

# Sergi Delgado Segura

---

CONTACT INFORMATION	Department of Computer Science, University College London. MPEB 622, Gower Street, London WC1E 6BT.	email: s.delgado@ucl.ac.uk personal website: srgi.me
RESEARCH INTERESTS	Privacy, Bitcoin, Cryptocurrencies, Security, Networks, Distributed systems.	
CURRENT POSITION	<b>University College London</b> , London, United Kingdom <i>Research Assistant (Postdoc), Information Security Group</i>	<b>October 2018 – Present</b>
EDUCATION	<b>Autonomous University of Barcelona</b> , Bellaterra, Barcelona, Spain <i>Doctor of Philosophy in Computer Science</i> <b>October 2015 – September 2018</b> <ul style="list-style-type: none"><li>• Advisors: Prof. Jordi Herrera Joancomartí and Prof. Guillermo Navarro Arribas</li></ul> <b>University of Illinois at Urbana-Champaign</b> , Champaign, Illinois, United States of America <i>Research stay</i> <b>August 2017 – December 2017</b> <ul style="list-style-type: none"><li>• Advisor: Prof. Andrew Miller</li></ul> <b>Open University of Catalonia</b> , Barcelona, Spain <i>Master's Degree in Computer Security</i> <b>September 2014 – July 2015</b> <b>Autonomous University of Barcelona</b> , Bellaterra, Barcelona, Spain <i>Bachelor's degree in Computer Engineering</i> <b>September 2008 – July 2014</b>	
SELECTED PUBLICATIONS	<b>Delgado-Segura, S.</b> , Pérez-Solà, C., Herrera-Joancomartí, J., and Navarro-Arribas, G. (2016). “Bitcoin Private Key Locked Transactions”, <i>Information Processing Letters</i> , 2018. <a href="https://doi.org/10.1016/j.ip1.2018.08.004">https://doi.org/10.1016/j.ip1.2018.08.004</a> <b>Delgado-Segura, S.</b> , Pérez-Solà, C., Navarro-Arribas, G, Herrera-Joancomartí, J. (2018). “Analysis of the Bitcoin UTXO set”, <i>The 5th Workshop on Bitcoin and Blockchain Research (BITCOIN'18)</i> , 2018. <a href="http://fc18.ifca.ai/bitcoin/papers/bitcoin18-final6.pdf">http://fc18.ifca.ai/bitcoin/papers/bitcoin18-final6.pdf</a> <b>Delgado-Segura, S.</b> , Pérez-Solà, C., Herrera-Joancomartí, J, Navarro-Arribas, G, and Borrell J. (2018). “Cryptocurrency networks: a new P2P paradigm”, <i>Mobile Information Systems</i> , 2018. <a href="http://dx.doi.org/doi:10.1155/2018/2159082">http://dx.doi.org/doi:10.1155/2018/2159082</a> <b>Delgado-Segura, S.</b> , Pérez-Solà, C., Navarro-Arribas, G, and Herrera-Joancomartí, J. (2017). “A fair protocol for data trading based on Bitcoin transactions”, <i>Future Generation Computer Systems</i> , 2017, ISSN 0167-739X. <a href="http://dx.doi.org/10.1016/j.future.2017.08.021">http://dx.doi.org/10.1016/j.future.2017.08.021</a> . <b>Delgado-Segura, S.</b> , Tanas, C. and Herrera-Joancomartí, J. (2016). “Reputation and Reward: Two Sides of the Same Bitcoin”, <i>Sensors</i> , 16(6), p.776. <a href="http://www.mdpi.com/1424-8220/16/6/776">http://www.mdpi.com/1424-8220/16/6/776</a> Tanas, C., <b>Delgado-Segura, S.</b> and Herrera-Joancomartí, J. (2015). “An Integrated Reward and Reputation Mechanism for MCS Preserving Users' Privacy”, <i>International Workshop on Data Privacy Management</i> (pp. 83-99). Springer International Publishing. <a href="https://link.springer.com/chapter/10.1007/978-3-319-29883-2_6">https://link.springer.com/chapter/10.1007/978-3-319-29883-2_6</a>	
PREPRINTS	Pérez-Solà, C., <b>Delgado-Segura, S.</b> , Navarro-Arribas, G. and Herrera-Joancomartí, J. (2018). “Another coin bites the dust: An analysis of dust in UTXO based cryptocurrencies”, <i>IACR Cryptology ePrint Archive</i> , 2018, 513. <a href="https://eprint.iacr.org/2018/513.pdf">https://eprint.iacr.org/2018/513.pdf</a> Pérez-Solà, C., <b>Delgado-Segura, S.</b> , Navarro-Arribas, G. and Herrera-Joancomartí, J. (2017). “Double-spending Prevention for Bitcoin zero-confirmation transactions”, <i>IACR Cryptology ePrint Archive</i> , 2017, p. 394. <a href="https://eprint.iacr.org/2017/394.pdf">https://eprint.iacr.org/2017/394.pdf</a>	
TEACHING	<b>Autonomous University of Barcelona</b> , Bellaterra, Barcelona, Spain <i>Teaching Assistant: Information Security</i>	<b>October 2017 – September 2018</b>

**Autonomous University of Barcelona**, Bellaterra, Barcelona, Spain

*Teaching Assistant: Information Security*

**October 2016 – September 2017**

**Autonomous University of Barcelona**, Bellaterra, Barcelona, Spain

*Teaching Assistant: Computer Networks*

**October 2015 – September 2016**

OTHER  
PROFESSIONAL  
EXPERIENCE

*Research technician*

**September 2014 – September 2015**

Research technician for different projects the department was involved in, such as the development of a active Delay Tolerant Network (aDTN), and an Ubiquitous Secure Electronic Voting platform (USev).

*System administrator*

**July 2013 – September 2014**

System administrator of a Master's degree department, giving support to different areas including: Moodle administration, web development (HTML, PHP, JS, CSS), database administration and help desk.

PROGRAMMING

Python, Bitcoin Scripting, L<sup>A</sup>T<sub>E</sub>X 2<sub>ε</sub>, Java, C, Bash, Docker.

PROJECTS

**bitcoin\_tools** [https://github.com/sr-gi/bitcoin\\_tools](https://github.com/sr-gi/bitcoin_tools)

Bitcoin tools is a Python library created for teaching and researching purposes. It's main objective is twofold. First it aims to ease the understanding of Bitcoin transaction creation, by using well-documented and easy to understand python code. Second, it aims to provide a tool able to create custom transactions / scripts. Either scriptSig and scriptPubKey can be built from human readable strings created using Script syntax.

**STATUS** <https://git.io/vAzHL>

STATUS (Statistical Analysis Tool for Utxo Set) is an open source tool that provides an easy way to access, decode and analyze data from the Bitcoin's utxo set.

STATUS is coded in Python 2 and works for both the existing versions of Bitcoin Core's utxo set, that is, the first defined format (versions 0.8 - 0.14) and the recently defined one (version 0.15).

STATUS reads from a LevelDB folder (usually located under .bitcoin/chainstate) and parses all the utxo entries into a json file. From the parsed file, STATUS allows you to perform two type of analysis, a utxo based one, and a transaction based one, by decoding all the parsed information from the chainstate.

PUBLIC PROFILES

**GitHub** <https://github.com/sr-gi>

**Bitcoin Stack Exchange** <https://bitcoin.stackexchange.com/users/30668/sr-gi>