CBT: Cryptocurrencies and Blockchain Technology

Thursday, September 26, 2019

08:00 – 08:45

Registration

08:45 – 10:00

Room: Schengen II
General Welcome & Invited Talk I
Chairs: Joaquin Garcia-Alfaro & Alex Biryukov
Invited Talk Title: *Off Blockchain Protocols*
Speaker: Arthur Gervais, Imperial College London, UK

10:00 – 10:30

Coffee Break

10:30 – 12:00

Session 1: Lightning Networks and Short Papers

Room: Schengen II
Chair: Rainer Böhme, University of Innsbruck, Austria

TEE-Based Distributed Watchtowers for Fraud Protection in the Lightning Network, *By Marc Leinweber, Matthias Grundmann, Leonard Schönborn and Hannes Hartenstein*

Payment Networks as Creation Games, *By Georgia Avarikioti, Rolf Scheuner and Roger Wattenhofer*

Short Papers

An Efficient Micropayment Channel on Ethereum, *By Hisham Galal, Muhammad Elsheikh and Amr Youssef*

Extending Atomic Cross-Chain Swaps, *By Jean Yves Zie, Jérémy Briffaut, Benjamin Nguyen and Jean-Christophe Deneuville*

12:00 – 13:30

Lunch Break

13:30 – 14:45
Session 2: Smart Contracts and Applications
Room: Schengen II
Chair: Hannes Hartenstein, KIT, Germany

The Operational Cost of Ethereum Airdrops, *By Michael Fröwis and Rainer Böhme*

Blockchain Driven Platform for Energy Distribution in a Microgrid, *By Arjun Choudhry, Ikechukwu Dimobi and Zachary Gould*

Practical Mutation Testing for Smart Contracts, *By Joran Honig, Maarten Everts and Marieke Huisman*

14:45 – 15:15
Coffee break

15:15 – 16:45
Session 3: Payment Systems & Invited Talk II
Room: Schengen II
Chair: Joaquin Garcia-Alfaro, Télécom SudParis, France

Online Payment Network Design, *By Georgia Avarikioti, Kenan Besic, Yuyi Wang and Roger Wattenhofer*

Invited Talk II

Title: *Compact Blockchains & Proofs-of-Necessary Work*
Speaker: Joseph Bonneau, New York University, USA

17:00 – 20:30
Social Activity

20:30 – 22:00
Gala Dinner

Friday, September 27, 2019

09:00 – 10:00

Invited Talk III

Room: Schengen II
Chair: Alex Biryukov, University of Luxembourg, Luxembourg
Invited Talk Title: *Finality from Proof-of-Work Quorums*
Speaker: Rainer Böhme, University of Innsbruck, Autria

10:00 – 10:30

Coffee break

10:30 – 13:00

Session 4: Privacy, Mining and Short papers

Room: Schengen II
Chair: Guillermo Navarro, Universitat Autonoma de Barcelona

Simulation Extractability in Groth's zk-SNARK, *By Shahla Atapoor and Karim Baghery*

Auditable Credential Anonymity Revocation Based on Privacy-Preserving Smart Contracts, By Rujia Li, David Galindo and Qi Wang

Bonded Mining: Difficulty Adjustment by Miner Commitment, *By George Bissias, David Thibodeau and Brian Levine*

A Multi-Protocol Payment System to Facilitate Financial Inclusion, *By Kazım Rıfat Özyılmaz, Nazmi Berhan Kongel, Ali Erhat Nalbant and Ahmet Özcan*

Short Papers

12 Angry Miners (Short Paper), *By Aryaz Eghbali and Roger Wattenhofer*

A minimal core calculus for Solidity contracts, *By Massimo Bartoletti, Letterio Galletta and Maurizio Murgia*

Multi-Stage Contracts in the UTXO Model, *By Alexander Chepurnoy and Amitabh Saxena*

13:00 – 14:00

Farewell Lunch

Keynote Speakers

Arthur Gervais

Imperial College London
South Kensington, London SW7 2AZ, UK

Title: Off Blockchain Protocols
Date: Thursday, September 26, 2019
Hour: 09:00
Room: Schengen II
Workshops: CBT, DPM, STM

Abstract

A plethora of recent research works have demonstrated different mechanisms on how to perform blockchain transactions without writing every single interaction to the underlying ledger. Instead, these protocols utilize the expensive and low-rate blockchain only as a recourse for disputes. Off-chain protocols promise to complete transactions in sub-seconds rather than minutes or hours while retaining asset security, reducing fees and allowing blockchains to scale. This talk will explore the various lines of research covering off-chain transactions. We will discuss their security and privacy provisions and identify unsolved challenges, indicating promising avenues of future work.

Short Biography

Arthur Gervais is a Lecturer (equivalent Assistant Professor) of Computer Science at Imperial College London. Gervais's research focuses on applied cryptography, network and distributed ledger security, privacy as well as their scalability properties. He was the first to objectively compare the security properties of different proof of work blockchains, and further outlining the tensions between scalability and security. With "Do you need a Blockchain?", he built a widely adopted framework to understand objectively if a blockchain is indeed the appropriate technical solution to a problem. Gervais co-founded two startups in the blockchain space. *Liquidity.Network*, where he acts as CEO, develops a second layer scaling solution to enable higher transaction throughputs on existing blockchains. For *ChainSecurity*, Gervais helped to design the first automated formal smart contract security verification tool Securify.ch. Gervais served on many program committees including top-tier academic security conferences such as ACM CCS. Gervais co-organized the inaugural *CryptoValley Conference in Zug* and he advises the blockchain observatory forum of the European Union.

Keynote Speakers (cont.)

Joseph Bonneau
New York University, USA

Title: Compact Blockchains & Proofs-of-Necessary Work
Date: Thursday, September 26, 2019
Hour: 15:45
Room: Schengen II
Workshop: CBT

Abstract

Incrementally verifiable computation can produce a short proof that an *entire* blockchain history is correct. This enables even light clients to track the blockchain efficiently with minimal trust assumptions. The main challenge is to incentivize creating these proofs. This talk will overview the challenges and possible solutions for solving this incentive problem in a proof-of-work setting by having proof creation double as a proof-of-work puzzle.

Short Biography

Joseph holds a Bachelor of Science and Master of Science from Stanford University. In 2012 he received a Doctor of Philosophy in Computer science from University of Cambridge. He started his career in 2007 as a Cryptographic Scientist at Cryptography Research, Inc. From 2012 to 2014 he worked as a Software Engineer at Google. From 2015 to 2017 he was a Technology Fellow at Electronic Frontier Foundation. Since 2017 Joseph has been an Assistant Professor at New York University.

Keynote Speakers (cont.)

Rainer Böhme

University of Innsbruck

Innsbruck, Austria

Title: Finality from Proof-of-Work Quorums
Date: Friday, September 27, 2019
Hour: 09:00
Room: Schengen II
Workshop: CBT

Abstract

We challenge the widely held belief that proof-of-work enables truly permissionless decentralized systems, but the price to pay is that state updates are never final. We propose HotPoW, a scalable permissionless distributed log protocol, as a positive example to support our claim that it is possible to build permissionless consensus protocols ***with*** finality based on proof-of-work. HotPoW adapts the three-phase commit pipeline recently presented in HotStuff (PODC 2019; used in LibraBFT) by relying on the stochastic uniqueness of proof-of-work quorums, a new theoretical concept for protocol design. We position HotPoW in the design space of consensus protocols and evaluate it with nodes that implement adversarial modifications. The protocol can tolerate network latency, churn, and targeted attacks on consistency and liveness at small overhead compared to Nakamoto consensus. We invite the community to prove our claim wrong, and provide running code to facilitate this task.

Short Biography

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.