Wireless Communications and Mobile Computing

WILEY | Hindawi

Special Issue on

Emerging Technologies towards Improving Confidentiality and Privacy in Blockchain

CALL FOR PAPERS

Blockchain, originally applied in bitcoin and other cryptocurrencies, is a decentralized, public, and immutable ledger which is used to record the process of transactions and digital asset by applying decentralization and cryptographic technologies. Since it provides traceability, transparency, and tradability, blockchain is a promising and revolutionary technology and has been used into various application fields (e.g., finance, e-health, IoT, etc.). Since its decentralization and trustless nature, blockchain technology has leaded to new opportunities and benefit businesses. According to ReportLiner, the global market size of blockchain is expected to grow from USD 3.0 billion in 2020 to USD 39.7 billion by 2025, at a dramatic compound annual growth rate (CAGR) of 67.3% during 2020-2025. The advent of blockchain and related technologies are changing economics.

Being different from public-key infrastructure where a public key is bound with an identity by a certificate generated by a central authority, a user generates her secret-public key pair and uses it independently without any authentication due to the decentralization feature of blockchain. Furthermore, due to the transparency feature, transaction details and address are public visible in blockchain. However, transaction details and address are sensitive in some application scenarios, such as smart contract, e-health, e-government, etc. Additionally, to protect privacy, some technologies were adopted (e.g., pseudonym) while malicious uses abused it to conduct illegal transactions without being identified (e.g., ransom). With the popularity of blockchain, security and privacy issues have been the primary concerns of blockchain users.

This Special Issue aims to bring together original research and review articles discussing new techniques and methods which can be applied to improve transactions' confidentiality and users' privacy in blockchain. We welcome submissions discussing how to support availability and accountability. In addition, research mentioning techniques and methods which support privacy-preserving computing and balance the relationship between privacy and accountability are also considered.

Potential topics include but are not limited to the following:

- Access control in blockchain
- Accumulator in blockchain
- Anonymous credential in blockchain
- Attribute-based encryption in blockchain
- Consensus algorithm in blockchain
- Group signature in blockchain
- Homomorphic encryption in blockchain
- Multi-signature in blockchain
- Multiple party computation in blockchain
- Privacy-preserving authentication in blockchain
- Pseudonym in blockchain
- Ring signature in blockchain
- Zero-knowledge proof in blockchain
- Zero-knowledge succinct non-interactive arguments of knowledge (zk-SNARKs) in blockchain
- Unlinkability in blockchain

Authors can submit their manuscripts through the Manuscript Tracking System at https://review.hindawi.com/submit?specialIssue=328048.

Papers are published upon acceptance, regardless of the Special Issue publication date.

Lead Guest Editor
Jinguang Han, Nanjing University of Finance and Economics, Nanjing, China
jghan22@gmail.com

Guest Editors
Liqun Chen, University of Surrey, Guilford, UK
liqun.chen@surrey.ac.uk

Li-Quan Chen, Southeast University, Nanjing, China
lqchen@seu.edu.cn

Willy Susilo, University of Wollongong, Wollongong, Australia
wsusilo@uow.edu.au

Submission Deadline
Friday, 14 January 2022

Publication Date
June 2022