The Bitcoin electronic cash system, introduced the new field of blockchain technology as a practical mechanism for a permissionless censor-resistant internet money. The decentralized network and public verifiability of Bitcoin make tradeoffs speed of execution and weak privacy are two of Bitcoin's main issues. Despite a common assumption that Bitcoin is anonymous, its privacy properties are insufficient for many commercial use cases. Every transaction is published in a global ledger, which allows small amounts of information (e.g., the identities of the participants in a single transaction) to be amplified if statistical analysis is used to learn much about the users' financial activity. This limits the commercial usefulness of the network and also harms individual privacy, as user behavior frequently reflects the pervasive assumption that Bitcoin is an anonymous system.

CALL FOR PAPERS

SECURITY & PRIVACY ON THE BLOCKCHAIN

(EUROS&B)

AN IEEE EURO SECURITY & PRIVACY
AND EUROCRYPT AFFILIATED WORKSHOP

Paris, 29 April 2017

The Security and Privacy on the Blockchain Workshop is a premier forum for research on adoption of blockchains as a wide, secure and privacy preserving solution for transactional systems. We solicit previously unpublished papers offering novel contributions in Bitcoin and Blockchain research. Papers may present advances in the theory, design, implementation, analysis, verification, or empirical evaluation and measurement of existing systems. Papers that shed new light on past results by means of sound theory or thorough experimentation are also welcome.

Topics of Interest include:

- Improving mining protocols and consensus decentralization resiliency
- Compact ring signature
- Compact range proofs
- Privacy Preserving Signature Aggregation
- Work on SNARKs
- Better SPV models
- Privacy Improvements to blockchain technology
- Improvements to Fungibility of blockchain-based assets
- Game theory of proof-of-work based consensus
- Systematization of Knowledge in the field
- Privacy of blockchains
- Security of blockchains
- Novel improvements to scalability and capacity vs centralization tradeoffs
- Formally provable techniques for smart contracts

This topic list is not meant to be exhaustive. S&B is interested in all aspects of the blockchain research, however papers without a clear application, will be considered out of scope and may be rejected without full review. We encourage submissions that are "far-reaching" and "risky".

Important Dates

All deadlines are Anywhere on Earth (AoE = UTC-12h).

Research Papers	Paper submission deadline	**December 14, 2016**
	Acceptance notification	**January 13, 2017**
	Camera ready version	**February 13, 2017**

Instructions for Paper Submission

All submissions must be original work; the submitter must clearly document any overlap with previously published or simultaneously submitted papers from any of the authors. Failure to point out and explain overlap will be grounds for rejection. Simultaneous submission of the same paper to another venue with proceedings or a journal is not allowed and will be grounds for automatic rejection. Contact the program committee chair if there are questions about this policy.

Anonymous Submission

Papers must be submitted in a form suitable for anonymous review: no author names or affiliations may appear on the title page, and papers should avoid revealing their identity in the text. When referring to your previous work, do so in the third person, as though it were written by someone else. Only blind the reference itself in the (unusual) case that a third-person reference is infeasible. Contact the program chairs if you have any questions. Papers that are not properly anonymized may be rejected without review.

Page Limit and Formatting

Short position papers may not exceed 4 pages total and full papers may not exceed 10 pages, including references and appendices. Papers must be formatted for US letter (not A4) size paper with margins of at least 3/4 inch on all sides. The text must be formatted in a two-column layout, with columns no more than 9 in. high and 3.375 in. wide. The text must be in Times font, 10-point or larger, with 12-point or larger line spacing. Authors are encouraged to use the IEEE conference proceedings templates.

Submission

Submissions must be in Portable Document Format (.pdf). Authors should pay special attention to unusual fonts, images, and figures that might create problems for reviewers. Your document should render correctly in Adobe Reader XI and when printed in black and white.

Conference Submission Server

The submission site will open on **October 15th, 2016** and will be announced at www.blockstream.com and through easychair.org.

Publication and Presentation

Authors are responsible for obtaining appropriate publication clearances. One of the authors of the accepted paper is expected to present the paper at the conference. Submissions received after the submission deadline or failing to conform to the submission guidelines risk rejection without review. Accepted publications will be subject to publication in IEEE proceedings.

Organization Committee

Chairs:

Marta Piekarska (Blockstream)
Harry Halpin (INRIA)

Program Committee:

Christopher Allen (Blockstream) - Chair
Foteini Baldimtsi (George Mason University)
Karthikeyan Bhargavan (INRIA)
Joseph Bonneau (Stanford)
Srdjan Capkun (ETH Zurich)
George Danezis (University College London)
Bryan Ford (EPFL)
Georg Fuchsbauer (École Normale Supérieure)
Shin'ichiro Matsuo (MIT)
Christian Decker (ETH Zurich)
Neha Narula (MIT)
Hart Montgomery, (Fujitsu)
Peter Todd (Bitcoin)
Madars Virza (MIT)
Pindar Wong (VeriFi)
Guy Zyskind (MIT)
Wendy Seltzer (W3C/MIT)
Sabrina Kirrane (Vienna University of Economics and Business)
Frank Wagner (Deutsche Telekom)
Jean-Pierre Seifert (Technische Universität Berlin)