Moving off the blockchain: a payment hub for fast, anonymous off-chain Bitcoin payments

Speaker: Dr. Foteini Baldimtsi  
Computer Science Department, George Mason University  
Friday, Jan 25, 2019  
1PM – 2PM, T3

Abstract

In this talk I will focus in two major technical challenges faced by Bitcoin today: (1) scaling Bitcoin to meet increasing use, and (2) protecting the privacy of payments made via Bitcoin. To address these challenges, I will present TumbleBit, a unidirectional unlinkable payment hub that uses an untrusted intermediary, the Tumbler, to perform off the blockchain transactions. TumbleBit allows to scale the volume and velocity of bitcoin-backed payments while being fully compatible with today's Bitcoin protocol. At the same time, Tumblebit offers anonymity to the transactions routed through the Tumbler, guaranteeing that no-one, not even the Tumbler, can link a payment from its payer to payee. I will explain how a combination of cryptographic tools and blockchain properties is used to make Tumblebit work and discuss how these techniques are relevant beyond Bitcoin.

Biography

Dr. Foteini Baldimtsi is an Assistant Professor in the Computer Science Department at George Mason University. She received her Ph.D. from Brown University in May 2014 and worked as a postdoctoral researcher in Boston University and University of Athens. Her research interests are in the areas of cryptography, security and data privacy. She focuses on designing provably secure cryptographic schemes for a variety of applications such as privacy preserving identity management, secure electronic payments and private and scalable blockchain transactions. She is a recipient of an IBM faculty award and her research is supported by NSF and the Zcash Foundation.