2019 Crypto Valley Conference on Blockchain Technology (CVCBT 2019)

Rotkreuz, Switzerland
24 – 26 June 2019

IEEE Catalog Number: CFP19P12-POD
ISBN: 978-1-7281-3670-7

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: CFP19P12-POD
ISBN (Print-On-Demand): 978-1-7281-3670-7
ISBN (Online): 978-1-7281-3669-1

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 Crypto Valley Conference on Blockchain Technology (CVCBT)

CVCBT 2019

Table of Contents

Accepted Papers

Revelio: A MimbleWimble Proof of Reserves Protocol 7
Arijit Dutta (Indian Institute of Technology Bombay) and Saravanan Vijayakumaran (Indian Institute of Technology Bombay)

SATOS: Storage Agnostic Tokens over Opaque and Substructural Types 12
Markus Knecht (University of Zurich) and Burkhard Stiller (University of Zurich)

BitVis: An Interactive Visualization System for Bitcoin Accounts Analysis 21
Yujing Sun (The University of Hong Kong), Hao Xiong (The University of Hong Kong), Siu Ming Yiu (The University of Hong Kong), and Kwok Yan Lam (Nanyang Technological University)

Refinement and Verification of CBC Casper 26
Ryuya Nakamura (The University of Tokyo / Research and Development, LayerX), Takayuki Jimba (Research and Development, LayerX), and Dominik Harz (Imperial College London)

Albatross – An optimistic consensus algorithm 39
Pascal Berrang (Nimiq Foundation), Philipp von Styp-Rekowsky (Nimiq Foundation), Marvin Wissfeld (Nimiq Foundation), Bruno França (Trinkler Software), and Reto Trinkler (Trinkler Software)

Short Paper: Anti-Withholding Reward System to Secure Blockchain Mining Pools 43
Arijet Sarker (University of Colorado Colorado Springs), Simeon Wuthier (University of Colorado Colorado Springs), and Sang-Yoon Chang (University of Colorado Colorado Springs)

Monetary Stabilization in Cryptocurrencies – Design Approaches and Open Questions 47
Ingolf G.A. Pernice (Weizenbaum-Institute/Humboldt-Universität zu Berlin), Sebastian Henningsen (Weizenbaum-Institute/Humboldt-Universität zu Berlin), Roman Proskalovich (Weizenbaum-Institute/Humboldt-Universität zu Berlin/Belarusian State University), Martin Florian (Weizenbaum-Institute/Humboldt-Universität zu Berlin), Hermann Elendner (Independent), and Björn Scheuermann (Weizenbaum-Institute/Humboldt-Universität zu Berlin)

Applying Private Information Retrieval to Lightweight Bitcoin Clients 60
Kaihua Qin (Imperial College London), Henryk Hadass (Imperial College London), Arthur Gervais (Imperial College London), and Joel Reardon (University of Calgary)

FastProxy: Hardware and Software Acceleration of Stratum Mining Proxy 73
Guanwen Zhong (Xilinx, Singapore), Haris Javaid (Xilinx, Singapore), Hassaan Saadat (University of New South Wales, Australia), Lingchao Xu (Bitmaintech Pte. Ltd., Singapore), Chengchen Hu (Xilinx, Singapore), and Gordon Brebner (Xilinx, USA)

Whispering Botnet Command and Control Instructions 77
Mathis Baden (University of Luxembourg), Christof Ferreira Torres (University of Luxembourg), Beltran Borja Fiz Pontiveros (University of Luxembourg), and Radu State (University of Luxembourg)

A Blockchain Proxy for Lightweight IoT Devices 82
Gero Dittmann (IBM Research – Zurich) and Jens Jelitto (IBM Research – Zurich)

Author Index **87**