



## Call for Papers · Workshop on *bitcoin* Research 2014

Associated with the 18th International Conference on Financial Cryptography and Data Security (FC'14)  
March 3-7, 2014, Accra Beach Hotel & SPA, Barbados. The workshop will take place on Friday, March 7, 2014.

The recent success of Bitcoin, a decentralized cryptographic currency, has raised new research questions on the opportunities and risks of virtual currencies. A handful of research papers have appeared in multiple disciplines, spanning a range of outlets, including top security conferences, legal journals, and reports of international financial organizations. This workshop aims to bring together interested scholars who study virtual currencies, Bitcoin in particular, and their supporting ecosystems from a technical or socio-economic perspective.

### TOPICS

Suggested topics include (but are not limited to) empirical and theoretical studies of:

- Bitcoin protocol and extensions (cryptography, scripting language, formalization etc.)
- Adoption and transition dynamics
- Threat models and attacks
- Anonymity and privacy
- Metrics and measurements
- Proof-of-work, -stake, -burn, and alternative defenses against Sybil attacks
- Mining hardware and models of pooled mining
- Bitcoin peer-to-peer network
- Transaction graph analysis
- User studies
- Economic and monetary aspects
- Business models for Bitcoin services and intermediaries
- Relation to other payment systems
- Financial markets
- Fraud detection and financial crime prevention
- Regulation and law enforcement
- Forensics and monitoring
- Legal, ethical and societal aspects of (decentralized) virtual currencies
- Case studies (e.g., of adoption, tools, attacks, forks, scams, ...)
- Novel applications

The workshop solicits submissions of manuscripts that represent significant and novel research contributions. Submissions must not substantially overlap with works that have been published or that are simultaneously submitted to a journal or a conference with proceedings. In-scope papers submitted to but not selected for the main FC'14 conference will automatically be considered for inclusion in the workshop. All submissions should follow the Lecture Notes in Computer Science format and should be no more than 15 pages including references and well-marked appendices. Peer reviewers are not required to read the appendices, so the full papers should be intelligible without them. Paper submissions must be anonymous, with no author names, affiliations, or obvious references. Accepted papers will appear in the proceedings published by Springer Lecture Notes in Computer Science. Authors who seek to submit their works to journals may opt-out by publishing an extended abstract only.

### IMPORTANT DATES

<b>Paper submission</b>	November 24, 2013
<b>Notification of acceptance</b>	December 22, 2013
<b>Final papers</b>	January 31, 2014

### TECHNICAL PROGRAM COMMITTEE

Elli Androulaki, IBM Research Zurich, Switzerland  
Rainer Böhme, Univ. of Münster, Germany (co-chair)  
Dominic Breuker, University of Münster, Germany  
Srdjan Capkun, ETH Zurich, Switzerland  
David Chen, Lightspeed Venture Partners  
Nicolas Christin, Carnegie Mellon University  
Jeremy Clark, Concordia University, Canada  
Benjamin Edelman, Harvard Business School  
Matthew Green, Johns Hopkins University

Ghassan Karame, NEC Labs, Heidelberg, Germany  
Stefan Katzenbeisser, TU Darmstadt, Germany  
Joshua Kroll, Princeton University  
Kirill Levchenko, UC San Diego  
Ian Miers, Johns Hopkins University  
Andrew Miller, University of Maryland, College Park  
Tyler Moore, SMU Dallas (co-chair)  
Fergal Reid, University College Dublin, Ireland  
Meni Rosenfeld, Bitcoil, Israel

### STUDENT STIPENDS

Note that the International Financial Cryptography Association offers travel stipends in particular for students who will be presenting at the conference or associated workshops, including the workshop on Bitcoin research.