

The 8th International Conference on
Application Intelligence and Blockchain
Security (AIBlock)

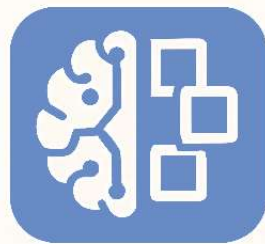
AIBlock 2026
24-27 July 2026



AIBlock 2026

Organized by

Lancaster University, UK



AIBlock

Application Intelligence
and Blockchain Security
Conference

Conference Schedule

08:45-16:00	Conference Period	
24 July, 2026	Friday	Online Link
08:45-09:00	Welcome and Opening	
Keynote Session Session Chair: Liqun Chen / Weizhi Meng		
09:00-09:40	Keynote 1	Prof. Xiapu Luo
09:40-10:20	Keynote 2	Dr. Guosheng Hu
10:20-11:00	Keynote 3	Prof. Man Ho Au
11:00-11:10	Event Break	
Session 1: LLM and Federated Learning Security Session Chair: Vyron Karpourakis		
11:10-11:25	Option-QNet: LLM-Driven Tail Risk Quantification for Options Pricing	Ruiqi Lin, Dianxin Wang, Jialu Wang, Zishen Peng and Jun Zheng
11:25-11:40	Knowledge-to-Data: LLM-Driven Synthesis of Structured Network Traffic for Testbed-Free IDS Evaluation	Konstantinos Karpourakis, Vyron Karpourakis, Efstratios Chatzoglou, Georgios Kambourakis and Stefanos Gritzalis
11:40-11:55	VCFedAdam: A Verifiable and Compressed FedAdam Aggregation Scheme for Federated Learning	Zhiwei Si, Chen Zhang, Xiuheng Liao, Chunhua Su and Ziang Wu
11:55-12:10	Sensitive Watermark Embedding for Trustworthy Inference in Vision-Language Models	Yanxi Lv, Chuanwenxi Zhou, Yiwen Wu, Wanlei Zhou, Yu-an Tan, Ning Shi and Mengxia Ren

12:10-13:30	Lunch Break	
Session 2: Communication Security and Big Data Session Chair: Shuailin Yang		
13:30 - 13:45	Toward Lattice-Based Gated Opening for Threshold Traceability in End-to-End Encrypted Messaging	Ting Ye and Jiageng Chen
13:45 - 14:00	A Lightweight Hybrid Framework for Malicious PE File Detection and Risk-Level Assessment	Rui Li, Shitong Wang and Ning Shi
14:00 - 14:15	Lattice-based Secure Sharing Mechanisms in Big Data	Hongfei Zhu, Qikun Zhang, Yajie Wang, Ning Shi and Hongyi Liu
14:15 - 14:30	Performance Improvements of ZK-Prover for rWasm: A Sound and Efficient AIR for 32-bit Division and Remainder	Mehmet Sabir Kiraz, Suleyman Kardas, Dmitry Savonin, Yao Wang and Aliaksei Dziadziuk
14:30 - 14:40	Event Break	
Session 3: Blockchain and Cyber-physical System Security Session Chair: Hongbo Wang		
14:40 - 14:55	Leveraging Consensus Protocols in a Consortium Blockchain for Radioactive Waste Tracking	Jingjie Tu, Weizhi Meng, Lei Wang, and Zhongming Zhang
14:55 - 15:10	Physics-Informed Dual-Stream Ranking for Maritime Anomalies under Interval-Aware Evaluation	Zheng Zhu and Wenjuan Li
15:10-15:25	Detection, Validation and Analysis of Deepfaking in Social Media	Cole Ouellette, Brian Almaguer, Xiaoyan Sun and Jun Dai
15:25-15:40	An Improved KGIN-based Recommendation Model with Multi-Head Attention and Contrastive Learning	Yuanyuan Yang, Qiongxin Liu and Ning Shi
15:50-16:00	Closing Session	

AIBlock 2026

25 July, 2026	Saturday
10:00-16:00	AI Workshop (by Invitation)
27 July, 2026	Sunday
Whole Day	Leaving

Keynote Information:



Daniel Xiapu Luo is a Professor at the Department of Computing and the Director of Research Centre for Blockchain Technology of The Hong Kong Polytechnic University. His research focuses on Blockchain and Smart Contracts Security, Mobile and IoT Security, and Network Security with significant publications in top-tier venues. His research led to more than ten best/distinguished paper awards, including ACM CCS'24 Distinguished Paper Award, ACM SIGSOFT Distinguished Paper Awards in ICSE'24, ISSTA'22 and ICSE'21, Best DeFi Papers Award 2023, Best Paper Award in INFOCOM'18, Best Research Paper Award in ISSRE'16, etc.

He received the BOCHK Science and Technology Innovation Prize (FinTech) for his contribution to blockchain security. He is listed among World's Top 2% Scientists by Stanford University. He is a member of HKMA CBDC Expert Group and an associate editor for IEEE/ACM Transactions on Networking, IEEE Transactions on Dependable and Secure Computing and ACM Transactions on Privacy and Security.

Title: Illuminating the Dark Forest: Understanding, Surviving, and Discovering MEV in DeFi

Abstract:

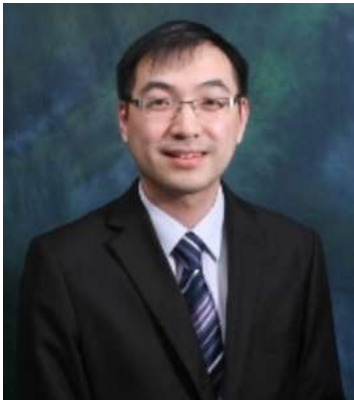
Maximal Extractable Value (MEV) has given rise to a competitive and adversarial ecosystem in decentralized finance, where sophisticated bots exploit transaction ordering for profit. In this talk, I will present our recent studies that collectively illuminate the MEV landscape — from profiling bot strategies and defending against MEV attacks to discovering MEV opportunities at scale.



Guosheng Hu is a senior lecturer of AI at University of Bristol. Additionally, he holds the title of Honorary Professor of Practice at Queen's University Belfast. Before that, he served as the Head of Research at Oosto (a leading visual AI company). Prior to his role at Oosto, he was a Research Fellow in the LEAR team at INRIA Grenoble Rhone-Alpes, France. Dr. Hu earned his PhD under the supervision of Prof. Josef Kittler at the University of Surrey, UK. His expertise lies in the intersection of computer vision and efficient AI.

Title: Reduce AI's Carbon Footprint - Accelerating Deep Learning Models

Abstract: AI-driven data centres, operating continuously and predominantly powered by fossil fuels, contribute significantly to global greenhouse gas emissions (2.5-3.7%). The widespread use of large foundation models such as ChatGPT exacerbates this environmental impact. This talk explores strategies for mitigating AI's carbon footprint through model acceleration, aiming to significantly reduce computations while maintaining the accuracy of AI models. This session will spotlight various model acceleration techniques, including Neural Architecture Search, Model Pruning and Quantisation, and others. Beyond academic advancements, the talk will also delve into successful industrial applications. Last, it will outline potential future research directions in the field of model acceleration.



Man Ho Allen Au is Professor and Associate Head (Research & Development) in the Department of Computing at The Hong Kong Polytechnic University, where he also serves as Director of the Research Centre for Blockchain Technology. He is also an Honorary Professor in the Department of Computer Science at The University of Hong Kong. His research spans applied cryptography, privacy-enhancing technologies, and secure decentralized systems, with a particular focus on zero-knowledge proofs and privacy-preserving mechanisms for regulated digital currencies and compliant DeFi. He serves on the Hong Kong Monetary Authority CBDC Expert Group.

Prof. Au is a two-time ZPrize winner and a laureate of the BOCHK Science and Technology Innovation Prize in FinTech. He has also served the international research community in several leadership roles, including as General Chair of ASIACRYPT 2026, RAID 2023, and ACM ASIACCS 2021, and Associate Editor of IEEE Transactions on Dependable and Secure Computing. His work aims to bridge cryptographic research with real-world deployment, strengthening trust and privacy in the digital economy.

AIBlock 2026

Title: The Privacy Paradox: Reconciling Anonymity and Regulation in Digital Currencies

Abstract: As regulated digital currencies and institutional Decentralised Finance mature, blockchain systems face a persistent tension: protecting user privacy while enabling lawful oversight. This “Privacy Paradox” is often framed as a forced choice between bank-style surveillance and crypto-style opacity. This presentation argues that such a trade-off is unnecessary. By deploying modern cryptographic primitives such as Linkable Ring Signatures and Zero-Knowledge Proofs, it is possible to architect “privately accountable” systems that preserve anonymity while supporting targeted auditability.

The discussion highlights three advancements: (1) a post-quantum linkable ring signature scheme that hardens digital identities against future quantum threats; (2) a scalable construction offering logarithmic signature size and rapid verification to mitigate blockchain bloat; and (3) lessons from Project Aurum 2.0, a retail CBDC prototype for the e-HKD pilot, which demonstrates ZKP-based anonymity within a regulatory sandbox. Together, these results provide a compliant, scalable, and privacy-preserving blueprint for the future of digital money.