universität innsbruck

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

SYMPOSIUM ON POST-BITCOIN CRYPTOCURRENCIES

AGENDA

09:15 - 09:30	Welcome and Introduction Dr. Bernhard Haslhofer AIT Austrian Institute of Technology
09:30 - 10:00	The Post-Bitcoin Era: Cryptocurrencies are Here to Stay Prof. Dr. Rainer Böhme University of Innsbruck
10:00 - 10:30	De-Anonymization in Bitcoin and Beyond Prof. Sarah Meiklejohn, PhD University College London
10:30 - 11:00	Coffee Break
11:00 - 11:30	Towards Better Privacy with Monero Malte Möser, MSc Princeton University
11:30 - 12:00	Tracking Payment Flows in Ethereum Michael Fröwis, MSc University of Innsbruck
12:00 - 13:00	Lunch Break
13:00 - 13:30	Cryptocurrencies & Counterterrorism: Cooperative Solutions for Law Enforcement Agencies Prof. Dr. Daniel G. Arce University of Texas at Dallas
13:30 - 14:00	Chances and Risks of Cryptocurrencies' Transparency – A Legal Perspective Dr. Paulina Jo Pesch KIT Karlsruhe
14:00 - 14:30	Regulating Real Cryptocurrency Ecosystem Prof. Ross J. Anderson FRS FREng Cambridge University
14:30 - 15:00	Wrap up, Outlook and Closing Dr. Bernhard Haslhofer AIT Austrian Institute of Technology
15:00 - 16:00	Coffee / Open Discussions

SPEAKERS & TALKS

Prof. Dr. Rainer Böhme

Title: The Post-Bitcoin Era: Cryptocurrencies Are Here to Stay

Abstract: Bitcoin has been around for almost a decade. Looking back at past accomplishments and unfulfilled hopes, I revisit the future role of cryptocurrencies in the economy. Although wide adoption as a means of payment is unlikely in the short run, I'll argue that regulators cannot ignore recent technical developments when trying to resolve the tensions between safeguarding financial privacy, effective crime fighting and consumer protection, and adequate financial supervision, thereby setting the scene for the following talks in the symposium.

Short Bio: Rainer Böhme is professor of Computer Science at the University of Innsbruck and head of the Security and Privacy Laboratory. He is a pioneer of interdisciplinary cryptocurrency research and co-founder of one of the leading academic venues in Bitcoin and blockchain research. He served as spokesperson of the German BITCRIME research project (2014-2017) and is principal investigator in the European Commission's Horizon 2020 project TITANIUM (2017-2020) as well as in the VIRTCRIME research project (2018-2019) funded by the Austrian government.

Prof. Sarah Meiklejohn, PhD

Title: De-Anonymization in Bitcoin and Beyond

Abstract: A long line of recent research has demonstrated that existing cryptocurrencies often do not achieve the level of anonymity that users might expect they do, due to the ability to combine publicly available information with minimal data gathered by hand. I'll discuss how this works for Bitcoin before moving on to present how it also works for more advanced "privacy coins" such as Zcash.

Short Bio: Sarah Meiklejohn is a Reader (Associate Professor) in Cryptography and Security at UCL, in the Computer Science department. She is affiliated with the Information Security Group, and is also a member of the Open Music Initiative and the Initiative for Cryptocurrencies and Contracts (IC3).

Malte Möser, MSc

Title: Towards Better Privacy with Monero

Abstract: Monero is a privacy-centric cryptocurrency that aims to improve upon the limited privacy available in transparent cryptocurrencies like Bitcoin. In this talk I will provide an overview of the mechanisms that Monero uses to achieve greater privacy and explain how these improve upon Bitcoin. Busting a few common myths, I'll discuss both historic and current limitations that can degrade users' privacy, highlighting the unique challenges in designing privacy-preserving cryptocurrencies.

Short Bio: Malte Möser is a PhD student in the Department of Computer Science at Princeton University and a Graduate Student Fellow at the Center for Information Technology Policy. His research focuses on the security and privacy of cryptographic currencies. You can follow him on Twitter at @maltemoeser.

Michael Fröwis, MSc

Title: Tracking Payment Flows in Ethereum

Abstract: This talk explains the differences of money-flow tracking in Ethereum and Bitcoin. They include 1) a simplified account mode supported by a generalized transaction logic, 2) the possibility of payments being initiated by code accounts ("smart contracts"), 3) the abstraction from the system's default currency to user-defined virtual assets ("tokens"), 4) and different privacy conventions enforced by standard client software (e.g., "wallet contracts"). We outline challenges and solution approaches for forensic investigations and give selected illustrating examples.

Short Bio: Michael Fröwis is a PhD student in the Department of Computer Science at the University of Innsbruck. His research focuses on privacy, smart contract analysis, and blockchain forensics. Before joining the University of Innsbruck, he has worked as a software developer in a bank.

Prof. Dr. Daniel G. Arce

Title: Cryptocurrencies & Counterterrorism: Cooperative Solutions for Law Enforcement Agencies

Abstract: Terrorism and the criminal use of cryptocurrencies are borderless phenomena. As such, both require coordination among law enforcement agencies. This presentation discusses how successes in counterterror coordination can be adapted to address the use of cryptocurrencies for money laundering and terrorism financing.

Short Bio: Daniel Arce is the Ashbel Smith Professor of Economics at the University of Texas at Dallas. Professor Arce is a game theorist whose research interests include (counter)terrorism and cybersecurity. He has won two Fulbright grants and was named an Outstanding Teacher by the University of Texas System's Board of Regents.

Dr. Paulina Jo Pesch

Title: Chances and Risks of Cryptocurrencies' Transparency – A legal perspective

Abstract: Cryptocurrency transaction ledgers present a high degree of transparency. Their publicity enables investigators, regulators, and private actors to trace transaction flows. This not only creates opportunities for law enforcement and AML regulation but also poses risks to data protection. The talk sheds light on the chances and risks of cryptocurrencies' transparency from a legal perspective.

Short Bio: Dr. Paulina Jo Pesch studied law with focus on IT law at the University of Münster. She has researched cryptocurrencies and blockchain systems since 2014. She particularly coordinated the German sub-project of the BITCRIME project – on the prosecution and prevention of cybercrime with cryptocurrencies. At present, she is a post-doctoral researcher at the Karlsruhe Institute of Technology and examines legal requirements for the investigation of criminal activities involving cryptocurrencies under EU data protection law in the TITANIUM project.

Prof. Ross J. Anderson FRS FREng

Title: Regulating Real Cryptocurrency

Abstract: Cryptocurrencies started as an anarchist experiment, came of age on the Silk Road, spawned ransomware and matured into an investment bubble. So what have governments done? Mostly their focus has been on collecting copies of customers' utility bills, or "know-your-customer". As it's known. Is this enough? Not at all. The cryptocurrency world has morphed since 2014 into a shadow banking system, with most transactions now "off-blockchain", that is, handled by bitcoin exchanges. While they represent themselves as being like gold merchants, where the customer owns the asset, they mostly behave like banks – where the customer merely has a call against a pool of assets, and has to stand in line if the bank goes bust. And, surprise surprise, over a third of bitcoin exchanges have indeed gone bust. What must be done? First, regulators must understand the cryptocurrency world as it actually is, not as its promoters represent it. Second, when companies act like banks, they must be regulated like banks -- which means the E-Money Directive, Payment Services Directive 2, Basel III, fit and proper persons in charge and clear accounting standards. It also means no transactions with evil exchanges, so regulators need to to think about whitelists and blacklists. The default should be that exchanges are regulated just like banks, with the burden on them to argue why any particular regulatory regime should not apply.

Short Bio: Ross Anderson is Professor of Security Engineering at Cambridge University. He was one of the founders of the discipline of security economics, and leads the Cambridge Cybercrime Centre, which collects and analyses data about online wickedness. He was one of the designers of the international standards for prepayment electricity metering and powerline communications; he was also a pioneer of peer-to-peer systems, hardware tamper-resistance and API security.

Dr. Bernhard Haslhofer

Title: Emerging Technologies and Regulatory Challenges in the Post-Bitcoin Era

Abstract: A decade ago Bitcoin, the first practical cryptocurrency, started as an idealistic experiment with a number of initial promises and expectations; some of them still hold, others turned out to be different. Today cryptocurrencies are widely known and adopted by relevant user groups and now form a market that attracts the attention of regulators and supervisors, who seem to converge on the view that cryptocurrency exchange services and wallet providers require regulation. The challenge will be to find the right balance between enabling innovation and providing technical and legal security for legitimate users on the one side and supporting law enforcement in the mitigation and prevention of illegitimate activities on the other side. However, any upcoming regulation and policies that to do not consider recent technical developments might miss the target. Therefore, the goal of this symposium will bring together a group of renowned scientists who will present latest scientific and technical results in the field of cryptocurrency research and to highlight the new challenges businesses, users, and regulators will face in the light of Post-Bitcoin Cryptocurrencies.

Short Bio: Dr. Bernhard Haslhofer works as a Senior Scientist at the Austrian Institute of Technology's Digital Insight Lab. Previously, he was an EU Marie Curie Fellow at Cornell University Information Science (NY, USA) and a PostDoc at the University of Vienna from where he also received his Ph.D in Computer Science. He also holds Master's degrees in Economics and Computer Science. He usually works in multidisciplinary settings to which he contributes methods drawn from fields like Machine Learning, Network Analytics, or Information Retrieval and Text Mining. At the moment, he primarily works on investigating and developing novel methods for analyzing cryptocurrency ecosystems such as Bitcoin.

Contact

AIT Austrian Institute of Technology

Center for Digital Safety & Security
Giefinggasse 4 | 1210 Wien | Austria

www.ait.ac.at

Dr. Bernhard Haslhofer
Digital Insight Lab

T +43 664 88390692
F +43 (0) 50550 - 4150
bernhard.haslhofer@ait.ac.at

University of Innsbruck

Department of Computer Science
Technikerstraße 21A | 6020 Innsbruck | Austria

www.uibk.ac.at

Prof. Dr. Rainer Böhme
Security and Privacy Lab

T +43 512 507-53202
F +43 512 507-53018
rainer.boehme@uibk.ac.at