Computer Science Colloquium

Proof systems for governance, transparency, and privacy

|EDFiozgi/

Host: Zhong Shao

Friday March 2, 2021
4:00 p.m.
Speaker: Benjamin Fisch

Zoom Presentation

Abstract: Record-keeping has long played a critical role in society, from governing property ownership to establishing historical "truth". Today, our dependence on digital records is becoming absolute, from our personal wealth, commerce, and identities to sources of knowledge and news. This has elevated the importance of three competing dimensions: Who has control over how records are managed? Who can verify the integrity of record maintenance? Who can see the information in records? Over the last decade, these questions have sparked the development of digital record-keeping systems called "blockchains".

This talk will cover three proof systems that bring new capabilities for governance, transparency, and privacy in blockchains. I will first talk about new techniques for balancing transparency and privacy that achieve order-of-magnitude efficiency improvements over the prior state of the art. Next, I will talk about two new proof systems pertaining to governance: Verifiable Delay Functions (VDFs) and Proofs-of-Replication (PoReps). VDFs enable an unbiased leader election protocol that will be used within the consensus of Ethereum 2.0. PoReps enable a "permission-less" consensus protocol where voting power is based on data storage capacity instead of Bitcoin's energy-wasteful "proof-of-work". PoReps are deployed in Filecoin, a decentralized storage network exceeding a capacity of two exabytes that secures a cryptocurrency worth over two billion dollars.

Bio: Ben is a PhD candidate at Stanford University advised by Dan Boneh and a recipient of the NSF Graduate Research Fellowship. His research focuses on verifiability in information systems, with special attention on applications of applied cryptography to blockchains. Several of his research results have had an impact on the blockchain industry. His seminal work on Verifiable Delay Functions (VDFs) sparked the VDF Alliance, a multi-million initiative composed of academic, non-profit, and corporate collaborators. VDFs will play an important role in several deployed blockchains including Ethereum.

Yale University