## Contents

On the Malleability of Bitcoin Transactions .......................... 1  
*Marcin Andrychowicz, Stefan Dziembowski, Daniel Malinowski, and Łukasz Mazurek*

Trends, Tips, Tips: A Longitudinal Study of Bitcoin Transaction Fees .......... 19  
*Malte Möser and Rainer Böhme*

ZombieCoin: Powering Next-Generation Botnets with Bitcoin ............. 34  
*Syed Taha Ali, Patrick McCorry, Peter Hyun-Jeen Lee, and Feng Hao*

Cuckoo Cycle: A Memory Bound Graph-Theoretic Proof-of-Work .......... 49  
*John Tromp*

When Bitcoin Mining Pools Run Dry .................................. 63  
*Aron Laszka, Benjamin Johnson, and Jens Grossklags*

Issues in Designing a Bitcoin-like Community Currency ................... 78  
*David Vandervort, Dale Gaucas, and Robert St Jacques*

The Bitcoin Market Potential Index .................................. 92  
*Garrick Hileman*

Cryptographic Currencies from a Tech-Policy Perspective: Policy Issues and Technical Directions ....................... 94  
*Emily McReynolds, Adam Lerner, Will Scott, Franziska Roesner, and Tadayoshi Kohno*

Blindcoin: Blinded, Accountable Mixes for Bitcoin ........................ 112  
*Luke Valenta and Brendan Rowan*

Privacy-Enhancing Overlays in Bitcoin ................................ 127  
*Sarah Meiklejohn and Claudio Orlandi*

Search-and-Compute on Encrypted Data ................................ 142  
*Jung Hee Cheon, Miran Kim, and Myungsun Kim*

Accelerating SWHE Based PIRs Using GPUs ........................... 160  
*Wei Dai, Yarkin Doröz, and Berk Sunar*

Combining Secret Sharing and Garbled Circuits for Efficient Private IEEE 754 Floating-Point Computations ....................... 172  
*Pille Pullonen and Sander Siim*
Cryptanalysis of a (Somewhat) Additively Homomorphic Encryption Scheme Used in PIR ........................................ 184
  *Tancrède Lepoint and Mehdi Tibouchi*

Homomorphic Computation of Edit Distance .................................. 194
  *Jung Hee Cheon, Miran Kim, and Kristin Lauter*

  *Mayank Varia, Sophia Yakoubov, and Yang Yang*

Users’ Privacy Concerns About Wearables ..................................... 231
  *Vivian Genaro Motti and Kelly Caine*

On Vulnerabilities of the Security Association in the IEEE 802.15.6 Standard ........................................................ 245
  *Mohsen Toorani*

Visual Cryptography and Obfuscation: A Use-Case for Decrypting and Deobfuscating Information Using Augmented Reality ............... 261
  *Patrik Lantz, Bjorn Johansson, Martin Hell, and Ben Smeets*

Ok Glass, Leave Me Alone: Towards a Systematization of Privacy Enhancing Technologies for Wearable Computing ........................ 274
  *Katharina Krombholz, Adrian Dabrowski, Matthew Smith, and Edgar Weippl*

Design and Analysis of Shoulder Surfing Resistant PIN Based Authentication Mechanisms on Google Glass ........................... 281
  *Dhruv Kumar Yadav, Beatrice Ionascu, Sai Vamsi Krishna Ongole, Aditi Roy, and Nasir Memon*

Glass OTP: Secure and Convenient User Authentication on Google Glass ....... 298
  *Pan Chan, Tzipora Halevi, and Nasir Memon*

**Author Index** ........................................................................ 309
Financial Cryptography and Data Security
FC 2015 International Workshops, BITCOIN, WAHC, and Wearable, San Juan, Puerto Rico, January 30, 2015,
Revised Selected Papers
Brenner, M.; Christin, N.; Johnson, B.; Rohloff, K. (Eds.)
2015, XII, 309 p. 59 illus., Softcover
ISBN: 978-3-662-48050-2