# Contents

## Part I First Workshop on Bitcoin Research

### Bitcoin Transactions, Policy and Legal Issues

- How Did Dread Pirate Roberts Acquire and Protect his Bitcoin Wealth? 3
  *Dorit Ron and Adi Shamir*

- Towards Risk Scoring of Bitcoin Transactions 16
  *Malte Möser, Rainer Böhme, and Dominic Breuker*

- Challenges and Opportunities Associated – With a Bitcoin-Based Transaction Rating System 33
  *David Vandervort*

- Bitcoin: A First Legal Analysis With Reference to German and US-American Law 43
  *Franziska Boehm and Paulina Pesch*

### Bitcoin Security

- Empirical Analysis of Denial-of-Service Attacks in the Bitcoin Ecosystem 57
  *Marie Vasek, Micah Thornton, and Tyler Moore*

- Game-Theoretic Analysis of DDoS Attacks Against Bitcoin Mining Pools 72
  *Benjamin Johnson, Aron Laszka, Jens Grossklags, Marie Vasek, and Tyler Moore*

- The Bitcoin P2P Network 87
  *Joan Antoni Donet Donet, Cristina Pérez-Solà, and Jordi Herrera-Joancomartí*

### Improving Digital Currencies

- Fair Two-Party Computations via Bitcoin Deposits 105
  *Marcin Andrychowicz, Stefan Dziembowski, Daniel Malinowski, and Łukasz Mazurek*

- Increasing Anonymity in Bitcoin 122
  *Amitabh Saxena, Janardan Misra, and Aritra Dhar*

  *Christina Garman, Matthew Green, Ian Miers, and Aviel D. Rubin*
**Bitcoin Poster Abstracts**

On Offline Payments with Bitcoin (Poster Abstract) .......................... 159
  *Alexandra Dmitrienko, David Noack, Ahmad-Reza Sadeghi, and Moti Yung*

One Weird Trick to Stop Selfish Miners: Fresh Bitcoins,
A Solution for the Honest Miner (Poster Abstract) .......................... 161
  *Ethan Heilman*

From Bitcoin to the Brixton Pound: History and Prospects for Alternative
Currencies (Poster Abstract) ..................................................... 163
  *Garrick Hileman*

**Part II Applied Homomorphic Cryptography and Encrypted Computing**

High-Speed Fully Homomorphic Encryption Over the Integers .............. 169
  *Xiaolin Cao, Ciara Moore, Máire O’Neill, Neil Hanley,
  and Elizabeth O’Sullivan*

Practical and Privacy-Preserving Policy Compliance for Outsourced Data... 181
  *Giovanni Di Crescenzo, Joan Feigenbaum, Debayan Gupta,
  Euthimios Panagos, Jason Perry, and Rebecca N. Wright*

Bandwidth Efficient PIR from NTRU ........................................... 195
  *Yarkin Doröz, Berk Sunar, and Ghaith Hammouri*

Toward Practical Homomorphic Evaluation of Block Ciphers Using Prince... 208
  *Yarkin Doröz, Aria Shahverdi, Thomas Eisenbarth, and Berk Sunar*

A Scalable Implementation of Fully Homomorphic Encryption
Built on NTRU ................................................................. 221
  *Kurt Rohloff and David Bruce Cousins*

Restructuring the NSA Metadata Program .................................... 235
  *Seny Kamara*

**Author Index** ................................................................. 249
Financial Cryptography and Data Security
FC 2014 Workshops, BITCOIN and WAHC 2014, Christ Church, Barbados, March 7, 2014, Revised Selected Papers
Böhme, R.; Brenner, M.; Moore, T.; Smith, M. (Eds.)
2014, XII, 249 p. 36 illus., Softcover
ISBN: 978-3-662-44773-4