



# Department of Computer Science

## Foundations of Blockchain Systems

**Julian Loss**

University of Maryland

Hosted by Iulian Neamtii

**DATE:** Wednesday, February 24, 2021

**TIME:** 2:30 PM - 3:30 PM

**LOCATION:** <https://njit.webex.com/njit/j.php?MTID=m32aeea24b047d60aa4e01ea2064b2f06>

<https://cs.njit.edu/seminars>

**Abstract:** One of the most successful applications of modern cryptography has been its use in electronic and digital payment systems. In traditional systems, a trusted authority handles all payments (e.g., a bank or a credit card company). More recently, blockchain systems have emerged as a trust-free and increasingly popular alternative. In a blockchain system, users jointly emulate the trusted authority by running a distributed protocol to agree on the transaction history of users (i.e., the blockchain). Making blockchain systems a secure and scalable environment poses many new and fascinating challenges that require solutions from both cryptography and distributed computing. In my talk, I will explain the different areas of my research and their importance as components that make up a blockchain system. For each of these areas, I will also list some of the open questions that I plan to work on in the near future.

**Bio:** Julian Loss obtained his MSc in computer science from ETH Zurich in 2016 and his Ph.D. from the Ruhr University of Bochum in 2019. He is currently a postdoc at the University of Maryland in the group of Jonathan Katz. His interests include classic cryptographic primitives such as digital signatures and multi-party computation as well as blockchain/consensus protocols.