Synthesis Lectures on
Information Security, Privacy, and Trust

SYNTHESIS
COLLECTION OF TECHNOLOGY

Aljosha Judmayer · Nicholas Stifter ·
Katharina Krombholz · Edgar Weippl

Blocks and Chains

Introduction to Bitcoin, Cryptocurrencies, and Their Consensus Mechanisms

Springer

Blocks and Chains

Introduction to Bitcoin, Cryptocurrencies, and Their Consensus Mechanisms

Synthesis Lectures on Information Security, Privacy, & Trust

Editors

Elisa Bertino, ***Purdue University***
Ravi Sandhu, ***University of Texas, San Antonio***

The Synthesis Lectures Series on Information Security, Privacy, and Trust publishes 50- to 100-page publications on topics pertaining to all aspects of the theory and practice of Information Security, Privacy, and Trust. The scope largely follows the purview of premier computer security research journals such as ACM Transactions on Information and System Security, IEEE Transactions on Dependable and Secure Computing and Journal of Cryptology, and premier research conferences, such as ACM CCS, ACM SACMAT, ACM AsiaCCS, ACM CODASPY, IEEE Security and Privacy, IEEE Computer Security Foundations, ACSAC, ESORICS, Crypto, EuroCrypt and AsiaCrypt. In addition to the research topics typically covered in such journals and conferences, the series also solicits lectures on legal, policy, social, business, and economic issues addressed to a technical audience of scientists and engineers. Lectures on significant industry developments by leading practitioners are also solicited.

Blocks and Chains: Introduction to Bitcoin, Cryptocurrencies, and Their Consensus Mechanisms
Aljosha Judmayer, Nicholas Stifter, Katharina Krombholz, and Edgar Weippl
2017

Digital Forensic Science: Issues, Methods, and Challenges
Vassil Roussev
2016

Differential Privacy: From Theory to Practice
Ninghui Li, Min Lyu, Dong Su, and Weining Yang
2016

Privacy Risk Analysis
Sourya Joyee De and Daniel Le Métayer
2016

Introduction to Secure Outsourcing Computation
Xiaofeng Chen
2016

Database Anonymization: Privacy Models, Data Utility, and Microaggregation-based Inter-model Connections
Josep Domingo-Ferrer, David Sánchez, and Jordi Soria-Comas
2016

Automated Software Diversity
Per Larsen, Stefan Brunthaler, Lucas Davi, Ahmad-Reza Sadeghi, and Michael Franz
2015

Trust in Social Media
Jiliang Tang and Huan Liu
2015

Physically Unclonable Functions (PUFs): Applications, Models, and Future Directions
Christian Wachsmann and Ahmad-Reza Sadeghi
2014

Usable Security: History, Themes, and Challenges
Simson Garfinkel and Heather Richter Lipford
2014

Reversible Digital Watermarking: Theory and Practices
Ruchira Naskar and Rajat Subhra Chakraborty
2014

Mobile Platform Security
N. Asokan, Lucas Davi, Alexandra Dmitrienko, Stephan Heuser, Kari Kostiainen, Elena Reshetova, and Ahmad-Reza Sadeghi
2013

Security and Trust in Online Social Networks
Barbara Carminati, Elena Ferrari, and Marco Viviani
2013

RFID Security and Privacy
Yingjiu Li, Robert H. Deng, and Elisa Bertino
2013

Hardware Malware
Christian Krieg, Adrian Dabrowski, Heidelinde Hobel, Katharina Krombholz, and Edgar Weippl
2013

Private Information Retrieval
Xun Yi, Russell Paulet, and Elisa Bertino
2013

Privacy for Location-based Services
Gabriel Ghinita
2013

Enhancing Information Security and Privacy by Combining Biometrics with Cryptography
Sanjay G. Kanade, Dijana Petrovska-Delacrétaz, and Bernadette Dorizzi
2012

Analysis Techniques for Information Security
Anupam Datta, Somesh Jha, Ninghui Li, David Melski, and Thomas Reps
2010

Operating System Security
Trent Jaeger
2008

Blocks and Chains: Introduction to Bitcoin, Cryptocurrencies, and Their Consensus Mechanisms

Aljosha Judmayer, Nicholas Stifter, Katharina Krombholz, and Edgar Weippl

ISBN: 978-3-031-01224-2 paperback
ISBN: 978-3-031-02352-1 ebook

DOI 10.1007/978-3-031-02352-1

A Publication in the Springer series
SYNTHESIS LECTURES ON INFORMATION SECURITY, PRIVACY, & TRUST

Lecture #20
Series Editors: Elisa Bertino, *Purdue University*
Ravi Sandhu, *University of Texas, San Antonio*
Series ISSN
Print 1945-9742 Electronic 1945-9750

Blocks and Chains

Introduction to Bitcoin, Cryptocurrencies, and Their Consensus Mechanisms

Aljosha Judmayer, Nicholas Stifter, Katharina Krombholz, and Edgar Weippl
SBA Research

SYNTHESIS LECTURES ON INFORMATION SECURITY, PRIVACY, & TRUST #20

ABSTRACT

The new field of cryptographic currencies and consensus ledgers, commonly referred to as *blockchains*, is receiving increasing interest from various different communities. These communities are very diverse and amongst others include: technical enthusiasts, activist groups, researchers from various disciplines, start-ups, large enterprises, public authorities, banks, financial regulators, business men, investors, and also criminals. The scientific community adapted relatively slowly to this emerging and fast-moving field of cryptographic currencies and consensus ledgers. This was one reason that, for quite a while, the only resources available have been the Bitcoin source code, blog and forum posts, mailing lists, and other online publications. Also the original Bitcoin paper which initiated the hype was published online without any prior peer review. Following the original publication spirit of the Bitcoin paper, a lot of innovation in this field has repeatedly come from the community itself in the form of online publications and online conversations instead of established peer-reviewed scientific publishing. On the one side, this spirit of fast free software development, combined with the business aspects of cryptographic currencies, as well as the interests of today's time-to-market focused industry, produced a flood of publications, whitepapers, and prototypes. On the other side, this has led to deficits in systematization and a gap between practice and the theoretical understanding of this new field. This book aims to further close this gap and presents a well-structured overview of this broad field from a technical viewpoint. The archetype for modern cryptographic currencies and consensus ledgers is Bitcoin and its underlying Nakamoto consensus. Therefore we describe the inner workings of this protocol in great detail and discuss its relations to other derived systems.

KEYWORDS

block, chain, blockchain, Bitcoin, cryptographic currency, Proof-of-Work, Nakamoto consensus, consensus ledger

Contents

Acknowledgments

This research was funded by COMET K1, FFG–Austrian Research Promotion Agency, FFG Bridge Early Stage 846573 A2Bit and FFG Bridge 1 858561 SESC. We want to thank our reviewers, Foteini Baldimtsi, Patrick McCorry and Jong Ho Won, for useful feedback and discussions.

Aljosha Judmayer, Nicholas Stifter, Katharina Krombholz, and Edgar Weippl
May 2017