2nd ZKPROOF WORKSHOP

APRIL 10-12, 2019

ZKProof.org

SPONSORS

PLATINUM SPONSORS

qedit

Zcash Foundation

GOLD SPONSORS

vmware

BEAM

SILVER SPONSORS

CPIIS CHECK POINT INSTITUTE FOR INFORMATION SECURITY

clearmatics

ethereum foundation

STRATUMN

Protocol Labs

ING

SPECIAL CONTRIBUTORS

Microsoft

CHARTER & CODE OF CONDUCT

ZKPROOF CHARTER

The goal of the ZKProof Standardardization effort is to advance the use of Zero-Knowledge Proof technology by bringing together experts from industry and academia and producing Community Standards for the technology. We set the following guiding principles:

- We seek to represent all aspects of the technology, research and community in an inclusive manner.
- Our goal is to reach consensus where possible, and to properly represent conflicting views where consensus was not reached.
- As an open initiative, we wish to communicate our results to the industry, the media and to the general public, with a goal of making all voices in the event heard.
  - Participants in the event might be photographed or filmed.
  - We encourage you to tweet, blog and share with the hashtag #ZKProof.
  - Our official twitter handle is @ZKProof.

ZKPROOF CODE OF CONDUCT

All participants, speakers and sponsors of the ZKProof Standards Workshop shall adhere to the following code of conduct to ensure a safe and productive environment for everybody*:

At the workshop, you agree to:

- Respect the boundaries of other attendees.
- Respect the opinions of other attendees even if you are not in agreement with them.
- Avoid aggressively pushing your own services, products or causes.
- Respect confidentiality requests by participants.
- Look out for one another.

These behaviors don't belong at the workshop:

- Invasion of privacy
- Being disruptive, drinking excessively, stalking, following or threatening anyone.
- Abuse of power (including abuses related to position, wealth, race or gender).
- Homophobia, racism or behavior that discriminates against a group or class of people.
- Sexual harassment of any kind, including unwelcome sexual attention and inappropriate physical contact.

If you have any question, please refer to contact@zkproof.org

*This code of conduct is adapted from that of TEDx.

DAY 1

APRIL 10, 2019

RESEARCH & INDUSTRY SHOWCASE

8:00	**REGISTRATION & LIGHT BREAKFAST**
8:50	Welcoming Remarks Platinum Sponsors & Steering Committee
9:10	ZKP for Audits of Unsolicited Consumer Communication Hitarshi Buch and Harihara Natarajan, Wipro
9:35	Applications of Zero Knowledge Proofs in the Banking Industry Eduardo Moraes, ING
10:00	Bringing ZKP to Traditional Industries, Physical World Use-Cases Shiri Lemel, QEDIT
10:25	Privacy Pass: A Lightweight Zero-Knowledge Protocol Designed for the Web Nick Sullivan, Cloudflare
10:50	**BREAK**
11:10	Tooling Infrastructure for Zero-Knowledge Proofs Henry de Valence, Zcash Foundation
11:35	An R1CS Based Implementation of Bulletproofs Cathie Yun, Interstellar
12:00	Fragile Nonce Selection and ZKPs as a Solution Andrew Poelstra, Blockstream
12:25	Notes from the SNARKonomicon: Techniques for Writing SNARK Programs Izaak Mekler, O(1) Labs
12:50	Zero Knowledge Proofs and Self-Sovereign Identity Jordi Baylina, Iden3

Day 1 continued on next page >>

Scan the QR code to learn more about the scheduled talks.

DAY 1

APRIL 10, 2019

RESEARCH & INDUSTRY SHOWCASE

13:15	**LUNCH**
14:30	zk-SHARKs: Combining Succinct Verification and Public-Coin Setup Madars Virza, MIT
14:55	LegoSNARK: Modular Design and Composition of Succinct Zero-Knowledge Proofs Dario Fiore, IMDEA
15:20	Sonic: zkSNARKs from Linear-Size Universal and Updatable SRS Sean Bowe, Electric Coin Company
15:45	DIZK: A Distributed Zero-Knowledge Proof System Howard Wu, Berkeley & Dekrypt Capital
16:10	**BREAK**
16:30	Enterprise Features for Confidential Asset Transfers Ori Wallenstein, QEDIT
16:55	Zether: Towards Privacy in a Smart Contract World Shashank Agrawal, Visa Research
17:20	Succinct Proofs in Ethereum Barry Whitehat, Ethereum Foundation
17:45	Aurora: Transparent Succinct Arguments for R1CS Nick Spooner, UC Berkeley
18:10	**END OF DAY**
18:40	Reception at Venue

Scan the QR code to learn more about the scheduled talks.

DAY 2

APRIL 11, 2019

STANDARDS WORKSHOP

8:00	LIGHT BREAKFAST
9:00	Introducing the Standards Workshop Steering Committee
9:10	Public Accountability vs. Secret Law: Can They Coexist? Shafi Goldwasser, UC Berkeley, MIT and Weizmann
9:40	Efficient Zero-Knowledge Protocols: The Modular Approach Yuval Ishai, Technion
10:20	Privacy-Enhancing Cryptography at NIST Rene Peralta, NIST
11:00	BREAK
11:25	Community Standards: A Review and Further Work on the ZKProof Track Proceedings Moderators: Daniel Benarroch and Eran Tromer
12:45	LUNCH
14:00	Panel: Zero Knowledge in the Enterprise -Moderator: Jonathan Rouach Antonio Senatore, Carlos Kuchkovsky, Yael Kalai, David Archer and Mike Hearn
15:00	Bilinear Pairings based Zero-Knowledge Proofs Jens Groth, DFINITY
15:40	MPC-in-the-Head based Zero-Knowledge Proofs Amit Sahai, UCLA
16:20	BREAK
16:45	Community Standards: Interoperability of Zero-Knowledge Systems Moderators: Abhi Shelat and Sean Bowe

Scan the QR code to learn more about the scheduled talks.

DAY 3

APRIL 12, 2019

STANDARDS WORKSHOP

8:00	LIGHT BREAKFAST
9:00	GKR based Zero-Knowledge Proofs Yael Kalai, Microsoft Research
9:40	IOP based Zero-Knowledge Proofs Alessandro Chiesa, UC Berkeley
10:20	Discrete Log based Zero-Knowledge Proofs Dan Boneh, Stanford
11:00	BREAK
11:25	Community Standards: Commit-and-Prove Functionality Moderators: Jens Groth, Yael Kalai, Mariana Raykova and Muthu Venkitasubramaniam
12:45	LUNCH
14:00	From Public-Key Cryptography to PKI: Reflections on Standardizing the RSA Algorithm Jim Bidzos and Burt Kaliski, Verisign
15:00	Zero Knowledge Ideal Functionality Muthu Venkitasubramaniam, University of Rochester and Ligero
15:40	Open Discussion about ZKProof
16:20	BREAK
16:45	Community Standards: Deterministic Generation of Elliptic Curves for ZK Systems Moderators: Alessandro Chiesa and Sean Bowe
18:00	CLOSING REMARKS

Scan the QR code to learn more about the scheduled talks.

ZKProof.org