

2024 IEEE International Conference on Blockchain and Cryptocurrency (ICBC 2024)

**Dublin, Ireland
27-31 May 2024**



**IEEE Catalog Number: CFP24BLO-POD
ISBN: 979-8-3503-1675-9**

**Copyright © 2024 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:	CFP24BLO-POD
ISBN (Print-On-Demand):	979-8-3503-1675-9
ISBN (Online):	979-8-3503-1674-2
ISSN:	2832-8892

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

CURRAN ASSOCIATES INC.
proceedings
.com

TABLE OF CONTENTS

Machine Learning for Data Trust Evaluations in Blockchain-Enabled IoT Systems	1
<i>Rashmi Ratnayake, Madhusanka Liyanage, Liam Murphy</i>	
Smart Donations for Software Development Via Blockchain	3
<i>Yury Yanovich, Yash Madhwal, Igor Maximov</i>	
Biometric Authentication Service on Smart Contract.....	5
<i>Takayuki Suzuki, Ken Naganuma, Kaiho Fukuchi, Takatoshi Ohara</i>	
Blockchain-IoT Demo for Supply Chain Management.....	7
<i>Yash Madhwal, Yury Yanovich</i>	
Enabling Web2-Based User Authentication for Account Abstraction	9
<i>Xinxin Fan, Xueping Yang</i>	
PROOF: Decentralized Platform for Verifiable Outsourced Computation.....	11
<i>Spiros Grigoriatos, Katerina Doka, Nectarios Koziris</i>	
Demo: Radio Spectrum Data Collection with Distributed-Proof-of-Sense Blockchain Network	13
<i>Pramitha Fernando, Madhusanka Liyanage</i>	
Demonstrating a Hyperledger Fabric-Based Blockchain with Knowledge Graphs for a Supply Chain Ecosystem	15
<i>Gyan Wickremasinghe, Siofra Frost, Karen Rafferty, Vishal Sharma</i>	
Zk-IoT: Securing the Internet of Things with Zero-Knowledge Proofs on Blockchain Platforms	17
<i>Gholamreza Ramezan, Ehsan Meamari</i>	
Portal: Time-Bound and Replay-Resistant Zero-Knowledge Proofs for Single Sign-On.....	24
<i>Jan Lauinger, Serhat Bezmez, Jens Ernstberger, Sebastian Steinhorst</i>	
Towards a Standard Framework for Blockchain Interoperability: A Position Paper	31
<i>Rafael Belchior, Sabrina Scuri, Nuno Nunes, Thomas Hardjono, André Vasconcelos</i>	
Formalising a Gateway-Based Blockchain Interoperability Solution with Event-B	36
<i>Guzmán Llambias, Laura González, Raúl Ruggia</i>	
An Improved Algorithm to Identify More Arbitrage Opportunities on Decentralized Exchanges	45
<i>Yu Zhang, Tao Yan, Jianhong Lin, Benjamin Kraner, Claudio J. Tessone</i>	
Option Contracts in the DeFi Ecosystem: Motivation, Solutions, & Technical Challenges.....	52
<i>Srisht Fateh Singh, Panagiotis Michalopoulos, Andreas Veneris</i>	
The AMMazing Frontrunner: Practical Frontrunning on the XRP Ledger Automated Market Maker.....	59
<i>Vytautas Tumas, Aanchal Malhotra</i>	
Secure Transmission of Immutable Data for Low-Power, Long-Range Wireless IoT Services	66
<i>Andreas Baumgartner, Nada Akkari, Sudip Barua, Thomas Bauschert</i>	
A Study on Shared Objects in Sui Smart Contracts.....	72
<i>Roman Overko</i>	
SoK: DePIN Data Layer for Modular Blockchain.....	79
<i>Babu Pillai, Vinh Bui</i>	

Name Management Using IOTA in ICN	86
<i>Tepei Okada, Noriaki Kamiyama</i>	
SoK: DAG-Based Consensus Protocols	93
<i>Mayank Raikwar, Nikita Polyanskii, Sebastian Müller</i>	
A2C Reinforcement Learning for Cryptocurrency Trading and Asset Management.....	111
<i>Changhoon Kang, Jongsoo Woo, James Won-Ki Hong</i>	
Using Machine Learning for Predicting Arbitrage Occurrences in Cryptocurrency Exchanges	118
<i>Kristína Okasová, Kristián Košťál</i>	
Buy Crypto, Sell Privacy: Investigating the Cryptocurrency Exchange Evonax.....	125
<i>Alexander Brechlin, Jochen Schäfer, Frederik Armknecht</i>	
Trusted LLM Inference on the Edge with Smart Contracts.....	132
<i>Rabimba Karanjai, Weidong Shi</i>	
Towards a Trusted and Cryptocurrency-Enabled Decentralized Wireless Community Network	139
<i>Sungmin Choi, Zhuochen Xie, Tat Woo Tan, Yifan Liu, Yongqi Wu, Xingjun Wang</i>	
Performance Analysis of Decentralized Physical Infrastructure Networks and Centralized Clouds.....	146
<i>Jan Von Der Assen, Christian Killer, Alessandro De Carli, Burkhard Stiller</i>	
Proliferation of the Service-Centric Distributed Consensus Model and Its Impact on Ethereum	152
<i>David Guzman, Dirk Trossen, Trinh Viet Doan, Joerg Ott</i>	
A Low-Volatility Strategy Based on Hedging a Quanto Perpetual Swap on BitMEX.....	158
<i>Daniel Atzberger, Toshiko Matsui, Robert Henker, Willy Scheibel, Jürgen Döllner, William Knottenbelt</i>	
Unlocking DeFi Literacy: Understanding NFT Market Microstructure in the Decentralized Finance Landscape.....	163
<i>Sampad Sikder, Mashiat Amin Farin, Md. Ariful Islam, Tahlil Tahlil, Meah Tahmeed Ahmed</i>	
Bitcoin Inscriptions: Foundations and Beyond.....	168
<i>Ningran Li, Minfeng Qi, Qin Wang, Shiping Chen</i>	
Central Bank Digital Currency (CBDC): Design Requirements & Challenges	173
<i>Babu Pillai, Golam Sorwar</i>	
Detection of NFT Duplications with Image Hash Functions.....	178
<i>Arad Kotzer, Mostafa Naamneh, Ori Rottenstreich, Pedro Reviriego</i>	
Towards Proxy Staking Accounts Based on NFTs in Ethereum	185
<i>Viktor Valaštín, Roman Bitarovský, Kristián Košťál, Ivan Kotuliak</i>	
SoK: Cryptocurrency Wallets – a Security Review and Classification Based on Authentication Factors	192
<i>Ivan Homoliak, Martin Perešíni</i>	
Completely FROST-Ed: IoT Issued FROST Signature for Hyperledger Fabric Blockchain.....	200
<i>Mostafa Khattat, Roland Kromes</i>	
Gas-Efficient Decentralized Random Beacons.....	205
<i>V. P. Abidha, Togzhan Barakbayeva, Zhuo Cai, Amir Kafshdar Goharshady</i>	

An Untraceable Credential Revocation Approach Based on a Novel Merkle Tree Accumulator.....	210
<i>Nacereddine Sitouah, Francesco Bruschi, Francesco Lorenzo Pallotta, Riccardo Mencucci, Donatella Sciuto</i>	
Decentralised Redactable Blockchain: A Privacy-Preserving Approach to Addressing Identity Tracing Challenges.....	215
<i>Jun Wook Heo, Gowri Ramachandran, Raja Jurdak</i>	
Playing the MEV Game on a First-Come-First-Served Blockchain.....	220
<i>Burak Öz, Jonas Gebele, Parshant Singh, Filip Rezabek, Florian Matthes</i>	
Shared Send Mixers Untangling in Bitcoin Clustering Heuristics Adjustment.....	225
<i>Nikolay Larionov, Yury Yanovich</i>	
Quick Order Fairness: Implementation and Evaluation.....	230
<i>Christian Cachin, Jovana Micic</i>	
BakUP: Automated, Flexible, and Capital-Efficient Insurance Protocol for Decentralized Finance.....	235
<i>Srisht Fateh Singh, Panagiotis Michalopoulos, Andreas Veneris</i>	
A Blockchain-Based Decentralized and Incentive Compatible Distributed Computing Protocol.....	240
<i>Conor McMenamin, Vanesa Daza</i>	
ROAR: A Benchmark for NFT Rarity Meters.....	245
<i>Dmitry Belousov, Maksim Shuklin, Alexander Stepin, Yury Yanovich</i>	
Verifiable Querying Framework for Multi-Blockchain Applications.....	250
<i>Stanly Wilson, Kwabena Adu-Duodu, Yinhao Li, Ringo Sham, Ellis Solaiman, Omer Rana, Rajiv Ranjan</i>	
VELLET: Verifiable Embedded Wallet for Securing Authenticity and Integrity.....	254
<i>Hiroki Watanabe, Kohei Ichihara, Takumi Aita</i>	
Multi-Party Cross-Chain Asset Transfers.....	259
<i>André Augusto, Rafael Belchior, Andre Vasconcelos, Miguel Correia, Thomas Hardjono</i>	
Bridging BRC-20 to Ethereum.....	264
<i>Qin Wang, Guangsheng Yu, Shiping Chen</i>	
ShardingSim: A Modular Committee-Based Sharding Blockchain Simulator.....	273
<i>Yuehua Wu, Yunxiao Wang, Feihu Yan, Wenzhi Chen</i>	
Fast, Favorable, and Fair Blockchain-Based Exchange of Digital Goods Using State Channels.....	279
<i>Matthias Lohr, Sven Peldszus, Jan Jürjens, Steffen Staab</i>	
Towards a Harmonized Global Regulation: An Analysis of the MiCA Regulation and Its Implications for the European Crypto-Asset Market.....	288
<i>Cristina Carata, William J. Knottenbelt</i>	
Blockchain Smart Contract Vulnerability Detection and Segmentation Using ML.....	290
<i>Sabbir Ahmed, Luay Abdeljaber, Sharif Noor Zisad, Mohammad Shahadat Hossain, Latifur Khan</i>	
Incident Analysis of Decentralized Finance.....	293
<i>Cheng-Chieh Lin, Chia-Cheng Tsai, Shih-Wei Liao</i>	

A Universal System for OpenID Connect Sign-Ins with Verifiable Credentials and Cross-Device Flow.....	296
<i>Felix Hoops, Florian Matthes</i>	
Stability Analysis of Market-Making Mechanisms for Decentralized Cryptocurrency Exchanges	299
<i>Yean-Fu Wen, Chien-Ming Huang</i>	
Hierarchical Execution of Cross-Shard Transactions with Multiple Smart Contract Functions.....	302
<i>Hiroshi Matsuura, Takayuki Fujii</i>	
Global, Robust and Comparable Digital Carbon Assets.....	305
<i>Sadiq Jaffer, Michael W Dales, Patrick Ferris, Derek Sorensen, Thomas Swinfield, Robin Message, Srinivasan Keshav, Anil Madhavapeddy</i>	
Compliance Design Options for Offline CBDCs: Balancing Privacy and AML/CFT.....	307
<i>Panagiotis Michalopoulos, Odunayo Olowookere, Nadia Pocher, Johannes Sedlmeir, Andreas Veneris, Poonam Puri</i>	
What Drives the (In)stability of a Stablecoin?.....	316
<i>Yujin Potter, Kornrapat Pongmala, Kaihua Qin, Aria Klages-Mundt, Philipp Jovanovic, Christine Parlour, Arthur Gervais, Dawn Song</i>	
LIMBOCOIN: on the Denial-Of-Service of Token Based Retail CBDCs.....	325
<i>Aditya Ahuja, Siddhasagar Pani, Srujana Kanchanapalli, R Vigneswaran, M A Rajan, Sachin Lodha</i>	
Exploring the Market Dynamics of Liquid Staking Derivatives (LSDs).....	334
<i>Xihan Xiong, Zhipeng Wang, Qin Wang</i>	
How Does Stake Distribution Influence Consensus? Analyzing Blockchain Decentralization.....	343
<i>Shashank Motepalli, Hans-Arno Jacobsen</i>	
Financially-Stable Automated Market Making for Decentralized Fixed-Rate Lending and Trading.....	353
<i>Tuan Tran, Duc A. Tran, Khanh Truong</i>	
CypherChain: A Privacy-Preserving Data Aggregation Framework for Blockchain-Based DR Programs.....	362
<i>Samuel Karumba, Volkan Dedeoglu, Raja Jurdak, Salil S. Kanhere</i>	
Towards the Optimization of Gas Usage of Solidity Smart Contracts with Code Mining	365
<i>Avik Banerjee, Carl Egge, Stefan Schulte</i>	
Better Clients, Less Conflicts: Hyperledger Fabric Conflict Avoidance	368
<i>Bing-Jie Ji, Tung-Wei Kuo</i>	
From Slow Propagation to Partition: Analyzing Bitcoin Over Anonymous Routing	377
<i>Nazmus Sakib, Simeon Wuthier, Kelei Zhang, Xiaobo Zhou, Sang-Yoon Chang</i>	
Optimizing Block Propagation in Bitcoin Network with Region-Based Neighbor Selection Using Reinforcement Learning	386
<i>Wonseok Choi, Euidong Jeong, Jongsoo Woo, James Won-Ki Hong</i>	
DecentPeeR: A Self-Incentivised & Inclusive Decentralized Peer Review System.....	394
<i>Johannes Gruendler, Darya Melnyk, Arash Pourdamghani, Stefan Schmid</i>	
Delay Towers to Bootstrap Blockchains.....	397
<i>Shashank Motepalli, Hans-Arno Jacobsen</i>	

SolMover: Feasibility of Using LLMs for Translating Smart Contracts	400
<i>Rabimba Karanjai, Lei Xudagger, Weidong Shi</i>	
Is Wireless Bad for Consensus in Blockchain?	403
<i>Seungmo Kim</i>	
Altruism, Reciprocity, and Tokens to Reward Forwarding Data: is that Fair?	406
<i>Vahid Heidaripour Lakhani, Arman Babaei, Leander Jehl, Georgy Ishmaev, Vero Estrada-Galiñanes</i>	
Unpacking How Decentralized Autonomous Organizations (DAOs) Work in Practice.....	416
<i>Tanusree Sharma, Yujin Potter, Kornrapat Pongmala, Henry Wang, Andrew Miller, Dawn Song, Yang Wang</i>	
CredAct: Privacy-Preserving Activity Verification for Benefits Schemes in Self-Sovereign Identity	425
<i>Rahma Mukta, Hye-Young Paik, Qinghua Lu, Salil S. Kanhere</i>	
End-To-End Verifiable Decentralized Federated Learning.....	434
<i>Chaehyeon Lee, Jonathan Heiss, Stefan Tai, James Won-Ki Hong</i>	
Protecting Non Fungible Mutable Tokens: An Application in the Metaverse	443
<i>Damiano Di Francesco Maesa, Francesco Donini, Paolo Mori, Laura Ricci</i>	
Energy-Efficient Data Anchoring for IoT Devices	452
<i>Seyed Amid Moeinzadeh Mirhosseini, Stefan Craß, Bernhard Uhl, Leander B. Hörmann, Christian Kastl</i>	
An Ensemble Method of Deep Reinforcement Learning for Automated Cryptocurrency Trading	461
<i>Shuyang Wang, Diego Klabjan</i>	
Second Layer Network Impact on Bitcoin Mining Fees and Network Value.....	464
<i>Saulo Dos Santos, Japjeet Singh, Bakhshish Singh Dhillon, Ruppa K. Thulasiram, Shahin Kamali</i>	
PrivHChain: Monitoring the Supply Chain of Controlled Substances with Privacy-Preserving Hierarchical Blockchain	467
<i>Hyeonbum Lee, Kyuhwan Lee, Wenyi Tang, Shankha Shubhra Mukherjee, Jae Hong Seo, Taeho Jung</i>	
Privacy-Preserving Account-Abstraction for Teams on EVM Chains.....	476
<i>Thierry Sans, David Ziming Liu</i>	
How to Redact the Bitcoin Backbone Protocol	485
<i>Enrique Larraia, Mehmet Sabir Kiraz, Owen Vaughan</i>	
A Tip for IOTA Privacy: IOTA Light Node Deanonymization Via Tip Selection	494
<i>Hojung Yang, Suhyeon Lee, Seungjoo Kim</i>	
Strategic Bidding Wars in On-Chain Auctions	503
<i>Fei Wu, Thomas Thiery, Stefanos Leonardos, Carmine Ventre</i>	
Efficient and Reliable Service Detection on Bitcoin	512
<i>Vincent Jacquot, Nada Hammad, Benoit Donnet</i>	
Private, Anonymous, Collateralizable Commitments Vs. MEV.....	521
<i>Conor McMenamin, Vanesa Daza</i>	

Abstracting Bitcoin Lightning Network Complexity with Ultraviolet	528
<i>Davide Patti, Salvatore Monteleone, Enrico Russo, Maurizio Palesi, Vincenzo Catania</i>	
Bytecode Skeletons for Sample Selection in the Analysis of Blockchain Programs	531
<i>Monika Di Angelo, Gernot Salzer</i>	
Monero Traceability Heuristics: Wallet Application Bugs and the Mordinal-P2Pool Perspective	540
<i>Nada Hammad, Friedhelm Victor</i>	
Lock-Free Concurrent Smart Contracts.....	549
<i>Zachary Painter, Damian Dechev</i>	
Enhanced Mutation Testing of Smart Contracts in Support of Code Inspection	558
<i>Sebastian Banescu, Morena Barboni, Andrea Morichetta, Andrea Polini, Edward Zulkoski</i>	
(In)Correct Smart Contract Specifications	567
<i>Derek Sorensen</i>	
Icon: Automated Verification of Inter-Transaction Properties in Tezos Smart Contracts with Unknowns.....	576
<i>Yuki Nishida, Kohei Suenaga, Atsushi Igarashi</i>	
Towards a Deeper Understanding of the Cardano Macro-Economics.....	585
<i>Mostafa Chegenizadeh, Sheng-Nan Li, Claudio J. Tessone</i>	
Rational Economic Behaviours in the Bitcoin Lightning Network	594
<i>Andrea Carotti, Cosimo Sguanci, Anastasios Sidiropoulos</i>	
A Two-Stage Encrypted Cryptomining Traffic Detection Mechanism in Campus Network	602
<i>Haoran Sun, Ruisheng Shi, Lina Lan, Zhiyuan Peng, Chenfeng Wang</i>	
Gasless On-Chain Password Manager: A Comparative Analysis Across EVM-Based Platforms	611
<i>Tahlil Tahlil, Syead Tanvir Islam Movin, Sania Azhmee Bhuiyan, Mahabub Alahi</i>	
SRNG: An Efficient Decentralized Approach for Secret Random Number Generation.....	615
<i>Togzhan Barakbayeva, Zhuo Cai, Amir Kafshdar Goharshady</i>	
ZkGen: Policy-To-Circuit Transpiler.....	620
<i>Jan Lauinger, Jens Ernstberger, Sebastian Steinhorst</i>	
Short Paper: Unpredictable Transaction Arrangement for MEV Mitigation in Ethereum.....	625
<i>Jan Droll, Oliver Stengele, Hannes Hartenstein</i>	
Analysis of Earned Rewards in a Blockchain with Two Selfish Miners	630
<i>Sheng-Wei Wang</i>	
The Spatiotemporal Scaling Laws of Bitcoin Transactions.....	635
<i>Lajos Kelemen, István András Seres, Ágnes Backhausz</i>	
Decentralized Commit-Reveal Scheme to Defend Against Front-Running Attacks on Decentralized EXchanges.....	640
<i>Nakhoon Choi, Heeyoul Kim</i>	
ML2SC: Deploying Machine Learning Models as Smart Contracts on the Blockchain	645
<i>Zhikai Li, Steve Vott, Bhaskar Krishnamachari</i>	

Machine Learning in DeFi: Credit Risk Assessment and Liquidation Prediction	650
<i>Georgios Palaiokrassas, Sandro Scherrers, Eftychia Makri, Leandros Tassiulas</i>	
Enhancing Ethereum PoA Clique Network with DAG-Based BFT Consensus	655
<i>Yongrae Jo, Chanik Park</i>	
Integrating Behavioral Finance Factors with Temporal Convolutional Networks for Enhanced Cryptocurrency Return Predictions	660
<i>Jiacheng Fu, Marco Mandolfo, Giuliano Noci</i>	
Enhancing Coin Selection in UTXO-Based Blockchains Through Modified Greedy Algorithms.....	665
<i>Manvir Schneider</i>	
Congesting Ethereum After EIP-1559.....	667
<i>Kianoush Arshi, Amir Kafshdar Goharshady</i>	
Servicifying zk-SNARKs Execution for Verifiable Off-chain Computations	670
<i>Alvaro Alonso Domenech, Jonathan Heiss, Stefan Tai</i>	
ContractSafeguard: Practical Bug Bounty Platform for Smart Contracts with Intel SGX	672
<i>Kaiho Fukuchi, Ken Naganuma, Takayuki Suzuki, Takatoshi Ohara</i>	
An Evaluation of Lightweight CNNs for Smart Contract Vulnerability Detection	675
<i>Iqra Mustafa, Alan McGibney, Susan Rea</i>	
Leveraging Machine Learning for Multichain DeFi Fraud Detection	678
<i>Georgios Palaiokrassas, Sandro Scherrers, Iason Ofeidis, Leandros Tassiulas</i>	
Bitcoin, Gold, Oil Implied Volatility Spillover to Stock Market: Evidence from an Asymmetric Quantile Regression Model	681
<i>Toshiko Matsui, William J. Knottenbelt</i>	
Dynamically Available Consensus on a DAG with Fast Confirmation for UTXO Transactions	684
<i>Nikita Polyanskii</i>	
An Incentivization Scheme for a Fixed-Supply DLT with No Base Token Fees.....	687
<i>Olivia Saa, Andrew Cullen, Luigi Vigneri</i>	
POSTER: Towards an Identity Authentication Layer in CBDC Networks Using Self-Sovereign Identities	690
<i>João Pedro Alonso Almeida, Rodrigo Dutra Garcia, Gowri Ramachandran, Jó Ueyama</i>	
Support Remote Attestation for Decentralized Robot Operating System (ROS) Using Trusted Execution Environment	693
<i>Qian Wang, Brian Lee, Yuansong Qiao</i>	
SoK: Crosschain Token Bridges and Risk.....	696
<i>Uri Lee</i>	
SoK: Compression in Rollups	712
<i>Roshan Palakkal, Jan Gorzny, Martin Derka</i>	
Cryptoeconomics and Tokenomics as Economics: A Survey with Opinions.....	729
<i>I T O Kensuke</i>	
Pragmatic Analysis of Key Management for Cryptocurrency Custodians	747
<i>Yuto Takei, Kazuyuki Shudo</i>	

SoK: Public Blockchain Sharding 766
Md Mohaimin Al Barat, Shaoyu Li, Changlai Du, Y. Thomas Hou, Wenjing Lou

FATF Travel Rule’s Technical Challenges and Solution Taxonomy..... 784
Yuto Takei, Kazuyuki Shudo

Author Index