**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. Join us 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).

This Retreat is in on February 14-15, and co-located at Interlaken with the Swiss Blockchain Winter School on February 11-14, but is a totally separate event.

For Retreat registration, please [apply here](https://docs.google.com/forms/d/e/1FAIpQLSdYwvouF4V6hoocwzdpRjoxQm2NH1ab7e3HyWmkcAQMsVqIlg/viewform).

For Blockchain Winter School information and registration on February 11-14, please see that event’s [site](https://blockchainschool.epfl.ch).



Congress Centre Kursaal Interlaken in Interlaken, Switzerland

There are several lodging accommodations near the Congress Centre, within an 8-15 minute walk. A sample of local hotels is [listed here](https://drive.google.com/file/d/1M8vALzLH4bMpLkmSWxs3xup6uVZKs_mh/view?usp=sharing) for reference. Please contact the hotels early to make your reservations, as this is a popular winter destination.

For information about the Interlaken area, please contact the Congress Center staff:

**Interlaken Congress & Events AG**

Strandbadstrasse 44

CH-3800 Interlaken

Phone: +41 33 827 62 00

Email: [info@interlaken-congress.ch](mailto:info@interlaken-congress.ch)

URL: [www.interlaken-congress.ch](https://interlaken.e-vent.online/webform/Home/E0DC1E702D2F424EA094D27C9D161284/www.interlaken-congress.ch)

IC3 Winter Retreat Agenda - Please check back later for agenda updates.

|  |  |
| --- | --- |
| **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  Enis Ceyhun Alp - Heterogeneous sharded blockchain architecture  Patrick McCorry - Scaling Cryptocurrencies via State Channels  Mustafa Al-Bassam - Fraud Proofs for light clients  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  Dawn Song - Oasis Labs |
| 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 - Asynchronous MPC Scalability: 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  Mic Bowman - Intel and SGX Update  Bernd Rosauer & Monica Sturm - Siemens  Bob McElrath - Fidelity  Sascha Hanse - Aeternity |
| 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 |