IEEE Conference on Blockchain and Cryptocurrency (ICBC'23)

Moayad Aloqaily, MBZUAI, UAE and Vinayaka Pandit, IBM India Research Lab, India, TPC Co-Chairs

It is a great pleasure for us to write this brief report for the fifth IEEE Conference on Blockchain and Cryptocurrency (ICBC'23) on behalf of the entire Technical Program Committee of the conference, organizing committee, and the steering committee of the conference. The conference, held at Sofitel-Dubai between May 1st and May 5th of 2023, was very successful, with 120 participants and 694 authors from 37 countries. Dubai provided the perfect background for a conference on Blockchain, as it aims to become the first city to truly decentralize the governance through its Dubai Blockchain Strategy (https://www.digitaldubai.ae/initiatives/blockchain) and the vibrant blockchain startup ecosystem in the city.

The objective of the conference remains the same as when it was started: to foster state of the art research in the fast-changing field of blockchain and cryptocurrency through a program consisting of topical keynotes and panel discussions, research papers, posters, SoKs, demos, and tutorials. In this report, we shall provide a brief overview of the technical highlights of the conference.

In response to the call for papers inviting submissions for full research papers, short research papers, and posters, we received a total of 266 submissions. In total, the submitted papers accounted for 694 authors from 37 countries. The strength of the technical program committee was 175 members. The submissions were managed on the EDAS system. The review process, which lasted eight weeks, consisted of two phases: In the first phase, we ensured that each submitted paper received at least three high-quality reviews and ordered the papers based on the average score they received across all the reviews that they received. This was followed by a meeting of the technical program committee (TPC), in which the TPC chairs presented an objective method to accept the papers into different categories based on the review scores. In the second phase, the reviews were made available to the authors for a period of one week to post their rebuttal followed by a week for the reviewers to revise their reviews. Finally, the papers were accepted into different categories based on the method outlined during the TPC meeting. Through this process, we accepted 33 full research papers, 25 short research papers, 27 posters, five SoKs, and 10 demos. The distribution of the authors from different countries and the most used keywords are shown in the figure below. We accepted four proposals for tutorials through a separate call for proposals. The conference also featured two technical workshops: CrossChain and CryptoEx.

After the selection of the contributed program as described above, we invited three leading researchers from the field to deliver keynotes on the most important topics for the community. Further, three panel discussions on the most actively debated topics in the community were also identified. Thus, the program consisting of keynotes, panel discussions, full research papers, short research papers, posters, demos, SoKs, and tutorials was spread across five days, from May 1st to May 5th. They were presented through a total of 17 technical presentation sessions. The detailed program is available on the conference web page (https://icbc2023.ieee-icbc.org/). In what follows, we will provide the highlights of the technical program.

Day 1 (May 1, 2023)

The conference got off to a brisk start on May 1st with four tutorials in the morning session. The topics of the tutorials were:

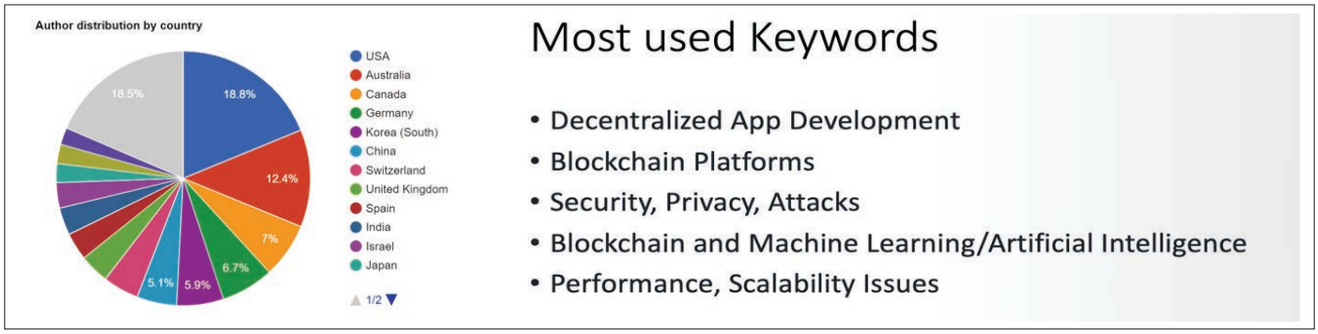
- Machine Economy: from theory to practice—given by researchers from IoTex and Kent State University.
- Cross chain communication through authenticated queries on EVM based chains—given by Dr. Damiano Di Francesco Maesa from University of Pisa, Italy.
- Executing a blockchain based confidential application in minutes—given by researchers from iExec.
- Self-sovereign identity and decentralization in identity management: opportunities and challenges—given by researchers from University of New South Wales, Australia.

The afternoon of May 1st had two short paper sessions with each short paper presented for 15 minutes. The first session focused on privacy, security, and identity. The second session focused on cryptocurrencies, non-fungible token (NFT), and prediction markets. This clearly showed that the community is focusing on research issues that are relevant to the real-life systems that are being built, especially the emergence of NFTs in the last two years, namely, the privacy and identity issues that have arisen in the context of multi-party collaboration, and the use of blockchain to implement decentralized decision making.

Day 2 (May 2, 2023)

The conference was formally inaugurated on the second day, May 2nd. During this session, we announced six candidate papers for the best paper award. These papers were selected based on the aggregate scores from the reviews. The final decision would be based on the review scores and presentation. The morning session featured the first keynote, given by Prof. Davor Svetinovi (Khalifa University, UAE). Professor Svetinovic's talk was titled, "Blockchain Turbulences: from trust to censorship resistance." He delivered the talk based on three pieces of work that were carried out by his team, and connected them to the broader themes on decentralizing the trust and achieving censorship resistance. The second day also featured a panel discussion on, "Blockchain for Post-Quantum AI and security: How much help it may bring?" This panel discussion was moderated by Prof. Adel Ben Mnaouer. The panelists were Prof. Davor Svetinovic, Dr. Vinayaka Pandit (IBM Research), and Mr. Siddarth Banerjee (Kondola Networks). The panel discussed what components of today's blockchain system design could be exposed to risk in the post-quantum era, whether there is a need to adopt post-quantum cryptography in the short-term, and the issues that arise in using AI on blockchain networks. The panel discussion indicated that the threat of quantum computing does not warrant adopting post-quantum cryptography right away, although the panelists advised to keep an eye on the progresses in the field. The panelists highlighted the need to preserve privacy while enabling multi-party AI, and the availability of emerging tools to handle the challenges.

The second day featured three full paper sessions. The first focused on issues related to decentralized databases, analytics, and visualizations. In this session, the papers focused on decentralized database synchronization and a centralized database with multi-party control. One of the highlights of this session was the paper on smart contract data monitoring and visualization by Seng Kuang Yap et al. This paper was a candidate for the best paper award. The paper presented a framework to monitor the data pertaining to smart contract executions with the aim of providing performance insights, anomaly detection, and identification of operational risks. The second session focused on blockchain applications, featuring talks on blockchain for voting, custodial wallets, and fair exchange protocol for vehicle passports. Compared to previous years, the application sessions represented a progression in the sense that it featured topics



that are highly relevant for the new classes of applications that are being built today, for example, custodial wallets. The third full paper session focused on the security aspects with three presentations ranging from mitigating lives attacks in DAG-based ledgers, blockchain-based framework for delegation of cyber threat intelligence, and solution to detect and thwart pump&dump attacks on cryptocurrencies.

Apart from the full paper sessions, the second also featured a demo session and a poster session. The demo session had five demos on contract wallets, blockchain-based grrenhouse gas emission reporting and verification, blockchain-based financing, connecting smart devices to smart contracts, and network analysis. The poster session featured five posters on topics like privacy enabled enterprise data sharing, improving reputation management, proof of learning consensus, distributed randomness generation, and zero-knowledge proof based off-chain compute and storage.

Day 3 (May 3, 2023)

Day three featured three full paper sessions, two poster sessions, a SoK paper session, a Demo session, a keynote, and a panel discussion. The keynote on day three was given by Prof. Stefan Tai (photo attached) of Technical University of Berlin on, "Repurposing but Uncompromising the Blockchain." The keynote elaborated on/off-chain awareness (along and beyond the lines of oracles and layer two solutions) allowing to achieve a meaningful, secure, and trustworthy interplay of blockchains with non-blockchain components. The speaker discussed their work on ZoKrates, using ZKPs for verifiable off-chain computations as one example for tackling said challenges through a reshaped understanding of blockchain transactions and a concerted interplay of on- and off-chain components. Day three also featured a thought-provoking panel discussion on, "CBDCS - Will They Ever Happen? When? In what form?" This panel discussion was moderated by Dr. Moayad Aloqaily (MBZUAI University, Abu Dhabi, UAE), Dr. Hoda A. Alkhzaimi, (Assistant Professor, Director, Center of Cyber Security NYUAD, President of Emirates Digital Association for Women), and Alia Al-Saadawi, (Researcher at American University Sharjah, UAE). The discussion explored the following aspects: the current state of development of CBDCS as well as their challenges and applications.

On day 3, during the SoK paper session, five SoK papers were presented featuring various topics, including scalability techniques for BFT consensus, taxonomy of machine learning on Blockchain, and Anonymity of Lightweight Clients in Cryptocurrency Systems.

The first full paper session of day three featured talks on blockchain and crypto applications. The second session of day three was focused on blockchain protocols, such as consensus protocols. The third full paper session of day three focused also on blockchain applications, such as transaction fees, Byzantine Fault Tolerant services, and frontrunning in the XRP ledger and storage for blockchain.

Day three featured a first poster session with five posters on topics like token fees, PoW, Bitcoins, SLA monitoring for 6G, blockchain sharding, Ethereum Gas usage, and smart contract.

The second poster session with five posters focused on topics like Hyperledger fabric, credential revocation, flying AdHoc Network (FANET), Bitcoin, and attack detection.

Day three featured a Demo session with five demos focus-

FIGURE 1. Opening and poster sessions.

FIGURE 2. Panel.

FIGURE 3. Keynote speaker: Stefan Tai.

ing on various topics, including Demonstrating Low Cost SIM Bluetooth Token for Generation Of Ethereum Transactions, NFT SMASH: Game to Test Your NFT Rarity Sense, B4B.World: Decentralized Influencer Marketing Platform, a Blockchain-based Data Sharing Marketplace with a Federated Learning Use Case, and DeMonitor: Monitoring Decentralization in Blockchains using BigQuery.

Day 4 (May 4, 2023)

Day four featured three full paper sessions, one poster session, a keynote, and a panel discussion. The keynote on day four was given by Prof. Adnan Imeri (Luxembourg Institute of Science and Technology) on, "Blockchain as an Enabler Technology of Self-Sovereign Identities and Verifiable Credential". Professor Imeri could not be present in Dubai and delivered the keynote virtually. The keynote elaborated on how blockchain can enable self-sovereign identity (SSI) and verifiable credential (VC). The talk explored the technical challenges and the transformational potential of SSI and VC. Day four also featured a thought provoking panel discussion on, "Are Private Blockchains Dead?" This panel discussion was moderated by Prof. Salil Kanhere and the panelists were Prof. Burkhard Stiller (University of Zurich), Mr. Artem Barger (Eternyze IT Services), and Prof. Deepak Puthal (Khalifa University, Dubai). The discussion explored the following aspects: do private blockchain networks satisfy basic needs of decentralization, need of private blockchains in enterprise and regulatory settings, and does innovation in private blockchains match that of public blockchains. The panel discussion seemed to indicate that while the private blockchain lack some of essential decentralization aspects of public blockchains, they cater to some unique requirements in the enterprise and regulatory domain. One of the panelists highlighted that applications like Central Bank Digital Currency (CBDC) required private blockchain approach. Thus, the panel concluded that while the public blockchain will continue to attract majority of the innovation talent, the private blockchain will evolve in its own way guided by the enterprise and regulatory requirements.

The first full paper session on day four featured talks on Decentralizing Web Services, Miner Extractable Value (MEV)-resistant blockchain design, and agent based modeling of Ethereum consensus. The second session on day four was focused on applications ranging from privacy-preserving review system, trust management for resource sharing on 6G-IoT, and a blockchain agnostic interoperability framework. The third full paper session of day four featured two candidates of best paper award. It featured talks on highly scalable layer two network design, atomic state sharding for account-based blockchains, and an intriguing talk that examined the occurrence of the Braess paradox in layer two payment networks. It featured the paper, "SREP: Out-Of-Band Sync of Transaction Pools for Large-Scale Blockchains," by Noval Boskov et al., which was a candidate for the best paper award. The paper modeled the problem of transaction synchronization outside of block propagation channel. The paper presented a graph-theoretic formulation and presented a formal proof of its convergence. The paper also demonstrated the empirical benefits of achieving transaction synchronization outside block propagation channel. This session also featured, "Goldfish: Peer selection using Matrix completion in unstructured P2P network," by Bowen Xue et al—another candidate for the best paper award. This paper formulated the problem of peer selection in unstructured P2P networks as a problem of matrix completion and presented a streaming algorithm for the same. The paper presented a convincing empirical evidence of the efficacy of their new approach.

Day four featured a poster session with five posters on topics like improved liquidity provisioning, internet of energy systems, blockchain for heterogenous TEEs, Decentralized Function as a services (DFaaS), and CAP theorem from cryptocurrencies.

FIGURE 4. Best Paper Award: Young Choon Lee

At the end of day four, the best paper award was announced. The TPC chairs and the general chairs made sure that at least two of them attended the presentation of each of the candidates. The papers were rated based on the aggregate review scores and the scores for the presentation. In evaluating the presentations, the committee considered the clarity of the presentation, clear elucidation of the importance of the problem and results, and the effectiveness of addressing audience questions. As it turned out, there were two compelling choices with different characteristics. One was a practice paper demonstrating its applicability in system deployments and another with core theoretical contributions. Considering their contrasting nature, the committee felt it appropriate to recognize both the papers as the joint-winners of the Best Paper awards. The joint-winners of the best paper award were:

1. Smart Contract Data Monitoring and Visualization
   Authors: Seng Kuang Yap (Aglive Research, Australia), Zhongli Dong (The University of Sydney, Australia), Mark Toohey (Aglive Lab, Australia), Young Choon Lee (Macquarie University, Australia), and Albert Zomaya (The University of Sydney, Australia)
2. SREP: Out-Of-Band Sync of Transaction Pools for Large-Scale Blockchains
   Authors: Novak Boskov (Boston University, USA), Sevval Simsek (Boston University, USA), Ari Trachtenberg (Boston University, USA), and David Starobinski (Boston University, USA)

The certificates for the Best Paper winners were given by the steering committee chair Prof. James Hong from POSTECH, Korea.

Day 5 (May 5, 2023)

Day five featured two full-day workshops: The International Conference on Blockchain and Cryptocurrency Crosschain Workshop (Crosschain Workshop 2023) and the first International Workshop on Cryptocurrency Exchanges (CryptoEx 2023). Cryptoex workshops featured three technical sessions, two poster sessions, a short paper session, and a keynote. The keynote was given by Dr. Zayeed Al Hemairy (Innovation & Blockchain Advisor, Dubai, UAE).

The first technical Cryptoex session on day five, with three papers, featured talks on concemtrated liquidity AMM DEX, decentralized exchanges, and liquidity technology.

The second technical session in Cryptoex workshop, counted four papers. It featured talks on centralized crypto markets, algorithmic Stablecoin, crypto assets, and crypto exchanges.

The third technical session in Cryptoex workshop, counted four papers. It featured talks on Web3 applications, NFT, and tokenized carbon credits.

On day five, Cryptoex workshop a first poster session with four posters focusing on various topics, including trades between centralized and decentralized exchanges, AI-enabled blockchain, NFT, and federated learning.

Cryptoex short paper session on day five featured four presentations on centralized web3 and crypto exchanges, as well as price arbitrage.

On day five, the workshop Crosschain featured three technical sessions. The first session presented four papers on various topics, including crosschain risk framework, bridge aggregations in a multi-chain, and Crosschain function calls. The second session, with four papers, featured topics including secure bridges and secure asset transfer protocol. The third session, with three papers, featured topics like CBDC, Hyperledger fabric, and XCMP.