Sergei Tikhomirov

Blockchain Protocol Researcher

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

I'm a blockchain researcher and protocol engineer focused on security, privacy, and scalability. I've worked across diverse topics—from smart contract security to P2P network privacy and protocol design. I currently develop incentivized communication protocols at Waku, using libp2p and zero-knowledge tools. I closely follow rollup and ZK developments, which I see as key to scaling blockchains while preserving decentralization. Previously at Chaincode Labs (Bitcoin Core contributors) and the University of Luxembourg (PhD), I've published peer-reviewed research on Ethereum security, deanonymization, and Lightning Network attacks. I'm also the co-host of Basic Block Radio, a technical podcast covering rollups, ZK, MEV, and more.

Professional Experience

2023 – present **Protocol Research Engineer**, *Waku (IFT / Status)*.
- Implemented a proof-of-concept incentivization protocol in Nim for Waku light nodes
- Developed smart contracts in Solidity for RLN, Waku's ZK-based spam protection
- Co-authored academic papers accepted to peer-reviewed venues (IEEE DAPPS, DLT)

2021 – 2022 **Postdoctoral Researcher**, *Chaincode Labs*, New York, US.
- Proposed a novel fee scheme against denial-of-service attacks in the Lightning Network (under development by major Lightning implementations)

2020 – 2021 **Postdoctoral Researcher**, *University of Luxembourg*, Luxembourg.
- Modeled the balance probing privacy attack in the Lightning Network
- Contributed to a chapter on security and privacy for "Mastering the Lightning Network"

2016 – 2020 **PhD Candidate**, *University of Luxembourg*, Luxembourg.
- Described a P2P-level 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 teaching assistant 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

Open Source Contributions

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`.

Podcast

Basic Block Radio, *A tech-focused Russian-language podcast started in 2017 with 200+ episodes and guests from Matter Labs, Zerion, Solana, 1inch, Aave, Chainlink, and more*, `https://basicblockradio.com/`.

Selected Publications

2024 **H. Cornelius, S. Tikhomirov, A. Revuelta, S. P. Vivier, A. Challani**, *The Waku Network as Infrastructure for dApps*, DLT 2024.

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*, IEEE EuroS&P, workshop.

2019 **A. Biruykov, S. Tikhomirov**, *Deanonymization and Linkability of Cryptocurrency Transactions Based on Network Analysis*, IEEE EuroS&P.

2018 **S. Tikhomirov, E. Voskresenskaya, I. Ivanitskiy, R. Takhaviev, E. Marchenko, Y. Aleksandrov**, *SmartCheck: Static Analysis of Ethereum Smart Contracts*, WETSEB 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*, FC 2017, workshop.

Education

2016–2020 **University of Luxembourg**, Laboratory of Algorithmics, Cryptology and Security, PhD: Security and Privacy of Blockchain Protocols and Applications. Advisor: Prof. Alex Biryukov.

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

Programming Skills

Code `Solidity, Python (network simulations), Nim (libp2p), Rust`

Markup `LaTeX, Markdown`

VCS `git`

Languages

English: fluent, German: intermediate, Russian: native

Nationality

Luxembourg (EU), Russia

Hobbies

Hiking, cycling, podcasting