

Dr. Orfeas Stefanos Thyfronitis Litos

o.thyfronitis-litos@imperial.ac.uk | github.com/OrfeasLitos | ORCID: 0000-0002-8229-297X

EMPLOYMENT

Research Associate (80% Full-Time Equivalent)

Oct. 2022 – Nov. 2025

Imperial College London

- BLOCC: Designed a blockchain-based system for journaling sensor data for the shipping industry
- Assistant Supervisor: supervised of the BSc and MSc dissertations of 4 students

Blockchain Science Consultant

Mar. 2022 – present

Common Prefix

- Incentive analysis of a stake-based threshold protocol
- Trustless Bitcoin bridging for Babylon
- Direct Bitcoin Staking for Sidechains & Liquid Staking Tokens
- Whitepaper for [Phygital Redemption Protocol](#)
- Cryptocurrency bridge for Blockchain interoperability

Research Associate

Oct. 2021 – Sep. 2022

Technical University of Darmstadt

- Designed a novel commit-chain for Bitcoin
- Formally verified the Lightning Network in [Why3](#)
- Supervisor of MSc dissertation of 1 student

Teaching Support

Sep. 2017 – May 2020

University of Edinburgh

- Teaching Assistant, Marker & Exam Marker for the Introduction to Modern Cryptography course
- Teaching Assistant & Tutor for the Computer Security course

High School Tutor

Sep. 2011 – May 2016

Athens, Private

- Mathematics, Physics, Chemistry, Biology

QUALIFICATIONS

Doctor of Philosophy

Informatics, University of Edinburgh

Thesis: [Reclaiming Scalability and Privacy in the Decentralized Setting](#)

May 2017 – Sep. 2021

- Supervisor of MSc dissertation of 1 student
- Schools & Workshops successfully completed: [VeriCrypt: An Introduction to Tools for Verified Cryptography 2020](#), [Summer School on real-world crypto and privacy 2018](#)

Graduate Degree

Electrical and Computer Engineering, National Technical University of Athens

Thesis: [Trust Is Risk: A Decentralized Financial Trust Platform](#)

Sep. 2010 – Feb. 2017

General Assembly Proposal: Direct student voting on acts, replacing election of representatives

Erasmus Placement

Informatics Engineering, Engineering Institute of Porto

Machine Learning Applications

Sep. – Dec. 2016

Erasmus

Informatics Engineering, Polytechnic University of Valencia

Sep. 2013 – June 2014

Awards

- [Bitcoin Research Prize 2025](#) for BitVM2

Invited Talks

- Keynote on Remote Staking at [MARBLE](#) 4 Jul 2025
- [Non-financial applications of blockchains](#) @ TEDxRutlish School 19 Dec 2024
- Presentation on online safety at Millbank Academy workshop 2023

Committee Memberships

- Programme Committee of IEEE Symposium on Security and Privacy '26
- Programme Committee of Financial Cryptography and Data Security (FC) '25 – '26
- Programme Committee of Crypto for Real World Assets (CRWA) '25
- Programme Committee and Session Chair of Scalability & Interoperability of Blockchains (SIB) '24
- Programme Committee of International Conference on Cryptology And Network Security (CANS) '24
- Technical Committee of International Conference on Blockchain and Cryptocurrency (ICBC) '24 – '25
- Department of Computing Equity, Diversity, and Culture Committee '23 – '24
- Europe Technology Policy Committee '23 – '24
 - * Contributor to the EU-US Trade and Technology Council on developing a taxonomy of critical terms related to artificial intelligence
- International Conference on Mathematical Research for Blockchain Economy (MARBLE) '22, '23 & '25
- Co-organizer of [decrypto seminar](#)

Subreviewer of academic articles

- Conferences: SBC '25, EC '25, FC '21 & '22, S&P '22, Eurocrypt '22, Crypto '21, ICDCS '21, AFT '21, CCS '20, CANS '17
- Journals: [TDSC](#), [TOPS](#), [JSys](#)

Contributions to open standards: [Bitcoin BIPs](#), [Lightning BOLTs](#)

ACADEMIC PUBLICATIONS (9 + 4, AUTHORS IN ALPHABETICAL ORDER EXCEPT FOR (*))

(*) Linus, R., Aumayr, L., Zamyatin, A., Pelosi, A., Avarikioti, Z., **Thyfronitis Litos, O. S.**, Maffei, M.: [BitVM2: Bridging Bitcoin to Second Layers](#). In: USENIX Security (2026). Also appeared in: Science of Blockchain Conference (2025)

Fabiański, G., Stefański, R., **Thyfronitis Litos, O. S.**: [A Formally Verified Lightning Network](#). In: Financial Cryptography and Data Security, Miyako Jima (2025)

Riahi, S., **Thyfronitis Litos, O. S.**: [Bitcoin Clique: Channel-free Off-chain Payments using Two-Shot Adaptor Signatures](#). In: Applied Cryptography and Network Security, Abu Dhabi (2024) and Science of Blockchain Conference (2024)

Avarikioti, Z., **Thyfronitis Litos, O. S.**: [Suborn Channels: Incentives Against Timelock Bribes](#). In: Financial Cryptography and Data Security, Grenada (2022)

Kiayias, A., **Thyfronitis Litos, O. S.**: [Composable Security Treatment of the Lightning Network](#). In: IEEE Computer Security Foundations Symposium, Virtual (2020)

Avarikioti, Z., **Thyfronitis Litos, O. S.**, Wattenhofer, R.: [Cerberus Channels: Incentivizing Watchtowers for Bitcoin](#). In: Financial Cryptography and Data Security, Kota Kinabalu (2020)

Kiayias, A., Livshits, B., Monteoliva Mosteiro, A., **Thyfronitis Litos, O. S.:** [A Puff of Steem: Security Analysis of Decentralized Content Curation](#). In: Tokenomics, International Conference on Blockchain Economics, Security and Protocols, Paris (2019)

Thyfronitis Litos, O. S., Zindros, D.: [Trust Is Risk: A Decentralized Financial Trust Platform](#). In: Financial Cryptography and Data Security International Conference, Malta (2017)

(*) Escudeiro, N., Escudeiro, P., Soares, F., **Thyfronitis Litos, O. S.,** Norberto, M., Lopes, J.: [Recognition of hand configuration: A critical factor in automatic sign language translation](#). In: Iberian Conference on Information Systems and Technologies, Lisbon (2017)

Kiayias, A., Teague, V., **Thyfronitis Litos, O. S.:** [Privacy Preserving Opinion Aggregation](#). Submitted for publication at ASIACCS'26

Kiayias, A., Schaller, M., **Thyfronitis Litos, O. S.:** [Elmo: Recursive Virtual Payment Channels for Bitcoin](#). Submitted for publication at ICBC'26

(*) Bal, E., Aumayr, L., İyidoğan, A., Scaffino, G., Karakuş, H., Aslan, C. E., **Thyfronitis Litos, O. S.:** [Clementine: A Collateral-Efficient, Trust-Minimized, and Scalable Bitcoin Bridge](#).

(*) Dong, X., Tas, N., **Thyfronitis Litos, O. S.,** Tse, D., Linus, R., Yang, L., Yu, M.: [Remote Staking with Economic Safety](#). To be submitted for publication. Also appeared in: Workshop on Scalability & Interoperability of Blockchains (2024)

(*) **Thyfronitis Litos, O. S.,** Wu, Z., Musumeci, A., Hu, S., Helsby, J., Breza, M., Knottenbelt, W.: [NodeChain: Cheap Data Integrity Without Consensus](#). Submitted for publication at DSN'26

SOFT SKILLS

Ability to work in a team	Effectively collaborate with researchers and industry partners
Ability to take initiative	Initiate projects, attract collaborators and see projects through
Experience in grant applications	Promote salient elements of relevant research to suitable funding bodies
Ability to work alone	Produce research on various topics with minimal third-party expertise available

LANGUAGES

English, Spanish	Fluent
French, Italian, German	Conversational
Greek	Maternal