Dr. Arthur Gervais

I am motivated by revolutionizing how society trades and interacts. Bitcoin and the security properties of its blockchain provide technical means to catalyze societal evolution. My research therefore focuses on the security, privacy and performance of blockchain technology. Because this technology is still in its infancy, I largely focus on understanding and quantifying the tension points and tradeoffs in terms of security, privacy and performance, with the goal to build a mainstream, scalable, open, and decentralized blockchain protocol.
Part of my research is e.g., the design of usable software that securely interacts with networks and hardware, connecting the real world with blockchain, and the design of practical and scalable blockchain platform. My research is inherently multidisciplinary and I frequently collaborate with colleagues worldwide in various fields (e.g., machine learning).

Lägernstrasse 6
8153 Rümlang
Switzerland

Website
http://arthurgervais.com

Email
arthur@gervais.cc

Mobile
+41 78 203 26 82

Updated
September 2018

Professional experience

10/2017 - **Lecturer (equivalent Assistant Professor), Imperial College London**
London, United Kingdom
- Research fields: Security, privacy and scalability of digital currencies (e.g., Bitcoin, Ethereum), Secure hardware – software interactions (e.g., cryptocurrency wallets, trusted hardware), secure authentication methods, web and machine learning privacy
- Teaching: Developed the first Blockchain course at Imperial attended by nearly 100 students.
- Massive Online Learning Platform https://achievement.network: First open source smart contract learning platform that compiles, deploys a smart contract on a blockchain and evaluates the result in one click. Students can track and share their progress to stay motivated
- Community: Established the first CryptoValley Conference on Blockchain Technology 2018, attended by an audience of over 900 people and assembled a world class PC as PC chair
- Research group: supervising 4 bright PhD students
- Funding: attracted over 300'000 GBP in research funding during 2017/2018

09/2017 - **Co-founder, CEO, LiquidChain AG**
Zurich, Switzerland
- Developed scaling solutions for open and decentralized blockchains
- First off-chain platform operational on the Ethereum mainet in June 2018
- Raised 26M USD in funding, community of over 15k members on Telegram
- Online available under https://liquidity.network, deployed on iOS and Android

07/2017 - **Lecturer (Dozent), Hochschule Luzern**
Rotkreuz, Switzerland
- European Commission Blockchain Observatory and Forum: blockchain opportunities regarding scalability, security and privacy (https://www.eublockchainforum.eu/)
- Collaboration with ConsenSys on the EU Blockchain Observatory

10/2017 **Co-founder, ChainSecurity AG**
Zurich, Switzerland
- Providing security services for blockchain based smart contracts
- First automated formal verification tool for Ethereum based smart contracts (www.securify.ch)

12/2016 - 08/2017 **Senior Researcher, ETH Zurich**
Zurich, Switzerland
- Research fields: Security and privacy of digital currencies (e.g., Bitcoin), web privacy
- 3 peer-reviewed publications, 4th year in a row ACM CCS, USENIX Security and ESORICS 2017
- Supervision of 1 Master thesis, 1 Bachelor thesis and 2 Semester theses

08/2015 - 11/2015 **Research Intern, Supervisor: Mic Bowman, Intel Labs**
Portland, United States of America
- Quantifying incentives for participation in blockchain based systems
- Received Letter of Intent from Intel consisting of a job offer upon PhD graduation

07/2011 - 12/2014 **CEO and Founder, Consulting and Management, Hatforce**
Leverkusen, Germany
- First startup to develop a bug bounty platform (like hackerone.com)
- Winner of the SSES (Stockholm School of Entrepreneurship) Venture Challenge, January 2012
- Semi-finalist of the Venture Challenge Competition, San Diego State University, USA, March 2012

12/2011 - 06/2012 **Junior Security Consultant, Nixu Ltd.**
Helsinki, Finland
- Master Thesis about SCADA/ICS security, elaborated security testing guidelines for ICS
- Detected important vulnerabilities in widespread Industrial Control Systems hardware

05/2010 - 08/2010 **Intern, IPv6 Networking, German Federal Office for Information Security (BSI)**
Bonn, Germany
- Deep analysis of the IPv6 protocol and its inherent protocol weaknesses
- Conducting various IPv6 related network attacks and analysis of possible defenses

06/2009 - 09/2009 **Intern, Programming, EADS Secure Networks Oy**
Jyväskylä, Finland
- Planned and programmed reliable tracing software in C++ and Java for the TETRA network

05/2005 - 01/2006 **Intern, Programming, Timmann GmbH & Co**
Tutzing, Germany
- Optimization of the AES reference implementation for use in FPGA's

Educational background

12/2012 - 12/2016 **Research Assistant and PhD Candidate, Advisor: Srdjan Capkun, ETH Zurich**
Zurich, Switzerland
- Research fields: Security and privacy of digital currencies (e.g., Bitcoin), web privacy
- Collaboration with Armasuisse (Thun, Switzerland) and NEC Laboratories (Heidelberg, Germany)
- Supervision of 6 Master thesis, 1 Bachelor thesis and 5 Semester theses
- 7 peer-reviewed publications, 3 years consecutively in tier 1 conference (ACM CCS)

09/2010 - 09/2012 **Double Master of Science in Security and Mobile Computing**, Erasmus Mundus NordSecMob
Royal Institute of Technology (KTH), Advisor: Peter Sjödin, Sweden (1 year)
Aalto University, Advisor: Tuomas Aura, Finland (6 months)
Relevant coursework: Advanced Networks, Routing Protocols, Internet Security and Privacy, Cryptographic Protocols, Software Security, Mobile Application Development

09/2008 - 09/2012 **Master of Science in Computer Engineering**
National Institute of Applied Sciences (INSA) Lyon, Advisor: Youakim Badr, France
Relevant coursework: C/C++ Programming, Java, Operating Systems, Project Management, Computer Architecture, Data Modeling, Reverse Engineering, Database Management Systems.

08/2006 - 06/2008 **Classes préparatoires**
National Institute of Applied Sciences (INSA) Lyon, France
2-year undergraduate scientific foundation course in Engineering Sciences in a department with emphasis on foreign exchanges and international scientific connections in Europe

06/2006 **High School Diploma**
Gymnasium Starnberg, Germany
Focus on Mathematics and Physics

Selected Invited Talks

Berkley	**Non-Custodial Financial Intermediaries** Berkley, Crypto Economics Security Conference, October 2018
Microsoft Research Cambridge	**Non-Custodial Financial Intermediaries** Research Workshop Imperial – Microsoft, September 2018
EDCON	**Non-Custodial Financial Intermediaries** Toronto, Ethereum Developer Conference, May 2018
Stanford	**Off-chain Transactions for Open and Decentralized Blockchains** Stanford, Blockchain Protocol Analysis and Security Engineering, January 2018
	On the Security and Performance of Proof of Work Blockchains Stanford, USA, Blockchain Protocol Analysis and Security Engineering, January 2017
Scaling Bitcoin	**On the Security and Performance of Proof of Work Blockchains** Milan, Italy, October 2016
	Tampering with the Delivery of Blocks and Transactions in Bitcoin Hong Kong, China, December 2015
Google	**Quantifying Web-Search Privacy** Zürich, Switzerland, May 2015
S4	**New Modicon PLC Vulns, SCAPY and ModbusSec** SCADA Security Scientific Symposium (S4) Miami, United States, January 2013
Cambridge University	**Security Analysis of Industrial Control Systems** **University of Cambridge Computer Laboratory, Security seminar series** Cambridge, United Kingdom, July 2012
Nuit du Hack	**SCADA System Attacks** Paris, France, June 2012
BSI	**IPv6 attacks and defenses in local area networks** **German IT-Security Conference "12. IT-Sicherheitskongress des BSI"** Won the „Best Student Award 2011" from the German Federal Office for Information Security Bonn, Germany, May 2011

Awards / Honors

2018	Scholarship for Blockchain Protocol Analysis and Security Engineering, Stanford Scholarship for Crypto Economics Security Conference, San Francisco
2017	Scholarship for Blockchain Protocol Analysis and Security Engineering, Stanford
2016	Heidelberg Laureate Forum invitation Letter of Intent after internship completion at Intel Labs Acquired funding for Blockchain Summerschool ETH Zurich Scholarship for Scaling Bitcoin
2015	Scholarship for Scaling Bitcoin

2012 Winner of SSES (Stockholm School of Entrepreneurship) Venture Challenge

2011 Best Student Award from the German Federal Office for Information Security

2010 Erasmus Mundus NordSecMob Master Double Degree scholarship, 2010 – 2012

Academic Publications

2018 XCLAIM: Interoperability with Cryptocurrency-Backed Tokens
Alexei Zamyatin, Dominik Harz, J. Lind, Panayiotis Panayiotou, **Arthur Gervais**, William J. Knottenbelt
Eprint Report 643 (under submission)

NOCUST: A Non-Custodial 2nd-Layer Financial Intermediary
Rami Khalil and **Arthur Gervais**
Eprint Report 642 (under submission)

Securify: Practical Security Analysis of Smart Contracts
Petar Tsankov, Andrei Dan, Dana Drachsler-Cohen, **Arthur Gervais**, Florian Bünzli, Martin Vechev
in Proceedings of the ACM Conference on Computer and Communication Security (CCS), 2018

Do you need a Blockchain?
Karl Wüst and **Arthur Gervais**
1st Crypto Valley Conference on Blockchain Technology, 2018

TLS-N: Non-repudiation over TLS Enabling Ubiquitous Content Signing for Disintermediation
Hubert Ritzdorf, Karl Wüst, **Arthur Gervais**, Guillaume Felley, Srdjan Capkun
Network and Distributed System Security Symposium (NDSS), 2018

2017 REVIVE: Rebalancing Off-Blockchain Payment Networks
Rami Khalil and **Arthur Gervais**
in Proceedings of the ACM Conference on Computer and Communication Security (CCS), 2017

Arthur Gervais, Alexandros Filios, Vincent Lenders and Srdjan Capkun
Quantifying Web Adblocker Privacy
In Proceedings of the 22nd European Symposium on Research in Computer Security (ESORICS), 2017

ROTE: Rollback Protection for Trusted Execution
Sinisa Matetic, Mansoor Ahmed, Kari Kostiainen, Aritra Dhar, David Sommer, **Arthur Gervais**, Ari Juels, Srdjan Capkun
In Proceedings of the 26th USENIX Security Symposium, 2017

2016 On the Security and Performance of Proof of Work Blockchains
Arthur Gervais, Ghassan Karame, Karl Wüst, Vasileios Glykantzis, Hubert Ritzdorf, Srdjan Capkun
in Proceedings of the ACM Conference on Computer and Communication Security (CCS), 2016

Quantifying Location Privacy Leakage from Transaction Prices
Arthur Gervais, Hubert Ritzdorf, Mario Lucic, Srdjan Capkun
In Proceedings of the 21th European Symposium on Research in Computer Security (ESORICS), 2016

Ethereum Eclipse Attacks
Karl Wüst and **Arthur Gervais**
Technical Report, ETH Zurich, Department of Computer Science, 2016

Bitcoin Protocol Specification
Arthur Gervais and Ghassan Karame
Bitcoin and Blockchain Security (Chapter 3), ISBN: 978-1-63081-013-9 (Invited Chapter), 2016

2015 Tampering with the Delivery of Blocks and Transactions in Bitcoin
Arthur Gervais, Hubert Ritzdorf, Ghassan Karame, Srdjan Capkun
In Proceedings of the ACM Conference on Computer and Communication Security (CCS), 2015

Misbehavior in Bitcoin: A Study of Double-Spending and Accountability
Ghassan Karame, Elli Androulaki, Marc Roeschlin, **Arthur Gervais**, Srdjan Capkun
in ACM Transactions on Information and System Security (TISSEC), 2015

2014 On the Privacy Provisions of Bloom Filters in Lightweight Bitcoin Clients
Arthur Gervais, Ghassan Karame, Damian Gruber, Srdjan Capkun
In Proceedings of the 30th Annual Computer Security Applications Conference (ACSAC), 2014

Quantifying Web-Search Privacy
Arthur Gervais, Reza Shokri, Adish Singla, Srdjan Capkun and Vincent Lenders
in Proceedings of the ACM Conference on Computer and Communication Security (CCS), 2014

Is Bitcoin a Decentralized Currency?
Arthur Gervais, Ghassan Karame, Srdjan Capkun, Vedran Capkun
IEEE Security and Privacy Magazine, 2014

2013 Double-Spending Fast Payments in Bitcoin due to Client versions 0.8.1
Arthur Gervais, Hubert Ritzdorf, Ghassan Karame
Technical Report, ETH Zürich, Department of Computer Science, 2013

2012 Security Analysis of Industrial Control Systems
Arthur Gervais
Master Thesis

Other Publications

2012 Whitepaper on Industrial Automation Security in Fieldbus and Field Device Level
Magnus Sundell, Janne Kuivalainen, Juhani Mäkelä, **Arthur Gervais**, Jouko Orava, Mikko H. Hyppönen
Vacon, supplier of variable speed AC drives

Security Analysis of Google Wallet (text in German)
http://arthur.gervais.cc/Google_wallet.pdf
Hatforce

2011 Attacks and defenses in IPv6 local area networks (text in German)
Arthur Gervais
<KES> SecuMedia, IT security magazine of the German Federal Office for Information Security (BSI)

New Penetration Testing Business Model, Crowd-sourcing for IT-Security
Arthur Gervais
PenTest Magazine

Thesis Mentoring

Current PhD Students Rami Khalil, Lewis Gudgeon, Kaihua Qin, Alexei Zamyatin
Imperial College London

MSc/BSc Thesis Students at Imperial Aravind Jayadev Menon, Bogdan Stoicescu, Thibault Meunier, Krishi Shah, George Christoglou, Hongjiang Liu, Panayiotis Panayiotou, Henryk Hadass, Dylan Tracey, Joseph Katsioloudes

MSc/BSc Thesis Students at ETH Zurich	Luca Tondelli, Rami Khalil, Selma Steinhoff, Nicolas Badoux, Karl Wüst, Vasileios Glykantzis Alexandros Filios, Fabian Schewetofski, Lorenzo Wölckner, Mathias Wellig, Damian Gruber Guillaume Felley, Ferran Llamas, Alexandros Filios, Stathakopoulou Chrysoula, Jesse Badash

Teaching Experience

Lecturer

Principles of Decentralized Ledgers
Blockchain Security, Privacy, Scalability, Programmability
Imperial College London, Spring 2018, planned for 2019

Systems Security
Bitcoin Security and Privacy
ETH Zurich, Fall 2016

Blockchain and Internet of Things (BIoTs) Summerschool
ETH Zurich, Spring 2016

Primary School
Computer Science for children of the 4th and 5th grade
Vaduz, Lichtenstein, Fall 2016

Teaching Assistant

Information Security
ETH Zurich, Spring 2016

Foundations of Computer Science
ETH Zurich, Fall 2015, 2016

Security of Wireless Networks
ETH Zurich, Fall 2013, 2014

Design of Digital Circuits
ETH Zurich, Spring 2013

Introduction to Eiffel Programming
ETH Zurich, Fall 2016

Selected Skills

Languages

German:	Native speaker
French:	Bilingual
English:	Fluent
Spanish:	Intermediate

Technical

Programming:	Python, C/C++, Java, HTML, Java Script, CSS, Assembler
Network:	IPv4/v6, P2P, TCP, Routing
Security:	Bitcoin, SCADA, TLS, Web
Data Analysis:	Machine Learning basics
Operating Systems:	Linux, Mac OS, Windows

Selected Press

2018 **TV Interview on Blockchain Scalability**
Sky News

Ethereum Founder Acknowledges Promising Solution To Blockchains' Scalability Problem
Forbes

Ethereum's Raiden Network Has New Scaling Competiton
CoinDesk

New off-chain scaling solution, Liquidity Network aims to become the PayPal of Blockchain
International Business Times

2016 **Interview with the Swiss National Radio and Television (SRF)**
Blockchain Security and Privacy

Interview with the Austrian Science Radio Channel (ORF)
On the Security and Privacy of Proof of Work Blockchains

Interview and article with CoinDesk
On the Security and Privacy of Proof of Work Blockchains

2011 **Forbes Article about Hatforce**
Crowdsourcing meets Vulnerability Testing

Service

Program Committee
Blockchain Protocol Analysis and Security Engineering, BPASE'19
Computer and Communications Security, CCS'18
Bitcoin Workshop, BITCOIN'17
Cryptology and Network Security, CANS'17
Asia Conference on Computer and Communications Security**,** Shadow PC, ASIACCS'17
International Workshop on Cryptocurrencies and Blockchain Technology, CBT'17
Proceedings on Privacy Enhancing Technologies Symposium, PoPETS'18

Organizing Committee
Blockchain Summerschool, EPFL and ETH, 2017
CryptoValley Conference on Blockchain Technology 2018

Other
EU Blockchain Observatory, overview and guiding on blockchain scalability and security topics
Working Group Blockchain / ICO, Switzerland, 2018, recommendations on future regulations

Reviewer
CCS, 2013-2018
USENIX, 2013-2016
IEEE S&P (Oakland), 2013-2015
NDSS, 2013-2015
Euro S&P, 2015-2016
Mobicom, 2012, 2013, 2015
ESORICS, 2013-2014
PETS, 2014-2015
WiSec, 2013
ACSAC, 2014
ACNS, 2013
ICDCS, 2015
IJIS, 2016
JCST, 2016

Open Source Contributions
Massive Online Learning Platform for Blockchain Smart Contracts
https://achievement.network

Revive: Rebalancing Off-Blockchain Payment Networks
https://github.com/rami-khalil/revive

Blockchain Simulator
https://github.com/arthurgervais/Bitcoin-Simulator

Web Search Obfuscation Quantification Tool
http://arthur.gervais.cc/WebSearchPrivacy.zip

Web Adblocker Privacy Quantification Tool
http://arthur.gervais.cc/AdblockerPrivacy.zip

SCAPY Module for Modbus TCP
https://github.com/secdev/scapy/blob/master/scapy/contrib/modbus.py

References
References can be provided upon request.