Identity & Trust

on- and off-web

It has been asserted that the web is missing two critical layers of functionality: identity and payment. One can argue that identity is the more fundamental of the two as any robust payment system depends on trustable identities.

Indeed, the lack of widely adopted identity and payment layers on the web have led to the proliferation of surveillance-led business models over the last 25 years. Companies involved in this infer and track identities and monetize them through targeted advertisements. There is now an opportunity for change as a new generation of identity technologies incubated in the W3C and Linux Foundation (among others) come to fruition. Known as self-sovereign or distributed identity (DIDs), and verifiable claims, these technologies attempt to enable a more secure, privacy-respecting web that can span both on-line and off-line environments.

While many of the foundational technologies are in place for the web's identity layer, its adoption is far from certain as it requires a supportive ecosystem, ease-of-use, and the right economic incentives. This course will focus on the intersection of these concerns and explore a wide range of topics from hardware through software and user experience to economics.

The class will be conducted seminar style and involve presentations by students, guest lecturers, discussions, and projects. Some topics of interest are as follows:

- Self-sovereign identity and verifiable claims: deep dive
- Implementing efficient and easy to use hardware and software wallets
- Mapping use-cases to the technology: trade-offs between coverage & complexity
- Issues inherent in a unified approach to people, services, things and data
- Blockchains & distributed ledgers: what role do they play?
- Designing for the real-world: security, usability, scale
- Co-existing with and leveraging legacy identity and security technologies
- Rethinking micropayments: is it different this time?
- Smart contracts: how do we trust a world that runs as code?

The class will meet twice a week for 1.5 hours (3 credits) and will be graded based on engagement (projects, discussions and presentations). There will be a number of projects to choose from but students are encouraged to come up with their own project ideas. Projects and presentations can be done individually or in teams.

Who should attend? Anyone who is interested in complex system design: the cross product of cryptography, user experience, economics, and society. It's ok to care about some aspects more than others. If you have ideas, bring them!