Computer Science Colloquium

# Building secure distributed systems atop the insecure Internet

|EDFioz.gf/

Host: Anurag Khandelwal

## Monday March 25, 2021
## 10:30 a.m.
## Speaker: Maria Apostolaki

### Zoom Presentation

**Abstract:** Distributed systems are increasingly important for our everyday life, allowing for high performance, fault tolerance, and flexibility. Many of these systems nowadays rely on the inherently insecure Internet infrastructure. Surely though, they should have been designed to take this into account…?

In this talk, I will answer negatively to this question using a concrete example: public blockchain systems such as Bitcoin. These are novel distributed systems that are designed according to stringent failure models. In this context, I will explain how an adversary controlling pieces of Internet infrastructure can practically compromise: (i) Bitcoin's consensus protocol (by partitioning the network); (ii) Bitcoin's anonymity guarantees (by mapping pseudonyms to real-world identities); and (iii) Bitcoin's availability (by eclipsing clients).

While these attacks are worrying, I will also introduce practical and effective defenses to counter them both at the network and the application layer. Beyond Bitcoin, this work teaches essential lessons for distributed-system design.

**Bio:** Maria Apostolaki is a PhD Student at ETH Zurich advised by Laurent Vanbever. During her studies, she has been a visiting student at MIT (2019) and a research intern at Microsoft Research (2018) and Google (2017). Before joining ETH, she earned her diploma in Electrical and Computer Engineering at the National Technical University of Athens, Greece.

Her research focuses on building secure, performant, and deployable networked systems using both hardware and software. Her research led to discovering significant vulnerabilities in the Bitcoin system and spearheaded changes to the Bitcoin codebase. Maria's work received widespread media coverage and was awarded an Applied Networking Research Prize by IETF.

Yale University