



► Breaking Bitcoin vol II.

Amsterdam, 8-9th June 2019

CALL FOR SPEAKERS

THE EVENT

Breaking Bitcoin was born at the climax of the Scaling Debate. We, as a community, had enough of this focus on “scaling” when the real fundamentals are still under-researched. Privacy. Censorship-resistance. Decentralization. All for one ultimate goal: an extremely secure and resilient system to serve as the foundations of future infrastructure, services and products.

Breaking Bitcoin Vol. I (Paris, 2017) brought together 300 attendees from all over the world, for a world-class conference about Bitcoin protocol security. Let's do even better this year!

THE TALKS

Breaking Bitcoin Vol. II will host the world-best speakers on their respective area of expertise, to challenge the Bitcoin security model.

Hardware security, Governance, Protocol-level architecture, Social attacks, from both the theoretical and practical perspectives.

Breaking Bitcoin is aimed at Bitcoin professionals, academics and enthusiasts. Attendees are expected to be familiar and up to date with Bitcoin's state of the art.

As usual, the talks will be live-streamed and recorded.

CALL FOR SPEAKERS

Breaking Bitcoin is looking for speakers and panelists. We are open to academic and industry proposals, an attached research paper would be appreciated but not a requirement.

The conference is about security, attacks, vulnerabilities, points of failure and weaknesses around Bitcoin. This includes social, economic, hardware, privacy, network, etc; attacks. Speakers do not have to be experts in Bitcoin as long as the talk is relevant to the protocol (Example: SGX key extraction attack <https://www.youtube.com/watch?v=ARZJPVe1kE> at Breaking Bitcoin vol 1).

SUBMISSION

Proposals should be submitted to: proposals@breaking-bitcoin.com

Required:

- Title of the talk
- Abstract, paragraph explaining the context and content
- Previous speaker history if any
- Academic/research paper if any

We do not tolerate irresponsible disclosure nor zero-days at Breaking Bitcoin. If you wish to submit a talk covering a vulnerability not yet/being patched, you can pgp-encrypt your email, checking the following fingerprint for proposals@breaking-bitcoin.com , preferably from a few sources.

GPG Fingerprint=B840 1997 0DBD 88F3 CFFE A103 28EA 9690 19E0 20C0