Chen WG, Si XM. Special section on blockchain and cryptocurrency systems. JOURNAL OF COMPUTER SCIENCE AND TECHNOLOGY 33(3): 531–532 May 2018. DOI 10.1007/s11390-018-1837-0

Preface

Recently there has been a burst of interest in blockchain and cryptocurrencies, which blends computer science, finance and business in unprecedented ways. Multiple computer science areas, including cryptography, distributed systems, programming languages, game theory, and system security techniques, are involved and today's blockchain and cryptocurrency systems still face security, availability, scalability and performance issues. This special section is an effort to encourage and promote research on this area from the computer architecture and software perspective.

The goal of this special section is to present the state-of-the-art and high-quality original research papers in the area of computer architecture and systems on blockchain and cryptocurrencies. It receives 9 submissions. After two rounds of rigorous reviewing, 4 papers are accepted and included in this special section, which covers different perspectives of privacy in blockchain, as well as a digital evidence preservation system on Bitcoin.

Practical Constant-Size Ring Signature

Privacy has been one of the main concerns in the system similar to Bitcoin. Ring signature is a good method for those users who need better anonymity in cryptocurrency. The size of ring signature is one of the dominating parameters, and constant-size ring signature (where signature size is independent of the ring size) is much desirable.

In paper "Practical Constant-Size Ring Signature", Qin *et al.* solve this open question. They present a new constant-size ring signature scheme based on bilinear pairing and accumulator, which is provably secure under the random oracle (RO) model.

ShadowEth: Private Smart Contract on Public Blockchain

This paper is also on the privacy issues of public blockchain and it focuses on the smart contract solutions in Ethereum-like systems.

In paper "ShadowEth: Private Smart Contract on Public Blockchain", Yuan *et al.* present ShadowEth, a system that leverages hardware enclave to ensure the confidentiality of smart contracts while keeping the integrity and availability based on existing public blockchains like Ethereum. ShadowEth establishes a confidential and secure platform protected by Trusted Execution Environment (TEE) off the public blockchain for the execution and storage of private contracts. It only puts the process of verification on the blockchain.

Scalable and Privacy-Preserving Data Sharing Based on Blockchain

This paper is the third one to address the privacy issues on blockchain. It tries to address the issue of preserving privacy with multi-party data.

In paper "Scalable and Privacy-Preserving Data Sharing Based on Blockchain", Zheng *et al.* propose a trusted data sharing scheme using blockchain. They use blockchain to prevent the shared data from being tampered, and use the Paillier cryptosystem to realize the confidentiality of the shared data.

Lightweight and Manageable Digital Evidence Preservation System on Bitcoin

An effective and secure system used for evidence preservation is essential to possess the properties of anti-loss, anti-forgery, anti-tamper as well as perfect verifiability. The decentralized blockchain network is qualified as a

perfect platform for its secure anonymity, irrevocable commitment and transparent traceability.

In paper "Lightweight and Manageable Digital Evidence Preservation System on Bitcoin", Wang *et al.* present a lightweight digital evidence-preservation architecture which possesses the features of privacy-anonymity, audit-transparency, function-scalability and operation-lightweight on Bitcoin.

Acknowledgement

We would like to thank all the authors for their contributions, including those whose manuscripts were not accepted. Our special thanks also go to the reviewers for their valuable time and thorough evaluation of the manuscripts. We appreciate the Editor-in-Chief, Professor Guo-Jie Li, for hosting this special section in the Journal of Computer Science and Technology (JCST). We are also very grateful to the editorial office staff of JCST for their excellent work during the course of preparation for this special section.

Leading Editor:

Wen-Guang Chen, Professor, Department of Computer Science and Technology, Tsinghua University, Beijing
cwg@tsinghua.edu.cn

Guest Editor:

Xue-Ming Si, Professor, Shanghai Key Laboratory of Data Science, Fudan University, Shanghai
sxm@fudan.edu.cn

Wen-Guang Chen is a professor in the Department of Computer Science and Technology, Tsinghua University, Beijing, where he has been teaching since 2003. He received his B.S. and Ph.D. degrees both in computer science from Tsinghua University in 1995 and 2000 respectively. His research interest is in parallel and distributed computing. He is a CCF distinguished member and a CCF distinguished speaker, and an ACM member and the vice chair of ACM China Council. He has served in program committees of a variety of major conferences in the parallel and distributed computing area, including PLDI, PPoPP, SC, CGO, CCGrid, IPDPS, APSys, and ICPP. He is the editor-in-chief of Communication of ACM China Edition.

Xue-Ming Si is the deputy director of Shanghai Key Laboratory of Data Science, Fudan University, Shanghai, and a professor in the Department of Computer Science and Technology, Fudan University, Shanghai. His research interest includes cryptography, high-performance computing and blockchain. He has served as the chairman of a variety of major conferences on blockchain, network security and high-performance computing. He was awarded the First Class Prize of the National Science and Technology Progress Award of China three times and has received special government allowance from the State Council since 2001.