Exploring New Frontiers in Blockchain: Proof-of-Stake, Scalability, and More

Speaker: Dr. Hong-Sheng Zhou
Computer Science Department, Virginia Commonwealth University
Friday, April 19, 2019
1-2PM, T3

Abstract

Cryptocurrencies like Bitcoin and Ethereum have proven to be a phenomenal success. The underlying techniques hold a huge promise to change the future of financial transactions, and eventually our way of computation and collaboration. At the heart of the Bitcoin system is a blockchain, that records transactions between users in consecutive time windows. The blockchain is maintained in the open network environment i.e., the Internet, by a peer-to-peer network of nodes called Bitcoin miners via the so-called proof-of-work mechanism.

In this talk, I will start with a brief review of Bitcoin's proof-of-work based consensus design, and then I will demonstrate the main challenges and new frontiers in blockchain research. After that, we will present new solutions to these challenges.

---

First, we will discuss how to mimic Bitcoin's design via alternative mechanisms such as proof-of-stake. Despite the fact that proof-of-stake related mechanisms have been intensively investigated for constructing blockchain protocols in the past years, several major issues remain. I will present a pure proof-of-stake based consensus called “iChing” to illustrate our approach to addressing these issues, with the goal of constructing blockchain protocols in the open and large-scale network setting.

---

Second, we will discuss how to improve the performance of blockchain protocols. I will demonstrate a new framework called “BackPackers” to illustrate our ideas to improve the throughput and reduce the confirmation time. Our protocols, outperforming existing ones, are the first large-scale (i.e., > 1000 nodes), high-throughput (i.e., > 3000 tps), blockchain, most importantly supporting smart contracts.
--- Finally, if time permits, I will also discuss how to enable effective governance in blockchain protocols, and demonstrate some applications on top of blockchain.

Some results in this talk are based on my joint work with Thang Dinh, Lei Fan, Jonathan Katz, and Phuc Thai. No cryptography background is assumed.

**Biography**

Hong-Sheng Zhou is an Assistant Professor in the Computer Science Department at Virginia Commonwealth University, and a scientist and co-founder of Fractal Platform, a new blockchain startup. Hong-Sheng was a postdoc at Maryland Cybersecurity Center, as a recipient of NSF Computing Innovation Fellowship, under the direction of Jonathan Katz. Before that, he received his PhD at the University of Connecticut with Aggelos Kiayias as advisor.

Hong-Sheng is working on multiple directions in cryptography including Secure Computing (Multi-Party Computation, Blockchain Technologies, Voting, Functional Encryption and Obfuscation, Verifiable Computation), and Extreme Cryptography (Leakage/Tampering Resilience, Klepto Resilience, Quantum Resilience). He has published a number of papers in top cybersecurity and distributed computing conferences, such as CRYPTO, EUROCRYPT, CCS, and PODC. Hong-Sheng’s research has been funded by NSF and multiple industry awards.