✉ sergey.s.tikhomirov@gmail.com
s-tikhomirov.github.io
in sergeitikhomirov
serge_tikhomirov

Sergei Tikhomirov

To make blockchains useful, we must look beyond the hype and understand their drawbacks and trade-offs. Having both academic and industrial background with a focus on security and privacy, I gain and share deep technical knowledge on blockchain technologies.

Professional Experience

Oct 2016 – present **PhD candidate**, *University of Luxembourg*, Esch-sur-Alzette, Luxembourg.

- Security and privacy in Bitcoin and other blockchain networks
- Privacy-preserving cryptocurrencies (Dash, Monero, Zcash), incl. under a Zcash Foundation grant ("Empirical analysis of the Zcash blockchain" project, awarded Q4 2017)
- Secure programming practices in Ethereum
- Vulnerabilities in Solidity code, attacks on smart contracts
- Domain-specific languages for financial applications

Feb 2013 – Jul 2016 **Security Researcher**, *SmartDec*, Moscow.

- Doing research on software weaknesses in mobile and web applications
- Developing a tool for automatic detection of vulnerabilities and backdoors
- Performing security audits of Ethereum smart contracts (tokens, crowdsales, etc)
- Testing software for compliance with information security requirements

Oct 2014 – present **Author and Translator**, *Bitnovosti.com*.
Bitnovosti is the leading Russian-language website on Bitcoin and related topics

- Writing and translating articles on blockchain technologies

Publications

2018 **S. Tikhomirov, E. Voskresenskaya, I. Ivanitskiy, R. Takhaviev, E. Marchenko, Y. Aleksandrov**, *SmartCheck: Static Analysis of Ethereum Smart Contracts*, WETSEB-2018.

2018 **A. Biryukov, D. Khovratovich, S. Tikhomirov**, *Privacy-preserving KYC on Ethereum*, ERCIM Blockchain Workshop 2018.

2017 **S. Tikhomirov**, *Ethereum: State of Knowledge and Research Perspectives*, FPS-2017.

2017 **A. Biryukov, D. Khovratovich, S. Tikhomirov**, *Findel: Secure Derivative Contracts for Ethereum*, WTSC-2017.

Education

2008–2013 **Lomonosov Moscow State University**, *Faculty of Computational Mathematics and Cybernetics*, Department of Automation for Scientific Research. GPA 4.4 out of 5.0.

Master Thesis

Title *Optimization of investment portfolio*

Supervisor Professor Andrey Lukyanitsa

Description Applying genetic algorithms to the problem of investment portfolio optimization

Projects

Basic block radio, *A Russian-language podcast on blockchain technologies (8k monthly listeners)*, https://basicblockradio.libsyn.com/.

CryptoLUX asset management, *A PoC privacy-preserving smart contract solution for asset management*, Joint 1st prize at the Luxblock hackathon, 2017 (CryptoLUX team).

Pethreon, *A smart contract for recurring payments*, https://github.com/s-tikhomirov/pethreon.

Smart contract languages, *A curated list of smart contract programming languages*, https://github.com/s-tikhomirov/smart-contract-languages.

Solidity LaTeX highlighting, *A template for Solidity code examples for LaTeX*, https://github.com/s-tikhomirov/solidity-latex-highlighting.

Massive Online Open Courses (completed, selection)

Cybersecurity Specialization, *University of Maryland, College Park*.
Included courses on Software Security, Cryptography, Hardware Security, Usable Security, and a Capstone project. All mentioned courses passed in 2014 – 2016 and provided by Coursera.

Bitcoin and Cryptocurrency Technologies, *Princeton University*.

Malicious Software and its Underground Economy, *University of London*.

Cryptography I, *Stanford University*.

Functional Programming Principles in Scala, *École Polytechnique Fédérale de Lausanne*.

Functional Programming Design in Scala, *École Polytechnique Fédérale de Lausanne*.

Cloud Computing Concepts, *University of Illinois at Urbana-Champaign*.

Algorithms: Design and Analysis, *Stanford University*.

Algorithms, Part I, *Princeton University*.

Mining Massive Datasets, *Stanford University*.

Modern Combinatorics, *Moscow Institute of Physics and Technology*.

Computer Skills

Programming Solidity, Python, Java, Scala, C, C++, C#

Markup LaTeX, Markdown, XML / XSD, HTML

VCS git

Languages

English: fluent, German: fluent, Russian: native, French: basic