Digital Digital currencies enable transactions that are electronically authorized, cleared and settled. After decades of research and several failed business ventures attempting to establish a digital currency, Bitcoin—a secure and distributed protocol using public blockchain—was proposed and deployed in 2009. While still in its infancy, Bitcoin has achieved unprecedented success, enjoying a multi-billion dollar market capitalization and deployment by large retailers. In this presentation, we focus on explaining how Bitcoin protocol internally works, including secure transactions, public ledger, proof of work and distributed consensus. We also discuss issues related to anonymity and privacy, and present some open research problems in the Bitcoin protocol.

Dr. Gaby Dagher is an assistant professor in the Department of Computer Science at Boise State. He received his Ph.D. in Computer Science from the Department of Computer Science and Software Engineering at Concordia University, his Master of Applied Science in Information Systems Security from Concordia Institute for Information Systems Engineering (CIISE), and his Bachelor of Computer Science from Concordia University. His research interests are in Cyber-security, with emphasis on information security and privacy, applied cryptography, data mining, digital currencies and cloud computing.