2019 IEEE International Conference on Blockchain (Blockchain 2019)

Atlanta, Georgia, USA
14 – 17 July 2019

IEEE Catalog Number: CFP19U50-POD
ISBN: 978-1-7281-4694-2

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: CFP19U50-POD
ISBN (Print-On-Demand): 978-1-7281-4694-2
ISBN (Online): 978-1-7281-4693-5

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 Blockchain (Blockchain)

Blockchain 2019

Table of Contents

Welcome Message from the Cybermatics 2019 Congress Chairs ..... **xv**
Cybermatics 2019 Organizing Committee ..... **xvii**
Message from the Blockchain 2019 General Chairs ..... **xviii**
Message from the Blockchain 2019 Program Chairs ..... **xx**
Blockchain 2019 Organizing and Program Committees ..... **xxi**

I. Regular Papers

Attacks on Blockchain

TendrilStaller: Block Delay Attack in Bitcoin 1
Matthew Walck (Carnegie Mellon University), Ke Wang (Carnegie Mellon University), and Hyong S. Kim (Carnegie Mellon University)

Cascading Machine Learning to Attack Bitcoin Anonymity 10
Francesco Zola (Vicomtech), Maria Eguimendia (Vicomtech), Jan Lukas Bruse (Vicomtech), and Raul Orduna Urrutia (Vicomtech)

Hybrid Blockchain Architecture

BlockIPFS - Blockchain-Enabled Interplanetary File System for Forensic and Trusted Data Traceability 18
Emmanuel Nyaletey (Kennesaw State University), Reza M. Parizi (Kennesaw State University), Qi Zhang (IBM Thomas J. Watson Research Center), and Kim-Kwang Raymond Choo (University of Texas at San Antonio)

Hybrid Blockchain Design for Privacy Preserving Crowdsourcing Platform 26
Saide Zhu (Georgia State University), Huafu Hu (Georgia State University), Yingshu Li (Georgia State University), and Wei Li (Georgia State University)

A Hybrid Blockchain Architecture for Privacy-Enabled and Accountable Auctions 34
Harsh Desai (University of Texas at Dallas), Murat Kantarcioglu (University of Texas at Dallas), and Lalana Kagal (Massachussetts Institute of Technology)

Access Control for Electronic Health Records with Hybrid Blockchain-Edge Architecture .44
Hao Guo (University of Delaware), Wanxin Li (University of Delaware), Mark Nejad (University of Delaware), and Chien-Chung Shen (University of Delaware)

Blockchain Tools and Algorithms

Proximity Neighbor Selection in Blockchain Networks .52
Yusuke Aoki (Tokyo Institute of Technology) and Kazuyuki Shudo (Tokyo Institute of Technology)

Lockless Transaction Isolation in Hyperledger Fabric .59
Hagar Meir (IBM Haifa Research Lab), Artem Barger (IBM Haifa Research Lab), Yacov Manevich (IBM Haifa Research Lab), and Yoav Tock (IBM Haifa Research Lab)

Bitcoin Options Pricing Using LSTM-Based Prediction Model and Blockchain Statistics .67
Lun Li (Beijing Jiaotong University), Ali Arab (Pace University), Jiqiang Liu (Beijing Jiaotong University), Jingxian Liu (Beijing Jiaotong University), and Zhu Han (University of Houston)

Contract-Based Approach for Security Deposit in Blockchain Networks with Shards .75
Jing Li (University of Houston), Tingting Liu (Nanjing University of Science and Technology), Dusit Niyato (Nanyang Technological University), Ping Wang (York University), Jun Li (Nanjing University of Science and Technology), and Zhu Han (University of Houston)

Applied Cryptography in Blockchain

zk-AuthFeed: How to Feed Authenticated Data into Smart Contract with Zero Knowledge .83
Zhiguo Wan (Shandong University), Zhangshuang Guan (Shandong University), Yan Zhou (Shandong University), and Kui Ren (Zhejiang University)

Initial Public Offering (IPO) on Permissioned Blockchain Using Secure Multiparty Computation .91
Tzipora Halevi (Brooklyn College), Fabrice Benhamouda (Algorand Foundation), Angelo De Caro (IBM Research), Shai Halevi (Algorand Foundation), Charanjit Jutla (IBM Research), Yacov Manevich (IBM Research), and Qi Zhang (IBM Research)

Breeding Unicorns: Developing Trustworthy and Scalable Randomness Beacons .99
Samvid Dharanikot (University of Vienna), Michael Toft Jensen (Aalborg University), Sebastian Rom Kristensen (Aalborg University), Mathias Sass Michno (Aalborg University), Yvonne-Anne Pignolet (DFINITY), René Rydhof Hansen (Aalborg University), and Stefan Schmid (University of Vienna)

Game Theory in Blockchain

Bitcoin Mining with Transaction Fees: A Game on the Block Size .107
Suhan Jiang (Temple University) and Jie Wu (Temple University)

An Efficient Miner Strategy for Selecting Cryptocurrency Transactions ..116
Saulo Dos Santos (University of Manitoba), Chukwuka Chukwuocha (University of Manitoba), Shahin Kamali (University of Manitoba), and Ruppa K. Thulasiram (University of Manitoba)

Blockchain Dividing Based on Node Community Clustering in Intelligent Manufacturing CPS ..124
Suisheng Li (Guangdong University of Technology), Hong Xiao (Guangdong University of Technology), Hao Wang (Norwegian University of Science and Technology), Tao Wang (Guangdong University of Technology), Jingwei Qiao (Guangdong University of Technology), and Shaofeng Liu (Guangdong University of Technology)

Blockchain Applications

DaiMoN: A Decentralized Artificial Intelligence Model Network ..132
Surat Teerapittayanon (Harvard University) and H.T. Kung (Harvard University)

E^2 C-Chain: A Two-Stage Incentive Education Employment and Skill Certification Blockchain..140
Liu Liyuan (Kennesaw State University), Han Meng (Kennesaw State University), Zhou Yiyun (Kennesaw State University), and Parizi Reza (Kennesaw State University)

A Proposal for Account Recovery in Decentralized Applications ..148
Yanlin Zhu (Rensselaer Polytechnic Institute), Lirong Xia (Rensselaer Polytechnic Institute), and Oshani Seneviratne (Rensselaer Polytechnic Institute)

Ownership Preserving AI Market Places Using Blockchain ..156
Nishant Baranwal Somy (IIT Kharagpur), Kalapriya Kannan (IBM Research), Vijay Arya (IBM Research), Sandeep Hans (IBM Research), Abhishek Singh (IBM Research), Pranay Lohia (IBM Research), and Sameep Mehta (IBM Research)

Blockchain and IoT

ChainSplitter: Towards Blockchain-Based Industrial IoT Architecture for Supporting Hierarchical Storage ..166
Gang Wang (University of Connecticut), Zhijie Shi (University of Connecticut), Mark Nixon (Emerson Automation Solutions), and Song Han (University of Connecticut)

Towards Secure and Decentralized Sharing of IoT Data ..176
Hien Thi Thu Truong (NEC Laboratories Europe), Miguel Almeida (NEC Laboratories Europe), Ghassan Karame (NEC Laboratories Europe), and Claudio Soriente (NEC Laboratories Europe)

TrustChain: Trust Management in Blockchain and IoT Supported Supply Chains ..184
Sidra Malik (University of New South Wales), Volkan Dedeoglu (CSIRO Data61), Salil S. Kanhere (University of New South Wales), and Raja Jurdak (CSIRO Data61)

Blockchain Measurement

Evaluating the Impact of Network Latency on the Safety of Blockchain Transactions .194
Luming Wan (University of Otago), David Eyers (University of Otago), and Haibo Zhang (University of Otago)

A Measurement Study of Bitcoin Lightning Network .202
Yuwei Guo (University of British Columbia, Okanagan Campus), Jinfeng Tong (University of British Columbia, Okanagan Campus), and Chen Feng (University of British Columbia, Okanagan Campus)

On Forks and Fork Characteristics in a Bitcoin-Like Distribution Network .212
Vojislav B. Miši (Ryerson University), Jelena Miši (Ryerson University), and Xiaolin Chang (Beijing Jiaotong University)

DAG-Based Blockchain

Enhancing Blockchain Traceability with DAG-Based Tokens .220
Hiroki Watanabe (NTT Service Evolution Laboratories), Tatsuro Ishida (NTT Service Evolution Laboratories), Shigenori Ohashi (NTT Service Evolution Laboratories), Shigeru Fujimura (NTT Service Evolution Laboratories), Atsushi Nakadaira (NTT Service Evolution Laboratories), Kota Hidaka (NTT Service Evolution Laboratories), and Jay Kishigami (Muroran Institute of Technology)

Properties of the Tangle for Uniform Random and Random Walk Tip Selection .228
Bartosz Kusmierz (Wroclaw University of Science and Technology, IOTA Foundation), William Sanders (IOTA Foundation), Andreas Penzkofer (IOTA Foundation), Angelo Capossele (IOTA Foundation), and Alon Gal (IOTA Foundation)

II. Short Papers

Blockchain Performance Analysis I

A Theoretical Model for Fork Analysis in the Bitcoin Network .237
Yahya Shahsavari (École de Technologie Supérieure), Kaiwen Zhang (École de Technologie Supérieure), and Chamseddine Talhi (École de Technologie Supérieure)

IBFT Liveness Analysis .245
Roberto Saltini (PegaSys & ConsenSys Pty. Ltd.)

Fork Rate-Based Analysis of the Longest Chain Growth Time Interval of a PoW Blockchain .253
Yasukazu Aoki (Picolab Co., Ltd.), Noboru Koshizuka (University of Tokyo), and Hirotsugu Seike (YRP Ubiquitous Networking Laboratory)

Blockchain Performance Analysis II

Effective Scheme against 51% Attack on Proof-of-Work Blockchain with History Weighted Information .261
Xinle Yang (MOAC Blockchain Tech Inc.), Yang Chen (MOAC Blockchain Tech Inc.), and Xiaohu Chen (MOAC Blockchain Tech Inc.)

Data Mining-Based Ethereum Fraud Detection 266
Eunjin (Ej) Jung (University of San Francisco), Marion Le Tilly (Ecole Polytechnique), Ashish Gehani (SRI International), and Yunjie (Charles) Ge (University of San Francisco)

OpBench: A CPU Performance Benchmark for Ethereum Smart Contract Operation Code 274
Amjad Aldweesh (Newcastle University), Maher Alharby (Newcastle University), Maryam Mehrnezhad (Newcastle University), and Aad Van Moorsel (Newcastle University)

Permissioned Blockchain

On Sharding Permissioned Blockchains 282
Mohammad Javad Amiri (University of California Santa Barbara), Divyakant Agrawal (University of California Santa Barbara), and Amr El Abbadi (University of California Santa Barbara)

Traceability in Permissioned Blockchain 286
Tatsuo Mitani (Mitsubishi Chemical Systems, Inc. & Institute of Information Security) and Akira Otsuka (Institute of Information Security)

A Heuristic-Based Private Bitcoin Payment Network Formation Using Off-Chain Links 294
Enes Erdin (Florida International University), Mumin Cebe (Florida International University), Kemal Akkaya (Florida International University), Eyuphan Bulut (Virginia Commonwealth University), and A. Selcuk Uluagac (Florida International University)

A Fully Decentralized Time-Lock Encryption System on Blockchain 302
Wei-Jr Lai (National Taiwan University), Chih-Wen Hsueh (National Taiwan University), and Ja-Ling Wu (National Taiwan University)

Blockchain Protocol

Proteus: A Scalable BFT Consensus Protocol for Blockchains 308
Mohammad M. Jalalzai (Louisiana State University), Costas Busch (Louisiana State University), and Golden G. Richard Iii (Louisiana State University)

CoDAG: An Efficient and Compacted DAG-Based Blockchain Protocol 314
Shu Yang (Shenzhen University), Ziteng Chen (Shenzhen University), Laizhong Cui (Shenzhen University), Mingwei Xu (Tsinghua University), Zhongxing Ming (Tsinghua University), and Ke Xu (Tsinghua University)

Smart Contracts

Deviant: A Mutation Testing Tool for Solidity Smart Contracts 319
Patrick Chapman (Boise State University), Dianxiang Xu (Boise State University), Lin Deng (Towson University), and Yin Xiong (Towson University)

Remote Configuration of Integrated Circuit Features and Firmware Management via Smart Contract .325
Md Nazmul Islam (University of Massachusetts Amherst) and Sandip Kundu (University of Massachusetts Amherst)

Aurora: A Robust and Trustless Verification and Synchronization Algorithm for Distributed Ledgers .332
Federico Matteo Beni (University of Zagreb), Alen Hrga (University of Zagreb), and Ivana Podnar Žarko (University of Zagreb)

Blockchain Applications

Toward a Decentralized, Trust-Less Marketplace for Brokered IoT Data Trading Using Blockchain .339
Shaimaa Bajoudah (Newcastle University & Umm AlQura University), Changyu Dong (Newcastle University, UK), and Paolo Missier (Newcastle University)

Micro-Accreditation for Matching Employer E-Hire Needs .347
Zachary Zaccagni (University of North Texas), Aditya Paul (University of North Texas), and Ram Dantu (University of North Texas)

III. Symposium Papers

Blockchain Enhancement I

BeaconBlocks: Augmenting Proof-of-Stake with On-Chain Time Synchronization .353
Alexander Hartl (TU Wien), Tanja Zseby (TU Wien), and Joachim Fabini (TU Wien)

Token-Based Sharing Control for IPFS .361
Shigenori Ohashi (NTT Service Evolution Laboratories), Hiroki Watanabe (NTT Service Evolution Laboratories), Tatsuro Ishida (NTT Service Evolution Laboratories), Shigeru Fujimura (NTT Service Evolution Laboratories), Atsushi Nakadaira (NTT Service Evolution Laboratories), and Junichi Kishigami (Muroran Institute of Technology)

Blockchain Enhancement II

Decentralized and Collaborative AI on Blockchain .368
Justin D. Harris (Microsoft Research Montreal) and Bo Waggoner (Microsoft Research NYC)

FastChain: Scaling Blockchain System with Informed Neighbor Selection .376
Ke Wang (Carnegie Mellon University) and Hyong S. Kim (Carnegie Mellon University)

Smart Contract Defense through Bytecode Rewriting .384
Gbadebo Ayoade (University of Texas at Dallas), Erick Bauman (University of Texas at Dallas), Latifur Khan (University of Texas at Dallas), and Kevin Hamlen (University of Texas at Dallas)

Blockchain Security and Privacy

A Security Reference Architecture for Blockchains .390
Ivan Homoliak (Singapore University of Technology and Design), Sarad Venugopalan (Singapore University of Technology and Design), Qingze Hum (Singapore University of Technology and Design), and Pawel Szalachowski (Singapore University of Technology and Design)

Scalable Privacy-Preserving Query Processing over Ethereum Blockchain .398
Shlomi Linoy (University of New Brunswick), Hassan Mahdikhani (University of New Brunswick), Suprio Ray (University of New Brunswick), Rongxing Lu (University of New Brunswick), Natalia Stakhanova (University of New Brunswick), and Ali Ghorbani (University of New Brunswick)

Privacy-Preserving and Efficient Multi-Keyword Search over Encrypted Data on Blockchain .405
Shan Jiang (Hong Kong Polytechnic University), Jiannong Cao (Hong Hong Polytechnic University), Julie A. Mccann (Imperial College London), Yanni Yang (Hong Kong Polytechnic University), Yang Liu (Alibaba Group Holding Limited), Xiaoqing Wang (Alibaba Group Holding Limited), and Yuming Deng (Alibaba Group Holding Limited)

SSP: Self-Sovereign Privacy for Internet of Things Using Blockchain and MPC .411
Tiffany Hyun-Jin Kim (HRL Laboratories, LLC) and Joshua Lampkins (HRL Laboratories, LLC)

Blockchain Marketplace

Deterministic Sub-Wallet for Cryptocurrencies .419
Hossein Rezaeighaleh (University of Central Florida) and Cliff C. Zou (University of Central Florida)

C2P2: A Collective Cryptocurrency Up/Down Price Prediction Engine .425
Chongyang Bai (Dartmouth College), Thomas White (Dartmouth College), Linda Xiao (Dartmouth College), Venkatramanan Siva Subrahmanian (Dartmouth College), and Ziheng Zhou (Vechain Foundation Limited)

Toward a Decentralized Marketplace for Self-Maintaining Machines .431
Daniel Miehle (Technical University of Munich, Germany), Matthias M. Meyer (Bundeswehr University Munich, Germany), Andre Luckow (Munich University of Applied Sciences, Germany), Bernd Bruegge (Technical University of Munich, Germany), and Michael Essig (Bundeswehr University Munich, Germany)

BlockSim: Blockchain Simulator .439
Carlos Faria (INESC-ID, Instituto Superior Técnico, Universidade de Lisboa, Blockbird Ventures) and Miguel Correia (INESC-ID, Instituto Superior Técnico, Universidade de Lisboa, Blockbird Ventures)

Blockchain Platform I

ArtChain: Blockchain-Enabled Platform for Art Marketplace .447
Ziyuan Wang (Swinburne University of Technology), Lin Yang (Swinburne University of Technology), Qin Wang (Swinburne University of Technology), Donghai Liu (Swinburne University of Technology), Zhiyu Xu (Swinburne University of Technology), and Shigang Liu (Swinburne University of Technology)

A Decentralized Service-Platform towards Cross-Domain Entitlement Handling .455
Alexander Rech (Graz University of Technology), Christian Steger (Graz University of Technology), and Markus Pistauer (CISC Semiconductor GmbH)

BlockV: A Blockchain Enabled Peer-Peer Ride Sharing Service .463
Panchalika Pal (Indian Statistical Institute) and Sushmita Ruj (Indian Statistical Institute)

A Permissioned Blockchain Based Access Control System for IOT .469
Md. Azharul Islam (Missouri University of Science and Technology) and Sanjay Madria (Missouri University of Science and Technology)

Blockchain Platform II

Ensuring Genuineness for Selectively Disclosed Confidential Data Using Distributed Ledgers: Applications to Rail Wayside Monitoring .477
Matthias Lohr (University of Koblenz-Landau), Jonathan Hund (University of Koblenz-Landau), Jan Jürjens (University of Koblenz-Landau), and Steffen Staab (University of Koblenz-Landau)

Yugala: Blockchain Based Encrypted Cloud Storage for IoT Data .483
Sarada Prasad Gochhayat (Old Dominion University), Eranga Bandara (Old Dominion University), Sachin Shetty (Old Dominion University), and Peter Foytik (Old Dominion University)

EduCoin: a Secure and Efficient Payment Solution for MOOC Environment .490
Lingling Lu (Zhejiang University), Jianhai Chen (Zhejiang University), Zijun Tian (Zhejiang University), Qinming He (Zhejiang University), Butian Huang (Zhejiang University), Yang Xiang (Swinburne University of Technology), and Zhenguang Liu (Zhejiang Gongshang University)

From Oracles to Trustworthy Data On-Chaining Systems .496
Jonathan Heiss (TU Berlin), Jacob Eberhardt (TU Berlin), and Stefan Tai (TU Berlin)

Blockchain-Based Charging Coordination Mechanism for Smart Grid Energy Storage Units .504
Mohamed Baza (Tennessee Tech University), Mahmoud Nabil (Tennessee Tech University), Muhammad Ismail (Texas A&M University at Qatar), Mohamed Mahmoud (Tennessee Tech University), Erchin Serpedin (Texas A&M University at Qatar), and Mohammad Ashiqur Rahman (Florida International University)

Endorsement in Hyperledger Fabric .510
Elli Androulaki (IBM Research–Zurich), Angelo De Caro (IBM Research–Zurich), Matthias Neugschwandtner (IBM Research–Zurich), and Alessandro Sorniotti (IBM Research–Zurich)

AIChain Workshop

A Reputation Management Framework for Knowledge-Based and Probabilistic Blockchains .520.....
Tara Salman (Washington University in St. Louis), Raj Jain (Washington University in St. Louis), and Lav Gupta (University of Missouri)

Blockchain-Based Real Estate Market: One Method for Applying Blockchain Technology in Commercial Real Estate Market .528.....
Sobhan Latifi (Shahid Beheshti University of Tehran), Yunpeng Zhang (University of Houston), and Liang-Chieh Cheng (University of Houston)

LightChain Workshop

Section I

Performance Analysis of a Hyperledger Fabric Blockchain Framework: Throughput, Latency and Scalability .536.....
Murat Kuzlu (Old Dominion University), Manisa Pipattanasomporn (Chulalongkorn University & Virginia Tech), Levent Gurses (Movel, Inc.), and Saifur Rahman (Virginia Tech)

Air Gapped Wallet Schemes and Private Key Leakage in Permissioned Blockchain Platforms .541....
Amanda Davenport (University of Minnesota) and Sachin Shetty (Old Dominion University)

Blockchain Implementation for Analysis of Carbon Footprint across Food Supply Chain .546.....
Denisolt Shakhbulatov (New York Institute of Technology), Arshit Arora (New York Institute of Technology), Ziqian Dong (New York Institute of Technology), and Roberto Rojas-Cessa (New Jersey Institute of Technology)

A Lightweight Blockchain-Based Privacy Protection for Smart Surveillance at the Edge .552.....
Alem Fitwi (Binghamton University), Yu Chen (Binghamton University), and Sencun Zhu (Penn State University)

Section II

Formal Verification of Smart Contracts Using Interface Automata .556.....
Gabor Madl (IBM Research Almaden), Luis Bathen (IBM Research Almaden), German Flores (IBM Research Almaden), and Divyesh Jadav (IBM Research Almaden)

BlendMAS: A Blockchain-Enabled Decentralized Microservices Architecture for Smart Public Safety .564.....
Ronghua Xu (Binghamton University), Seyed Yahya Nikouei (Binghamton University), Yu Chen (Binghamton University), Erik Blasch (US Air Force Research Laboratory), and Alexander Aved (US Air Force Research Laboratory)

Scalable Distributed Random Number Generation Based on Homomorphic Encryption ..572.....
Thanh Nguyen-Van (Ginar Ltd. & Ho Chi Minh University of Technology), Tuan Nguyen-Anh (Ginar Ltd.), Tien-Dat Le (Ginar Ltd.), Minh-Phuoc Nguyen-Ho (Ho Chi Minh University of Technology), Tuong Nguyen-Van (Ho Chi Minh University of Technology), Nhat-Quang Le (Ginar Ltd.), and Khuong Nguyen-An (Ho Chi Minh University of Technology)

Smart Contract-Based Secured Business-to-Consumer Supply Chain Systems ..580.....
Feiyang Qu (Kennesaw State University), Hisham Haddad (Kennesaw State University), and Hossain Shahriar (Kennesaw State University)

Author Index 587 . . . . . .