2019 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON 2019)

Newark, California, USA
4 – 9 April 2019

IEEE Catalog Number: CFP19S63-POD
ISBN: 978-1-7281-1265-7

Copyright © 2019 by the Institute of Electrical and Electronics Engineers, Inc.
All Rights Reserved

Copyright and Reprint Permissions: Abstracting is permitted with credit to the source. Libraries are permitted to photocopy beyond the limit of U.S. copyright law for private use of patrons those articles in this volume that carry a code at the bottom of the first page, provided the per-copy fee indicated in the code is paid through Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923.

For other copying, reprint or republication permission, write to IEEE Copyrights Manager, IEEE Service Center, 445 Hoes Lane, Piscataway, NJ 08854. All rights reserved.

****** This is a print representation of what appears in the IEEE Digital Library. Some format issues inherent in the e-media version may also appear in this print version.***

IEEE Catalog Number: CFP19S63-POD
ISBN (Print-On-Demand): 978-1-7281-1265-7
ISBN (Online): 978-1-7281-1264-0

Additional Copies of This Publication Are Available From:

Curran Associates, Inc
57 Morehouse Lane
Red Hook, NY 12571 USA
Phone: (845) 758-0400
Fax: (845) 758-2633
E-mail: curran@proceedings.com
Web: www.proceedings.com

2019 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON)

DAPPCON 2019

Table of Contents

Message from General Chairs ix
Message from Program Chairs x
Organizing Committee xi
Program Committee xii
Steering Committee xiii
Keynotes xiv

Full Papers I: Blockchain Protocols

Blockchain: A Novel Approach for the Consensus Algorithm Using Condorcet Voting Procedure 1
David Vangulick (University of Liege), Bertrand Cornélusse (University of Liege), and Damien Ernst (University of Liege)

Alt-PoW: An Alternative Proof-of-Work Mechanism 11
Sarah Sharkey (Trinity College Dublin, Ireland) and Hitesh Tewari (Trinity College Dublin, Ireland)

Lock and Load: A Model for Free Blockchain Transactions through Token Locking 19
Paul Merrill (0Chain LLC / San Jose State University), Thomas Austin (0Chain LLC / San Jose State University), Jenil Thakker (San Jose State University), Younghee Park (San Jose State University), and Justin Rietz (San Jose State University)

Full Papers II: Applications

Tawki: Towards Self-Sovereign Social Communication 29
Martin Westerkamp (Technische Universität Berlin), Sebastian Göndör (Technische Universität Berlin), and Axel Küpper (Technische Universität Berlin)

Reducing Automotive Counterfeiting Using Blockchain: Benefits and Challenges .39
Donghang Lu (Purdue University, USA), Pedro Moreno-Sanchez (TU Wien, Austria), Amanuel Zeryihun (Ford Motor Company, USA), Shivam Bajpayi (Purdue University, USA), Sihao Yin (Purdue University, USA), Ken Feldman (Ford Motor Company, USA), Jason Kosofsky (Ford Motor Company, USA), Pramita Mitra (Ford Motor Company, USA), and Aniket Kate (Purdue University, USA)

A Usage-Based Mechanism for Securing Systems Via Blockchains .49
Eric Brigham (New College of Florida, USA), John A. Doucette (New College of Florida, USA), and Matthew Lepinski (New College of Florida, USA)

Full Papers III: Smart Contracts & Analytics

Supporting Reuse of Smart Contracts through Service Orientation and Assisted Development .59
Luca Guida (Politecnico di Milano) and Florian Daniel (Politecnico di Milano)

A Survey of Tools for Analyzing Ethereum Smart Contracts .69
Monika di Angelo (TU Wien, Austria and EURECOM, France) and Gernot Salzer (TU Wien, Austria and EURECOM, France)

Performance Modeling and Analysis of the Bitcoin Inventory Protocol .79
Yahya Shahsavari (École de technologie supérieure (ÉTS)), Kaiwen Zhang (École de technologie supérieure (ÉTS)), and Cahmseddine Talhi (École de technologie supérieure (ÉTS))

Full Papers IV: Identity & Token Economy

A Risk Redistribution Standard for Practical Cryptocurrency Payment .89
Yao-Chieh Hu (The Hong Kong University of Science and Technology, China), Ting-Ting Lee (The Hong Kong University of Science and Technology, China), and Chungsang Lam (Clemson University, United States)

Splitting and Aggregating Signatures in Cryptocurrency Protocols .100
S. Sharmila Deva Selvi (Indian Institute of Technology, Madras), Arinjita Paul (Indian Institute of Technology Madras), C. Pandu Rangan (Indian Institute of Technology Madras), Siva Dirisala (OCHAIN, USA), and Saswata Basu (OCHAIN, USA)

On the Practicality of a Smart Contract PKI .109
Christos Patsonakis (University of Athens), Katerina Samari (University of Athens), Aggelos Kiayiasy (University of Edinburgh and IOHK), and Mema Roussopoulos (University of Athenss)

Short Papers I: Blockchain Protocols

Proof-of-Learning: A Blockchain Consensus Mechanism Based on Machine Learning Competitions .119
Felipe Bravo-Marquez (University of Waikato), Steve Reeves (University of Waikato), and Martín Ugarte (Universidad Catolica de Chile)

Irregular-Program-Based Hash Algorithms .125
Qi Zhou (QuarkChain Foundation LTD)

An Improved Non-Interactive Zero-Knowledge Range Proof for Decentralized Applications .129
Ya Che Tsai (National Chengchi University, Taiwan), Raylin Tso (National Chengchi University, Taiwan), Zi-Yuan Liu (National Chengchi University, Taiwan), and Kung Chen (National Chengchi University, Taiwan)

Short Papers II: Applications I

A Secure Permissioned Blockchain Based System for Trademarks .135
Girish Showkatramani (USPTO), Nidhi Khatri (Arktix Solutions, Inc.), Arlene Landicho (Arktix Solutions, Inc.), and Darwin Layog (Arktix Solutions, Inc.)

PartChain: A Decentralized Traceability Application for Multi-Tier Supply Chain Networks in the Automotive Industry .140
Daniel Miehle (BMW Group, Germany), Dominic Henze (Technical University of Munich, Germany), Andreas Seitz (Technical University of Munich, Germany), Andre Luckow (BMW Group, Germany), and Bernd Bruegge (Technical University of Munich, Germany)

Integration of Blockchain and Internet of Things in a Car Supply Chain .146
Tim Reimers (Bundeswehr University Munich, Germany), Felix Leber (Bundeswehr University Munich, Germany), and Ulrike Lechner (Bundeswehr University Munich, Germany)

Short Papers III: Applications II

Leveraging Standards Based Ontological Concepts in Distributed Ledgers: A Healthcare Smart Contract Example .152
Mengyi Li (Rensselaer Polytechnic Institute), Lirong Xia (Rensselaer Polytechnic Institute), and Oshani Seneviratne (Rensselaer Polytechnic Institute)

DevID: Blockchain-Based Portfolios for Software Developers .158
Martijn de Vos (Delft University of Technology, The Netherlands), Mitchell Olsthoorn (Delft University of Technology, The Netherlands), and Johan Pouwelse (Delft University of Technology, The Netherlands)

Process Mining for Decentralized Applications .164
Marcel Müller (Technische Universität Berlin, Germany) and Peter Ruppel (Technische Universität Berlin, Germany)

Short Papers IV: Smart Contracts

An Alternative Paradigm for Developing and Pricing Storage on Smart Contract Platforms .170
Christos Patsonakis (University of Athens) and Mema Roussopoulos (University of Athens)

Modularizing Cross-Cutting Concerns with Aspect-Oriented Extensions for Solidity . 176
Chien-Che Hung (National Chengchi University, Taiwan), Kung Chen (National Chengchi University, Taiwan), and Chun-Feng Liao (National Chengchi University, Taiwan)

Strengthening Smart Contracts to Handle Unexpected Situations . 182
Shuze Liu (Rensselaer Polytechnic Institute, USA), Farhad Mohsin (Rensselaer Polytechnic Institute, USA), Lirong Xia (Rensselaer Polytechnic Institute, USA), and Oshani Seneviratne (Rensselaer Polytechnic Institute, USA)

Author Index 189