

2025 Crypto Valley Conference (CVC 2025)

**Rotkreuz, Switzerland
5-6 June 2025**



**IEEE Catalog Number: CFP25P12-POD
ISBN: 979-8-3315-8750-5**

**Copyright © 2025 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:	CFP25P12-POD
ISBN (Print-On-Demand):	979-8-3315-8750-5
ISBN (Online):	979-8-3315-8749-9

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

2025 Crypto Valley Conference (CVC) CVC 2025

Table of Contents

Conference Organization	vii
Sponsors	ix

AI, Applications, and Smart Contracts

AI Oracle: A Blockchain-Powered Oracle for LLMs and AI Agents	1
<i>Shange Fu (APRO Research, Australia) and Min Xie (APRO Research, Singapore)</i>	
Are you a DePIN? A Decision Tree to Classify Decentralized Physical Infrastructure Networks	11
<i>Michael S. Andrew (Who Loves Burrito?, USA) and Mark C. Ballandies (University of Zurich & WiHi, Switzerland)</i>	
Short Paper: SlotCollider - Detecting Storage Slot Collisions in Ethereum Smart Contracts	17
<i>Muhammad Umar Janjua (NextKore Ltd.), Abeeha Fatima (NextKore Ltd.), Muhammad Waiz Khan (NextKore Ltd.), Muhammad Danish Bilal (NextKore Ltd.), Talha Ahmad (NextKore Ltd.), and Maha Ayub (NextKore Ltd.)</i>	
Short Paper: Implementing Swap Contracts on Blockchain Networks	21
<i>Arad Kotzer (Technion - Israel Institute of Technology) and Ori Rottenstreich (Technion - Israel Institute of Technology)</i>	

Cryptoeconomics and Tokens

How May Bitcoin Mining Reduce Carbon Emission?	25
<i>Ioannis Bellos (George Mason University, USA), Jiasun Li (George Mason University, USA), and Hang Ren (George Mason University, USA)</i>	
Comprehensive Modeling Approaches for Forecasting Bitcoin Transaction Fees: A Comparative Study	27
<i>Jiangqin Ma (Georgia Institute of Technology, USA) and Erfan Mahmoudinia (Blockonomics, Iran)</i>	
Short Paper: A Low-Latency System for Collecting Massive Crypto Option Tick Data from Deribit	40
<i>Daniel Atzberger (University of Potsdam, Germany), Robert Henker (German Deep Tech Quantum GmbH, Germany), Jan Ole Vollmer (German Deep Tech Quantum GmbH, Germany), André Holdschick (German Deep Tech Quantum GmbH, Germany), Willy Scheibel (University of Potsdam, Germany), and Jürgen Döllner (University of Potsdam, Germany)</i>	

Identity, Governance, and Usability

Governance of Ledger-Anchored Decentralized Identifiers	44
<i>Sandro Rodriguez Garzon (Technische Universität Berlin / T-Labs, Germany), Carlo Segat (Technische Universität Berlin / T-Labs, Germany), and Axel Küpper (Technische Universität Berlin / T-Labs, Germany)</i>	
SoK: A Taxonomy for Distributed-Ledger-Based Identity Management	56
<i>Awid Vaziry (Technische Universität Berlin / T-Labs, Germany), Sandro Rodriguez Garzon (Technische Universität Berlin / T-Labs, Germany), Patrick Herbke (Technische Universität Berlin / T-Labs, Germany), Carlo Segat (Technische Universität Berlin / T-Labs, Germany), and Axel Küpper (Technische Universität Berlin / T-Labs, Germany)</i>	
Short Paper: Requirements and Benefits of a DAO Tokenomics Framework	81
<i>Florian Spychiger (Zurich University of Applied Sciences, Switzerland), Sabrina Wollenschläger (Zurich University of Applied Sciences, Switzerland), Matthias Hafner (Swiss Economics, Switzerland), and Nicolas Oderbolz (Swiss Economics, Switzerland)</i>	

Cryptographic Protocols, Attacks and Tools

Verifiable Weighted Secret Sharing	86
<i>Kareem Shehata (National University of Singapore), Fangqi Han (National University of Singapore), and Sri AravindaKrishnan Thyagarajan (University of Sydney)</i>	
Short Paper: Decentralized Fair Exchange for Assets across Blockchain and the Internet	102
<i>Long Chen (Institute of Software Chinese Academy of Sciences), Yuguo Liu (Institute of Software Chinese Academy of Sciences), Yuan Lu (Institute of Software Chinese Academy of Sciences), and Qiang Tang (The University of Sydney)</i>	
Dyna-hinTS: Silent Threshold Signatures for Dynamic Committees	106
<i>Aniket Kate (Purdue University), Pratyay Mukherjee (Supra Research), Samipa Samanta (Indian Institute of Technology Bombay), and Pratik Sarkar (Supra Research)</i>	
Timelock Shield: A Robust Defense Against MEV and Censorship Attacks in Blockchain	127
<i>Saksham Agrawal (Indian Institute of Technology Bombay, India; Hyperbots Inc., India) and Vinay J. Ribeiro (Indian Institute of Technology Bombay, India)</i>	
User Perceptions of Cryptocurrency Attacks – Extended Abstract	138
<i>Zsofia Baruwaa (University of Kent, UK), Sanjay Bhattacharjee (University of Kent, UK), Sahil Rey Chandnani (University of Kent, UK), and Zhen Zhu (University of Kent, UK)</i>	

Author Index	155
--------------------	-----