Contents

Third Workshop on Bitcoin and Blockchain Research, BITCOIN 2016

Stressing Out: Bitcoin “Stress Testing” ............................. 3
Khaled Baqer, Danny Yuxing Huang, Damon McCoy,
and Nicholas Weaver

Why Buy When You Can Rent? Bribery Attacks on Bitcoin-Style
Consensus ......................................................... 19
Joseph Bonneau

Automated Verification of Electrum Wallet ......................... 27
Mathieu Turuani, Thomas Voegtlin, and Michael Rusinowitch

Blindly Signed Contracts: Anonymous On-Blockchain and Off-Blockchain
Bitcoin Transactions .............................................. 43
Ethan Heilman, Foteini Baldimtsi, and Sharon Goldberg

Proofs of Proofs of Work with Sublinear Complexity ............. 61
Aggelos Kiayias, Nikolaos Lamprou, and Aikaterini-Panagiota Stouka

Step by Step Towards Creating a Safe Smart Contract: Lessons and Insights
from a Cryptocurrency Lab ......................................... 79
Kevin Delmolino, Mitchell Arnett, Ahmed Kosba, Andrew Miller,
and Elaine Shi

EthIKS: Using Ethereum to Audit a CONIKS Key Transparency Log .... 95
Joseph Bonneau

On Scaling Decentralized Blockchains: (A Position Paper) .......... 106
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

Bitcoin Covenants .................................................... 126
Malte Möser, Ittay Eyal, and Emin Gün Sirer

Cryptocurrencies Without Proof of Work .......................... 142
Iddo Bentov, Ariel Gabizon, and Alex Mizrahi

First Workshop on Secure Voting Systems, VOTING 2016

Coercion-Resistant Internet Voting with Everlasting Privacy ........ 161
Philipp Locher, Rolf Haenni, and Reto E. Koenig
<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Selene: Voting with Transparent Verifiability and Coercion-Mitigation</td>
<td>176</td>
</tr>
<tr>
<td>Peter Y.A. Ryan, Peter B. Rønne, and Vincenzo Iovino</td>
<td></td>
</tr>
<tr>
<td>On the Possibility of Non-interactive E-Voting in the Public-Key Setting</td>
<td>193</td>
</tr>
<tr>
<td>Rosario Giustolisi, Vincenzo Iovino, and Peter B. Rønne</td>
<td></td>
</tr>
<tr>
<td>Efficiency Comparison of Various Approaches in E-Voting Protocols</td>
<td>209</td>
</tr>
<tr>
<td>Oksana Kulyk and Melanie Volkamer</td>
<td></td>
</tr>
<tr>
<td>Remote Electronic Voting Can Be Efficient, Verifiable and Coercion-Resistant</td>
<td>224</td>
</tr>
<tr>
<td>Roberto Araújo, Amira Barki, Solenn Brunet, and Jacques Traoré</td>
<td></td>
</tr>
<tr>
<td>Universal Cast-as-Intended Verifiability</td>
<td>233</td>
</tr>
<tr>
<td>Alex Escala, Sandra Guasch, Javier Herranz, and Paz Morillo</td>
<td></td>
</tr>
<tr>
<td>4th Workshop on Encrypted Computing and Applied Homomorphic Cryptography, WAHC 2016</td>
<td></td>
</tr>
<tr>
<td>Hiding Access Patterns in Range Queries Using Private Information</td>
<td>253</td>
</tr>
<tr>
<td>Retrieval and ORAM.</td>
<td></td>
</tr>
<tr>
<td>Gamze Tillem, Ömer Mert Candan, Erkay Savaş, and Kamer Kaya</td>
<td></td>
</tr>
<tr>
<td>Optimizing MPC for Robust and Scalable Integer and Floating-Point Arithmetic</td>
<td>271</td>
</tr>
<tr>
<td>Liisi Kerik, Peeter Laud, and Jaak Randmets</td>
<td></td>
</tr>
<tr>
<td>On-the-fly Homomorphic Batching/Unbatching</td>
<td>288</td>
</tr>
<tr>
<td>Yarkin Doröz, Gizem S. Çetin, and Berk Sunar</td>
<td></td>
</tr>
<tr>
<td>Using Intel Software Guard Extensions for Efficient Two-Party Secure Function Evaluation</td>
<td>302</td>
</tr>
<tr>
<td>Debayan Gupta, Benjamin Mood, Joan Feigenbaum, Kevin Butler, and Patrick Traynor</td>
<td></td>
</tr>
<tr>
<td>CallForFire: A Mission-Critical Cloud-Based Application Built Using the Nomad Framework</td>
<td>319</td>
</tr>
<tr>
<td>Mamadou H. Diallo, Michael August, Roger Hallman, Megan Kline, Henry Au, and Vic Beach</td>
<td></td>
</tr>
<tr>
<td>Cryptographic Solutions for Genomic Privacy</td>
<td>328</td>
</tr>
<tr>
<td>Erman Ayday</td>
<td></td>
</tr>
<tr>
<td>Author Index</td>
<td>343</td>
</tr>
</tbody>
</table>
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