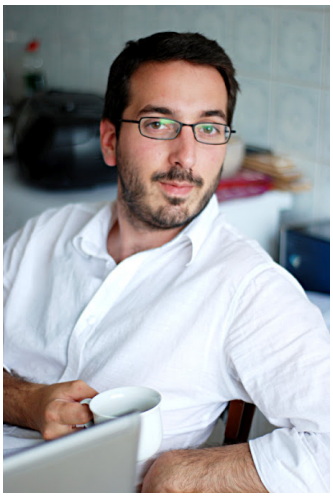

George Danezis

g.danezis@ucl.ac.uk
http://danez.is
@GDanezis

Decentralisation as a privacy-enhancing technology

Wednesday, June 1 2016, 09.30 - 11.00

Bitcoin and modern crypto-currencies have rekindled a wider interest in peer-to-peer disintermediated architectures both for high-integrity but also for privacy. The EU NEXTLEAP project in particular aims to leverage decentralization to build privacy-friendly key management, instant messaging and email. However, decentralization, besides benefits also brings costs and hidden assumptions that need to be accommodated. In this talk I will survey key decentralized privacy systems from the past 15 years, and attempt to draw lessons about how they employ decentralization: what they gain from it; but also what they lose and have to painstakingly re-engineer; as well as what remains, sometimes covertly, centralized. I will relate those designs with important contemporary distributed ledger problems, and reflect on how a focus on high-integrity, verifiability and auditability may provide a way forward – but also how it can be antithetical to the sought privacy.