

Sergei Tikhomirov

Blockchain Researcher

Berlin, Germany
✉ sergey.s.tikhomirov@gmail.com
📄 s-tikhomirov.github.io/about/
in [sergeitikhomirov](#)
🌐 [s-tikhomirov](#)

Professional Experience

- 2023 – present **Protocol Research Engineer**, *Status (Waku)*.
- Developed an incentivization strategy for a P2P messaging network
 - Co-authored academic papers about the Waku protocol
- 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*
Supervisor Prof. 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*.
- 2020 **S. Tikhomirov, P. Moreno-Sanchez, M. Maffei**, *A Quantitative Analysis of Security, Anonymity and Scalability for the Lightning Network*.
- 2019 **A. Biryukov, S. Tikhomirov**, *Deanonymization and Linkability of Cryptocurrency Transactions Based on Network Analysis*.
- 2018 **S. Tikhomirov, E. Voskresenskaya, I. Ivanitskiy, R. Takhaviev, E. Marchenko, Y. Aleksandrov**, *SmartCheck: Static Analysis of Ethereum Smart Contracts*.
- 2017 **S. Tikhomirov**, *Ethereum: State of Knowledge and Research Perspectives*.
- 2017 **A. Biryukov, D. Khovratovich, S. Tikhomirov**, *Findel: Secure Derivative Contracts for Ethereum*.

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>.

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

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

Programming Skills

Code Python, Rust, Scala, Nim

Markup LaTeX, Markdown

VCS git

Languages

English: fluent, German: intermediate, Russian: native

Nationality

Luxembourg (EU), Russia

Hobbies

Hiking, cycling, podcasting