Sergei Tikhomirov

Blockchain Researcher

Berlin, Germany
sergey.s.tikhomirov@gmail.com
s-tikhomirov.github.io/about/
sergeitikhomirov
s-tikhomirov

My mission is to advance individual financial sovereignty by combining deep research with pragmatic implementation.

Professional Experience

2021 – 2022 **Postdoctoral Researcher**, *Chaincode Labs*, New York, US.
- Co-authored a novel fee scheme against denial-of-service attacks in the Lightning Network

2020 – 2021 **Postdoctoral Researcher**, *University of Luxembourg*, Luxembourg.
- Modeled the balance probing privacy attack in the Lightning Network

2016 – 2020 **PhD Candidate**, *University of Luxembourg*, Luxembourg.
- Described a P2P-level transaction deanonymization method in Bitcoin, Monero, and Zcash
- Developed a vulnerability detection tool for Solidity smart contracts
- Designed a functional domain-specific language for financial contracts on Ethereum
- Worked as a TA for a computer networking course
- Supervised student projects on blockchain-related topics

2013 – 2016 **Information Security Analyst**, *SmartDec*, Moscow, Russia.
- Classified and formalized dangerous code patterns in various programming languages

Doctoral Thesis

Title *Security and Privacy of Blockchain Protocols and Applications*
Year 2020
Supervisor Professor Alex Biryukov

Selected Publications

2022 **C. Shikhelman, S. Tikhomirov**, *Unjamming Lightning: A Systematic Approach*.

2021 **A. Biryukov, G. Naumenko, S. Tikhomirov**, *Analysis and Probing of Parallel Channels in the Lightning Network*, FC 2022.

2020 **S. Tikhomirov, P. Moreno-Sanchez, M. Maffei**, *A Quantitative Analysis of Security, Anonymity and Scalability for the Lightning Network*, S&B 2020.

2019 **A. Biruykov, S. Tikhomirov**, *Deanonymization and linkability of cryptocurrency transactions based on network analysis*, Euro S&P 2019.

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

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

Education

2016–2020 **University of Luxembourg**, *Faculty of Science, Technology and Medicine*, Laboratory of Algorithmics, Cryptology and Security, PhD.

2008–2013 **Lomonosov Moscow State University**, *Faculty of Computational Mathematics and Cybernetics*, Department of Automation for Scientific Research, MSc, BSc.

Projects

Basic Block Radio, *A Russian-language podcast on blockchain technologies*, `https://basicblockradio.com/`.

LN Probing Simulator, *A simulator of probing attacks in the Lightning Network (Python)*, `https://github.com/s-tikhomirov/ln-probing-simulator`.

LN Jamming Simulator, *A jamming-focused Lightning Network simulator (Python)*, `https://github.com/s-tikhomirov/ln-jamming-simulator`.

LN Jamming Simulator (Rust), *A re-implementation of the jamming simulator in Rust*, `https://github.com/s-tikhomirov/ln-jamming-simulator-rust`.

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

Blockchain Podcasts, *A list of podcasts about blockchain / cryptocurrency*, `https://github.com/s-tikhomirov/blockchain-podcasts`.

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

Massive Online Open Courses (completed; selection)

Algorithms, Part I, *Princeton University*.

Algorithms: Design and Analysis, *Stanford University*.

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

Cryptography I, *Stanford University*.

Cybersecurity Specialization, *University of Maryland, College Park*.
Includes courses on Software Security, Cryptography, Hardware Security, and Usable Security.

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

Bitcoin and Cryptocurrency Technologies, *Princeton University*.

Programming Skills

Programming	`Rust, Python, Scala`
Markup / VCS	`LaTeX, Markdown, git`

Languages

English: fluent, German: intermediate, Russian: native

Nationality

Luxembourg (EU), Russia

Hobbies

Hiking, cycling, podcasting