

# Contents

## Third Workshop on Bitcoin and Blockchain Research, BITCOIN 2016

Stressing Out: Bitcoin “Stress Testing” . . . . .	3
<i>Khaled Baqer, Danny Yuxing Huang, Damon McCoy, and Nicholas Weaver</i>	
Why Buy When You Can Rent? Bribery Attacks on Bitcoin-Style Consensus . . . . .	19
<i>Joseph Bonneau</i>	
Automated Verification of Electrum Wallet . . . . .	27
<i>Mathieu Turuani, Thomas Voegtlin, and Michael Rusinowitch</i>	
Blindly Signed Contracts: Anonymous On-Blockchain and Off-Blockchain Bitcoin Transactions . . . . .	43
<i>Ethan Heilman, Foteini Baldimtsi, and Sharon Goldberg</i>	
Proofs of Proofs of Work with Sublinear Complexity . . . . .	61
<i>Aggelos Kiayias, Nikolaos Lamprou, and Aikaterini-Panagiota Stouka</i>	
Step by Step Towards Creating a Safe Smart Contract: Lessons and Insights from a Cryptocurrency Lab . . . . .	79
<i>Kevin Delmolino, Mitchell Arnett, Ahmed Kosba, Andrew Miller, and Elaine Shi</i>	
EthIKS: Using Ethereum to Audit a CONIKS Key Transparency Log . . . . .	95
<i>Joseph Bonneau</i>	
On Scaling Decentralized Blockchains: (A Position Paper) . . . . .	106
<i>Kyle Croman, Christian Decker, Ittay Eyal, Adem Efe Gencer, Ari Juels, Ahmed Kosba, Andrew Miller, Prateek Saxena, Elaine Shi, Emin Gün Sirer, Dawn Song, and Roger Wattenhofer</i>	
Bitcoin Covenants . . . . .	126
<i>Malte Möser, Ittay Eyal, and Emin Gün Sirer</i>	
Cryptocurrencies Without Proof of Work . . . . .	142
<i>Iddo Bentov, Ariel Gabizon, and Alex Mizrahi</i>	

## First Workshop on Secure Voting Systems, VOTING 2016

Coercion-Resistant Internet Voting with Everlasting Privacy . . . . .	161
<i>Philipp Locher, Rolf Haenni, and Reto E. Koenig</i>	

Selene: Voting with Transparent Verifiability and Coercion-Mitigation . . . . .	176
<i>Peter Y.A. Ryan, Peter B. Rønne, and Vincenzo Iovino</i>	
On the Possibility of Non-interactive E-Voting in the Public-Key Setting . . . .	193
<i>Rosario Giustolisi, Vincenzo Iovino, and Peter B. Rønne</i>	
Efficiency Comparison of Various Approaches in E-Voting Protocols . . . . .	209
<i>Oksana Kulyk and Melanie Volkamer</i>	
Remote Electronic Voting Can Be Efficient, Verifiable and Coercion-Resistant . . . . .	224
<i>Roberto Araújo, Amira Barki, Solenn Brunet, and Jacques Traoré</i>	
Universal Cast-as-Intended Verifiability . . . . .	233
<i>Alex Escala, Sandra Guasch, Javier Herranz, and Paz Morillo</i>	
<b>4th Workshop on Encrypted Computing and Applied Homomorphic Cryptography, WAHC 2016</b>	
Hiding Access Patterns in Range Queries Using Private Information Retrieval and ORAM. . . . .	253
<i>Gamze Tillem, Ömer Mert Candan, Erkey Savaş, and Kamer Kaya</i>	
Optimizing MPC for Robust and Scalable Integer and Floating-Point Arithmetic . . . . .	271
<i>Liisi Kerik, Peeter Laud, and Jaak Randmets</i>	
On-the-fly Homomorphic Batching/Unbatching. . . . .	288
<i>Yarkin Doröz, Gizem S. Çetin, and Berk Sunar</i>	
Using Intel Software Guard Extensions for Efficient Two-Party Secure Function Evaluation. . . . .	302
<i>Debayan Gupta, Benjamin Mood, Joan Feigenbaum, Kevin Butler, and Patrick Traynor</i>	
CallForFire: A Mission-Critical Cloud-Based Application Built Using the Nomad Framework . . . . .	319
<i>Mamadou H. Diallo, Michael August, Roger Hallman, Megan Kline, Henry Au, and Vic Beach</i>	
Cryptographic Solutions for Genomic Privacy. . . . .	328
<i>Erman Ayday</i>	
<b>Author Index . . . . .</b>	<b>343</b>

Financial Cryptography and Data Security  
FC 2016 International Workshops, BITCOIN, VOTING, and  
WAHC, Christ Church, Barbados, February 26, 2016,  
Revised Selected Papers  
Clark, J.; Meiklejohn, S.; Ryan, P.Y.A.; Wallach, D.;  
Brenner, M.; Rohloff, K. (Eds.)  
2016, XII, 343 p. 45 illus., Softcover  
ISBN: 978-3-662-53356-7