
Network Nervous System (NNS)	A special canister serving as the governance body
Node	The peer computer in data centers
Subnet	The blockchain for providing computing resources

### 3.1 Network Nervous System

To obtain a scalable and highly efficient system, the ICP must be able to host any number of canisters and to run them concurrently. The ICP introduces a novel Decentralized Autonomous Organization (DAO) that is called Network Nervous System (NNS). The NNS is designed for managing all the base nodes of the system through a Proof-of-Stake consensus protocol.

More specifically, NNS is a set of initial canister programs that oversee the whole network. For example, a data center may apply to the NNS to join the network. NNS also manages how the subnets are formed and how the replication of the nodes is managed. Moreover, the NNS is in charge of upgrading the ICP. For example, the users are enabled to submit proposals for changing the ICP design and implementation. NNS will host the proposal and then allow users to vote on the proposal. Finally, the NNS will implement and deploy the proposal, if the majority of the users have approved it.

### 3.2 Chain Key Cryptography

Most likely, the main scientific breakthrough provided by the ICP is the Chain Key Cryptography [12, 16]. In the ICP, a canister is replicated through a subnet, and those nodes in the subnet have to agree on the computation results. The high-level process is described below:

1. each node holds a secret key share;
2. if enough nodes agree on the result then they can jointly sign the message with their respective key share;
3. the user may verify the received message with a single public-key.

If some nodes have failed or crashed then the NNS will add new nodes to the subnet, and the remaining active nodes will reshare the secret key while keeping the same public key. In the ICP, all subnets have a public key and corresponding secret key shares, and all those public keys could be verified with a single 48-byte public key. Even if the Internet Computer had millions of nodes, the network would only need one public key to verify all messages. This technology is called Chain Key Cryptography [12]. The used protocol builds on Shamir secret sharing [28] and BLS signature [3], and moreover, it facilitates the secret sharing keys creation and refreshing.

## 4 Modelling and Simulation of the ICP Architecture

The aim of the Modelling and Simulation (M&S) techniques is to reproduce the behaviour of the system under investigation, in order to (i) study the dynamics of interaction among the various components, (ii) evaluate the resilience of the system under specific conditions (e.g. cyberattacks or failures) and (iii) assess the impact of possible future extensions or features to the system before its implementation or even to support their design. Specifically for the ICP architecture, different aspects are of interest under a M&S viewpoint. First of all, it

is important to model the consensus protocol, in order to analyze how the block creation flow is working.

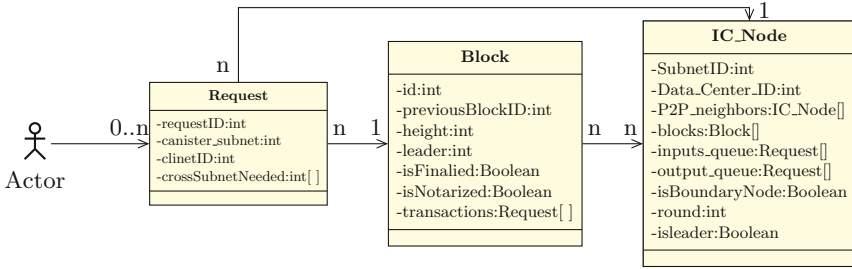
While state-of-the-art works regarding the simulation of Distributed Ledger Technology (DLT) focus on Bitcoin-like protocols, with only one blockchain collecting the incoming data [27], we are interested in modeling a DLT where multiple partial blockchains (i.e. subnets) work asynchronously in parallel, exchanging information when necessary. Furthermore, we think that, what is needed to model, are also the aspects specifically related to the DAO (i.e. the Decentralized Autonomous Organization [18]), that is in charge of managing the policies and the future developments of the DLT. This is because the level of security, scalability, decentralization and also the economical sustainability of the whole architecture strongly depends on the DAO's decisions.

A common problem in M&S is the level of detail to be chosen when abstracting the real system to a simulation model. In fact, a fine grained model that considers the very detailed aspects (such as the transmission of every network packet in the distributed system of interest) would permit a high-level model accuracy at the cost of a relevant complexity in the management of the obtained model and in the execution overhead of the simulator. On the other hand, a high-level model in which, for example, the communication aspects in the distributed system are neglected, would permit the building of a very simple (and fast) simulator with poor accuracy. Choosing the most appropriate level of detail to be used in the M&S is not easy and it is strongly linked to the desired outcomes of the simulator. For example, the modelling of some specific cyber-security attacks in a distributed system often requires a very specific level of abstraction in the communications. For these reasons, we think that in a scenario such as the ICP architecture in which we are interested in many different aspects of different abstraction layers, a solution based on a fixed level of abstraction would not be optimal. In fact, we plan to employ an approach that is based on multi-level modelling and simulation [17]. This approach is not new but it is still not very common in the simulation of complex systems. More in detail, we plan to build an ICP model in which the different components are represented by two (or more) simulated models that will be alternatively used depending on the specific analysis that we are interested in. For example, when the specific aspects related to the DAO will be investigated, some low-level details of the model will not be required and therefore the "high-level" (i.e. coarse-grained) version of some components will be used. On the other hand, when the security of the consensus protocol will be investigated then the "fine-grained" models will be required.

#### 4.1 Design and Implementation of an ICP Simulator

In order to model and simulate the ICP architecture, we decided to employ an agent-based approach. Agent-Based Simulation (ABS) is a widely diffused technique that in the years gained a lot of popularity in many different fields such as engineering, economics, and computational social sciences [21]. In ABS, the most relevant system components and modules are represented by means of

agents. Every agent is then characterized by a specific behavior and interacts with other agents using interactions (that are often implemented as messages). In other words, the system evolution is represented through changes in the local state of the agents (and of the environment) in which they are located.



**Fig. 2.** Class diagram of the main components of the ICP architecture.

Referring more specifically to the modeling of the ICP architecture, two types of agents populate our simulation scenario: firstly, there are the clients of the system, which can carry out transactions and requests to the system. Secondly, there are the nodes of the ICP, each one localized in a specific data center, and operating in a specific subnet. Figure 2 shows a possible modelling of the ICP nodes. All the nodes are located in a certain datacenter, belong to a specific subnet and maintain a set of blocks as well as a set of transactions still to validate.

The current implementation of the ICP architecture relies on a very low number of nodes, since 32 subnets exist, each one with 13 nodes contributing to store the transactions (except the NNS, which is dealt with as a special subnet, composed of 40 nodes) [13]. Thus, for the modelling and simulation of the current setup of the ICP architecture, the simulator’s scalability is not a big concern. However, it is expected and already planned that the future developments of the ICP will lead to a considerable growth of the network size, with many more nodes and subnets involved in the validation of transactions. We plan to use the developed simulation tools to be able to investigate and properly assess how such a network growth should be managed. For example, right now it is easy for the nodes to be directly in contact with all the other peers belonging to the same subnet, but with many more nodes managing a single subnet, a gossip algorithm might be adopted to efficiently disseminate blocks and transactions inside each subnet [5]. Moreover, from a simulation point of view, more simulated entities entail a larger amount of computing resources employed and a greater execution time. Thus, Parallel And Distributed Simulation (PADS) [15] approaches might be necessary to efficiently carry out the tests.

## 5 Conclusions

The Internet Computer Protocol (ICP) architecture is a third generation blockchain system that is being designed, implemented, and deployed to provide a secure and a scalable way for creating very large-scale distributed systems. In this position paper, we have introduced the ICP architecture and its main problems in terms of modelling and simulation. In fact, the usage of proper simulation techniques would permit us to investigate some very relevant aspects of the ICP architecture and support its design. The main issues related to the modelling and simulation of the ICP concern the specific level of detail used for abstracting the system in a model that can be then evaluated using a simulation. In the following of this paper, we described our current effort in the creation of an agent-based simulator of the ICP that is able to both provide the desired level of detail and the needed scalability. The creation of the ICP simulator is an ongoing activity that requires a relevant effort in many different phases (e.g., design, implementation, and validation) that will likely permit us to release a preliminary version of the simulator in the next months.

## References

1. Alharby, M., van Moorsel, A.: Blocksims: a simulation framework for blockchain systems. *SIGMETRICS Perform. Eval. Rev.* **46**(3), 135–138 (2019)
2. Becker, M., Bodó, B.: Trust in blockchain-based systems. *Internet Policy Rev.* **10**(2) (2021)
3. Boneh, D., Lynn, B., Shacham, H.: Short signatures from the Weil pairing. In: *International Conference on the Theory and Application of Cryptology and Information Security*, pp. 514–532. Springer (2001)
4. Buterin, V., et al.: A next-generation smart contract and decentralized application platform. *White Paper* **3**(37) (2014)
5. D’Angelo, G., Ferretti, S.: Highly intensive data dissemination in complex networks. *J. Parallel Distrib. Comput.* **99**, 28–50 (2017)
6. D’Angelo, G., Ferretti, S., Ghini, V.: Multi-level simulation of internet of things on smart territories. *Simul. Model. Pract. Theory* **73**, 3–21 (2017). *Smart Cities and Internet of Things*
7. D’Angelo, G., Ferretti, S., Marzolla, M.: A blockchain-based flight data recorder for cloud accountability. In: *Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems (CryBlock)* (2018)
8. Dfinity: a closer look at software canisters, an evolution of smart contracts (2021). <https://medium.com/dfinity/software-canisters-an-evolution-of-smart-contracts-internet-computer-flf92f1bfff>
9. Dfinity: The network nervous system: governing the internet computer (2021). <https://medium.com/dfinity/the-network-nervous-system-governing-the-internet-computer-1d176605d66a>
10. Dfinity: Resumption: how internet computer nodes quickly catch up to the blockchain’s latest state (2021). <https://medium.com/dfinity/resumption-how-internet-computer-nodes-quickly-catch-up-to-the-blockchains-latest-state-5af6e53e2a7>