北京大学前沿计算研究中心
Center on Frontiers of Computing Studies, Peking University

静园5号院
前沿讲座

Cryptography in Blockchains and Their Applications

Prof. Man Ho Au

Department of Computing
Hong Kong Polytechnic University

Host: 邓小铁 讲席教授
2023年9月19日 星期二 19:00
静园五院204室

Abstract

Conceptualized 12 years ago as a core component of Bitcoin, blockchain has gained a vast amount of interest. Informally speaking, a blockchain is a distributed, shared, and immutable ledger that maintains a growing list of ordered records. It became extremely popular among the industries in the last few years. Many companies are exploring applications of blockchain beyond cryptocurrencies.

In this talk, the speaker will discuss the role of cryptography in blockchains, and why it is crucial. He will also highlight some of the latest development in this area. Topics covered include variants of digital signatures, threshold cryptosystems, anonymous credentials, zero-knowledge proofs, and post-quantum cryptography. Finally, we will conclude the talk with challenges related to the adoption of blockchain technologies and insights developed from our experience.

Biography

Prof. Man Ho Au is a Full Professor at the Department of Computing of The Hong Kong Polytechnic University. Before that, he was an Associate Professor in the Department of Computer Science at the University of Hong Kong. His research interests include information security, cryptography, blockchain technology, and their applications. He has published over 200 refereed papers in top journals and conferences, including CRYPTO, ASIACRYPT, ACM CCS, NDSS, IEEE S&P, SIGMOD, SOSP, IEEE TIFS, IEEE TDSC, and others. He is a recipient of the 2009 PET runner-up award for outstanding research in privacy-enhancing technologies. His team won the ZPrize - Open Division Plonk-DIZK GPU Acceleration prize, which came with a cash award of 550K USD. He has served as a program committee/general chair of several international conferences, including ACM ASIACCS, RAID, SECURECOM, ISPEC, PROVSEC, among others. Currently, he is an associate editor of IEEE Transactions on Dependable and Secure Computing, Journal of Information Security and Applications, and an editorial board member of the Journal of Cryptologic Research.