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

University College London, London, United Kingdom

Research Associate (Postdoc), Information Security Group **October 2018 – Present**

Education

Autonomous University of Barcelona, Bellaterra, Barcelona, Spain

Doctor of Philosophy in Computer Science **October 2015 – September 2018**

- Advisors: Prof. Jordi Herrera Joancomartí and Prof. Guillermo Navarro Arribas

University of Illinois at Urbana-Champaign, Champaign, Illinois, United States of America

Research stay **August 2017 – December 2017**

- Advisor: Prof. Andrew Miller

Open University of Catalonia, Barcelona, Spain

Master's Degree in Computer Security **September 2014 – July 2015**

Autonomous University of Barcelona, Bellaterra, Barcelona, Spain

Bachelor's degree in Computer Engineering **September 2008 – July 2014**

Selected Publications

Delgado-Segura, S., Pérez-Solà, C., Herrera-Joancomartí, J., and Navarro-Arribas, G. (2016). "Bitcoin Private Key Locked Transactions", *Information Processing Letters*, 2018. https://doi.org/10.1016/j.ipl.2018.08.004

Delgado-Segura, S., Pérez-Solà, C., Navarro-Arribas, G, Herrera-Joancomartí, J. (2018). "Analysis of the Bitcoin UTXO set", *The 5th Workshop on Bitcoin and Blockchain Research (BITCOIN'18)*, 2018. http://fc18.ifca.ai/bitcoin/papers/bitcoin18-final6.pdf

Delgado-Segura, S., Pérez-Solà, C., Herrera-Joancomartí, J, Navarro-Arribas, G, and Borrell J. (2018). "Cryptocurrency networks: a new P2P paradigm", *Mobile Information Systems*, 2018. http://dx.doi.org/doi:10.1155/2018/2159082

Delgado-Segura, S., Pérez-Solà, C., Navarro-Arribas, G, and Herrera-Joancomartí, J. (2017). "A fair protocol for data trading based on Bitcoin transactions", *Future Generation Computer Systems*, 2017, ISSN 0167-739X. http://dx.doi.org/10.1016/j.future.2017.08.021.

Delgado-Segura, S., Tanas, C. and Herrera-Joancomartí, J. (2016). "Reputation and Reward: Two Sides of the Same Bitcoin", *Sensors*, 16(6), p.776. http://www.mdpi.com/1424-8220/16/6/776

Tanas, C., **Delgado-Segura, S.** and Herrera-Joancomartí, J. (2015). "An Integrated Reward and Reputation Mechanism for MCS Preserving Users' Privacy", *International Workshop on Data Privacy Management* (pp. 83-99). Springer International Publishing. https://link.springer.com/chapter/10.1007/978-3-319-29883-2_6

Preprints

Pérez-Solà, C., **Delgado-Segura, S.**, Navarro-Arribas, G. and Herrera-Joancomartí, J. (2018). "Another coin bites the dust: An analysis of dust in UTXO based cryptocurrencies", *IACR Cryptology ePrint Archive*, 2018, 513. https://eprint.iacr.org/2018/513.pdf

Pérez-Solà, C., **Delgado-Segura, S.**, Navarro-Arribas, G. and Herrera-Joancomartí, J. (2017). "Double-spending Prevention for Bitcoin zero-confirmation transactions", *IACR Cryptology ePrint Archive*, 2017, p. 394. https://eprint.iacr.org/2017/394.pdf

Teaching

Autonomous University of Barcelona, Bellaterra, Barcelona, Spain

Teaching Assistant: Information Security **October 2017 – September 2018**

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, LaTeX 2$_\varepsilon$, Java, C, Bash, Docker.

Projects

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`