**IC3 2019 Winter Retreat**

February 14-15, 2019 Congress Centre Kursaal Interlaken, Strandbadstrasse 44, 3800 Interlaken, Switzerland

IC3 faculty, students, sponsors and guests gather at IC3 Retreats to discuss the major technical challenges, issues and innovative solutions to widespread blockchain adoption. The 2019 Winter Retreat is in Switzerland with our IC3 colleagues from ETH Zurich and EPFL, as well as all other IC3 campuses (Cornell, Cornell Tech, UC Berkeley, UCL, UIUC, and the Technion).

The Retreat is on February 14-15, and co-located at Interlaken with the [Swiss Blockchain Winter School](https://blockchainschool.epfl.ch) on February 11-14, but is a totally separate event.

Registration for the Retreat is now closed. Please see the agenda below, and check back later for a summary of the event.



Congress Centre Kursaal Interlaken in Interlaken, Switzerland

IC3 Winter Retreat Agenda

|  |  |
| --- | --- |
| **Thursday**    8:00 - 8:45 | Continental Breakfast |
| 8:45 - 9:00 | Welcome - Ari Juels |
| 9:00 - 10:00 | Blockchains at Scale I - 10 minute talks (8 minutes + QA) |
|  | Cristina Basescu - Low-latency and locality-preserving blockchains  Oded Naor - Teechain: A Secure Asynchronous Blockchain Payment Network  Patrick McCorry - Scaling Cryptocurrencies via State Channels  Mustafa Al-Bassam - Replay attacks against cross-shard communication protocols  Yan Ji - Amplification of selfish mining in fraud-proof based blockchains |
| 10:00 - 10:30 | Break - 30 mins |
| 10:30 - 11:10 | Blockchain at Scale II - 10 minute talks (8 minutes + QA) |
|  | Enis Ceyhun Alp - Heterogeneous sharded blockchain architecture  Karl Wust - ZLiTE: Lightweight Clients for Shielded Zcash Transactions using Trusted Execution  Sergi Delgado Segura - TxProbe: Discovering Bitcoin's Network Topology Using Orphan Transactions  Surya Bakshi - Erays: Reverse Engineering Ethereum's Opaque Smart Contracts |
| 11:10 - 12:00 | Start-ups emerging from IC3 - 10 minute talks (8 minutes + QA) |
|  | Sergey Nazarov - Town Crier and Decentralised Oracles  Kevin Sekniqi - Avalanche  Noah Johnson - Oasis Labs  Soumya Basu - bloXroute |
| 12:00 - 13:30 | Lunch |
| 13:30 - 14:30 | Cryptography and Zero Knowledge - 10 minute talks (8 minutes + QA) |
|  | Jiaheng Zhang  & Tiancheng - Faster zero-knowledge interactive proofs  Mary Maller - Improvements to Updatable CRS  Samarth Kulshreshtha - Scaling Asynchronous Multi-Party Computation: A Systems Perspective  Kevin Liao - A Calculus for Composable, Computational Cryptography  Tom Yurek - Client-efficient Asynchronous Verifiable Secret Sharing and Anonymous Broadcast  Krishna Deepak Maram Lun Wang - CHURP: CHUrn-Robust Proactive secret sharing |
| 14:30 - 15:00 | Break - 30 minutes |
| 15:00 - 15:45 | Panel: Too much infrastructure, not enough use-cases/usability studies? |
| 15:45 - 17:00 | Industry and Community Use Cases - 10 minute talks (8 minutes + QA) |
|  | Dahlia Malkhi - Consensus Protocols  Angelo De Caro - Hyperledger Fabric Update  Michael Steiner - Intel and SGX Update  Jorge Cuellar - Siemens  Bob McElrath - Fidelity  Sascha Hanse - Aeternity  Nicola Greco - Protocol Labs  Simon Meier - Digital Asset Holdings  Christine Moy - JP Morgan |
| 17:00 - 18:00 | Networking Reception |
| 18:00 - | Dinner |

|  |  |
| --- | --- |
| **Friday**    7:15 - 8:00 | Continental Breakfast |
| 8:00 – 9:00 | Proof-of-Personhood (Audience Participation Session) |
| 9:00 - 10:00 | Consensus Protocols (Attacks, Defense, Models) - 10 minute talks (8 minutes + QA) |
|  | Kevin Negy & Sishan Long - Selfish Mining  Itay Tsabary - Gap game  Sanket Kanjalkar - “I Can’t Believe It’s Not Stakes”  Jian Liu - Saber: sharding by separating execution from consensus  Ethan Cecchetti - PIES and Proof of Replication  Phil Daian - The Dark Side of Blockchain - HFT, Bribery, Consensus Attacks, and More |
| 10:00 - 10:30 | Break - 30 mins |
| 10:30 - 11:40 | Reinforce Industrial use cases - 10 minute talks (8 minutes + QA) |
|  | Elefteris Kokoris-Kogias - Calypso on-chain secrets & policy enforcement  Tyler Kell - Lib-submarine  Kai Mast - Sharding blockchains  Alex Manuskin - Client Architecture |
| 11:40 - 12:00 | Standup of New Ideas and Research Directions |
| 12:00 - 12:15 | Closing Remarks |