Karl Wüst

Education

11/2016 – 09/2021 **PhD in Computer Science**, *System Security Group, ETH Zurich*.
Research in the area of Blockchain and Trusted Computing. Projects include the development of private and regulated transaction for use in centrally issued cryptocurrencies [6], privacy preserving lightweight clients for Bitcoin and Zcash [5, 7], and smart contract platforms for computationally complex smart contracts [2] and for legacy cryptocurrencies [1].

02/2015 – 07/2016 **MSc in Computer Science**, *ETH Zurich*.
Information Security Track, GPA: 5.57/6.0
Thesis **"Security of Blockchain Technologies"** (Grade 6.0/6.0):
Quantification of the security of Proof of Work based Blockchains with regards to double-spending and selfish mining based on optimal adversarial strategies (cf. [13]). Additionally, a practical security analysis of Ethereum and Stellar that lead to the discovery of three vulnerabilities in Ethereum (cf. [12]).

09/2011 – 02/2015 **BSc in Computer Science**, *ETH Zurich*.
GPA: *5.41/6.0*
Thesis **"Forensic File Repair"** (Grade 6.0/6.0):
Design and implementation of a novel approach to file repair that does not require knowledge about the file format, only access to a file viewer binary and some uncorrupted files (cf. [11]).

Employment

from 10/2021 **Tenure-Track Faculty**, *CISPA Helmholtz Center for Information Security*, Saarbrücken, Germany.

11/2016 – 09/2021 **Research Assistant**, *System Security Group, ETH Zurich*, Zurich, Switzerland.

02/2013 – 12/2014 **Student Teaching Assistant**, *ETH Zurich*, Zurich, Switzerland.

11/2007 – 04/2013 **Ski Instructor**, *Mountain Adventures AG*, Flims/Laax, Switzerland.

Publications

[1] **Karl Wüst**, Loris Diana, Kari Kostiainen, Ghassan Karame, Sinisa Matetic, and Srdjan Capkun. Bitcontracts: Supporting Smart Contracts in Legacy Blockchains. In *Network and Distributed System Security Symposium (NDSS)*, 2021.

[2] **Karl Wüst**, Sinisa Matetic, Silvan Egli, Kari Kostiainen, and Srdjan Capkun. ACE: Asynchronous and Concurrent Execution of Complex Smart Contracts. In *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, 2020.

[3] Sarah Allen, Srdjan Čapkun, Ittay Eyal, Giulia Fanti, Bryan A Ford, James Grimmelmann, Ari Juels, Kari Kostiainen, Sarah Meiklejohn, Andrew Miller, Eswar Prasad, **Karl Wüst**, and Fan Zhang. Design choices for central bank digital currency: Policy and technical considerations. Technical report, The Brookings Institution, 2020.

[4] Vasilios Mavroudis, **Karl Wüst**, Aritra Dhar, Kari Kostiainen, and Srdjan Capkun. Snappy: Fast on-chain payments with practical collaterals. In *Network and Distributed System Security Symposium (NDSS)*, 2020.

[5] Sinisa Matetic, **Karl Wüst**, Moritz Schneider, Kari Kostiainen, Ghassan Karame, and Srdjan Capkun. BITE: Bitcoin Lightweight Client Privacy using Trusted Execution. In *28th USENIX Security Symposium*, 2019.

[6] **Karl Wüst**, Kari Kostiainen, Vedran Capkun, and Srdjan Capkun. PRCash: Fast, Private

and Regulated Transactions for Digital Currencies. In *International Conference on Financial Cryptography and Data Security*, 2019.

[7] **Karl Wüst**, Sinisa Matetic, Moritz Schneider, Ian Miers, Kari Kostiainen, and Srdjan Capkun. ZLiTE: Lightweight Clients for Shielded Zcash Transactions using Trusted Execution. In *International Conference on Financial Cryptography and Data Security*, 2019.

[8] Patrick McCorry, Chris Buckland, Surya Bakshi, **Karl Wüst**, and Andrew Miller. You sank my battleship! A case study to evaluate state channels as a scaling solution for cryptocurrencies. In *3rd Workshop on Trusted Smart Contracts*, 2019.

[9] **Karl Wüst** and Arthur Gervais. Do you need a Blockchain? In *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*, 2018.

[10] Hubert Ritzdorf, **Karl Wüst**, Arthur Gervais, Guillaume Felley, and Srdjan Čapkun. TLS-N: Non-repudiation over TLS Enabling Ubiquitous Content Signing. In *Network and Distributed System Security Symposium (NDSS)*, 2018.

[11] **Karl Wüst**, Petar Tsankov, Saša Radomirović, and Mohammad Torabi Dashti. Force Open: Lightweight black box file repair. *Digital Investigation*, 20:S75–S82, 2017.

[12] **Karl Wüst** and Arthur Gervais. Ethereum Eclipse Attacks. Technical report, ETH Zurich, 2016.

[13] Arthur Gervais, Ghassan O Karame, **Karl Wüst**, Vasileios Glykantzis, Hubert Ritzdorf, and Srdjan Čapkun. On the Security and Performance of Proof of Work Blockchains. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 2016.

Talks

2021 NDSS. *Bitcontracts: Supporting Smart Contracts in Legacy Blockchains*.

2020 IC3 Retreat. *Bitcontracts: Supporting Smart Contracts in Legacy Blockchains*.

2020 CCS. *ACE: Asynchronous and Concurrent Execution of Complex Smart Contracts*.

2020 Heuking Kühn Lüer Wojtek (Law Firm) Webinar. *Do you need a Blockchain?*.

2020 IC3 Blockchain Summer Camp. *ACE: Asynchronous and Concurrent Execution of Complex Smart Contracts*.

2019 VISCon. *Do you need a Blockchain?*.

2019 AFT. *BITE: Bitcoin Lightweight Client Privacy using Trusted Execution*.

2019 Zcon1. *ZLiTE: Lightweight Clients for Shielded Zcash Transactions using Trusted Execution*.

2019 Financial Cryptography. *PRCash: Fast, Private and Regulated Transactions for Digital Currencies*.

2019 IC3 Retreat. *ZLiTE: Lightweight Clients for Shielded Zcash Transactions using Trusted Execution*.

2018 10 Jahre Blockchain (UZH ITSL & Legal Hackers). *Intro to Blockchain Technology*.

2018 CVCBT. *Do you need a Blockchain?*.

2018 NDSS. *TLS-N: Non-repudiation over TLS Enabling Ubiquitous Content Signing*.

2018 BPASE. *TLS-N: Non-repudiation over TLS Enabling Ubiquitous Content Signing*.

2018 High-Tech Connect Cyber Intelligence Event. *Blockchain Applications & Security*.

2017 DFRWS Europe. *Force Open: Lightweight black box file repair*.

Service

Reviewer

PC Member	ICBC (2019)
Reviewer	TDSC (2018), ITSM (2019), IET Information Security (2019), WWWJ (2020), TIFS (2021)
Ext. Reviewer	USENIX Security (2019)
Subreviewer	USENIX Security (2017, 2018, 2019), IEEE S&P (2017, 2018, 2019, 2020, 2021, 2022), CCS (2016, 2018), NDSS (2018, 2019, 2020, 2021, 2022), Euro S&P (2021), Financial Cryptography (2017, 2018), Mobicom (2017, 2018, 2019, 2021), WiSec (2018, 2020), ESORICS (2020), RAID (2018), CBT (2019)

Supervised Student Theses

2020	M. Grabocka. *Online Payments with TEE*. Semester Research Project.
2019	U. Tesic. *GPU Accelerated zk-SNARKs*. MSc Thesis.
2019	L. Diana. *Expressive Smart Contracts for Bitcoin*. MSc Thesis.
2019	A. Roque. *On the Security of DAG-based Blockchains*. BSc Thesis.
2018	S. Egli. *SGX-Ethereum*. MSc Thesis.
2018	N. Delius. *On the Security of Automated Bike Rental Services*. BSc Thesis.
2018	D. Brütsch. *Ethereum Block Verification*. MSc Thesis.
2018	F. de Rubeis. *Implementation of TLS-N for OpenSSL*. MSc Thesis.
2018	C. Bohn. *Implementation of an SGX-based Blockchain*. BSc Thesis.
2017	L. Tondelli. *On the Security, Performance and Stability of Bitcoin-NG*. MSc Thesis.
2017	S. Steinhoff. *Linkable Ring Signature using Ethereum Smart Contracts*. BSc Thesis.
2017	M. Göller. *TLS-N Proof Verification in EVM*. Semester Research Project.
2016	G. Felley. *TLS Proof*. Semester Research Project.

Teaching

2020	**Information Security Lab**, *Teaching Assistant*.
2018 – 2021	**Information Security**, *Teaching Assistant*.
2017 – 2020	**System Security**, *Head Teaching Assistant*.
2013 – 2014	**Introduction to Programming**, *Student TA*.
2013	**Data Structures & Algorithms**, *Student TA*.

Other

03/2019 – 02/2021	**Chairman of the Studies Committee**, *ETH Zurich, Department of CS*.
01/2018 – 02/2021	**Member of the Studies Committee**, *ETH Zurich, Department of CS*, Representative of the Scientific Staff.
01/2018 – 02/2021	**Member of the Department Conference**, *ETH Zurich, Department of CS*, Representative of the Scientific Staff.
03/2014 – 03/2015	**President**, *Verein der Informatik Studierenden an der ETH Zürich (VIS)*, VIS is the official CS student association at ETH Zurich.
11/2014 – 05/2015	**Member of the Selection Committee for Assistant Professorships in Computer Science**, *ETH Zurich, Department of CS*, Student Representative.
03/2013 – 09/2014	**Member of the Studies Committee**, *ETH Zurich, Department of CS*, Student Representative.
03/2013 – 09/2014	**Member of the Department Conference**, *ETH Zurich, Department of CS*, Student Representative.

03/2013 – 03/2014 **Board Member for University Policies**, *Verein der Informatik Studierenden an der ETH Zürich (VIS)*, VIS is the official CS student association at ETH Zurich.

Honors and Awards

2020 **ETH Spark Award Finalist**.
The Spark Award is an award for the best invention at ETH. Nominated for [4] and placed in top 5 out of 220 nominations.

2016 **Honorary Membership of VIS**.
Awarded lifelong honorary membership for extraordinary contributions.

Languages

German Native

English Fluent