Computer Science Colloquium

Trust or Decentralize? Balancing Trust and Performance in Decentralized Systems

Host: Zhong Shao

Friday March 11, 2021
10:30 a.m.
Speaker: Karl Wüst

Zoom Presentation

Abstract: In recent years, cryptocurrencies and blockchains have received widespread attention. These systems are generally designed to be decentralized in order to reduce the required trust assumptions as much as possible. However, there are choices to be made about how much to trust and how much to decentralize which in turn greatly affect the properties that can be achieved efficiently.

In this talk, I will discuss how these choices can be leveraged for large performance gains and to achieve new properties in smart contract systems and for privacy-preserving cryptocurrency transactions.

In particular, I will show how smart contract scalability can be improved by executing contracts in smaller committees, while at the same time allowing safe interaction between untrusted contracts. Further, I will show how lightweight blockchain clients for fully anonymous cryptocurrencies can be enabled efficiently, and how privacy and accountability can be balanced in central bank digital currencies.

Bio: Karl Wüst is a PhD Candidate in the System Security Group at ETH Zurich.

His research focuses on the security and privacy of blockchain technology with a particular focus on smart contract scalability and central bank cryptocurrencies. In his research, he combines techniques from cryptography, distributed systems, and trusted computing to balance the trade-off between reducing trust and achieving high performance. His research has been published at top venues in security (CCS, Usenix Security, NDSS) and resulted in multiple patent applications.

Yale University