MARTÍN ARNALDO CERESA

Postdoc Researcher

martin.ceresa@imdea.org | +34-684319338 | Madrid, Spain

martinceresa | martinceresa | martinceresa.github.io

0000-0003-4691-5831

TECH LANGUAGES

Haskell | Coq | C | Lean | Agda

Go | Python | Rust | SML | Erlang

Z | CSP | TLA/TLA+

TECH STACK

ViM | XMonad | Hakyll | Git | LaTeX

Markdown | GNU/Linux | Emacs (Doom)

Org

LANGUAGES

Spanish: Native | **English:** Fluent

Portuguese: Basic

REFERENCES

Prof. César Sánchez

IMDEA Software Instute

cesar.sanchez@imdea.org

Prof. Mauro Jaskelioff

FCEIA & IOG

mjaskelioff@gmail.com

RESEARCH EXPERIENCE

Postdoc Researcher | IMDEA Software Institute

03 2023 – Ongoing | Madrid, Spain

- Ongoing research: formalizing Fraud Proof games in *Lean*.
- Studied offline monitoring properties of smart-contracts.
- Designed and implemented (in Haskell) Termina, a **non**-turing complete language for embedded software.
- Developed a simulation environment for Tezos smart contracts in *Go*.
- Guided a PhD student and three interns.

Research Programmer | IMDEA Software Institute

10 2022 – 02 2023 | Madrid, Spain

Implemented (in Rust) an intermediate layer expanding previous Tezos indexer features to monitor Tezos smart-contract with HLola.

Visiting PhD Student | IMDEA Software Institute

08 2020 – 09 2022 | Madrid, Spain

- Implemented a Coq library, *Multi*, to prove and reason about multi-contract interaction inspired on the computational model of the Tezos blockchain.
- Formalized (in Coq) different execution strategies, inspired by Tezos execution model, while introducing online and onchain smart-contract monitoring capabilities.
- Participated in the development of a theory to introduce online transaction monitors to blockchain technologies.
- Participated in the implementation and development of Setchain, a new Byzantine-tolerant distributed data-structure.

Undergraduate Intern | IMDEA Software Institute

03 2013 – 09 2013 | Madrid, Spain

- Expanded the strategy toolbox of EasyCrypt, a modern proof assistant for cryptrographers.
- Learned about modern cryptography proofs and game simulation-based proofs.
- Implemented (in OCaml) two different tactics: field/ring equality and automatic optimistic sampling.

EDUCATION

PhD in Informatics | UNR

04 2015 – 04 2023 Rosario, Argentina

- Thesis: Effectful Improvement Theory.
- Summary: An improvement theory for programming languages with algebraic effects.
- Advisor: PhD. Mauro Jaskelioff

Computer Science Degree | UNR

03 2008 – 03 2015 Rosario, Argentina

- Title: Simulation of Parallel Programs in Haskell
- Summary: A graphic library to observe and study the "parallel structure" of parallel programs in Haskell.
- GPA: 9.60

PROJECTS

Termina 2023 – Ongoing Private Repo

Transpiler from Termina to C plus a RTOS runtime for embedded systems. Designed and implemented in Haskell and runtime in C.

Smart Multi Contract Interaction

2021 – 2022

Designed and implemented a Coq library to reason about multi smart-contract interaction following the computational model of the Tezos Blockchain.

Haskell Lola 2019 – 2020

Designed the core structure implementing HLola. Implemented the main abstraction lifting generic types of Haskell employed as data-theories in Lola.

QuickFuzz 2016 – 2017

Out-of-the-box fuzzy generation of arbitrary files. Implemented Haskell arbitrary instances for arbitrary data structures in Haskell.

MegaDeTh 2016 – 2017

Aggressive and generic instance derivation for recursive and mutually dependent Haskell data-types. Implemented entirely in Template Haskell.

EasyCrypt 2013

Implemented tactics to simplify equations over rings and fields. Designed and implemented automatic optimistic sampling.

TEACHING EXPERIENCE

Adjunct Professor | UNR

2019 – 2021 Rosario, Argentina

- Parallel and Concurrent Programs: I taught the basic problems and solutions of concurrent and parallel programming in C and Erlang.
- Compilers Course: I followed closely the book *Modern Compilers Implementation in ML* by *Andrew Appel* implementing a full-fledged compiler for the language *Tiger* without optimizations.

Teacher Assistant | UNR

2011 – 2019 Rosario, Argentina

My responsibilities included: assisting and conducting laboratory hours, crafting tests and final projects and grading them.

- Data Structures and Algorithms in C
- Compiler Theory and Practice
- Concurrent Programming in Erlang
- Introduction to pure programming languages and Haskell
- Parallel Thinking in Haskell
- Introduction to Lambda Calculus, STLC, Intermediate functional programming in Haskell
- Introduction to Intuitionistic Logic
- Introduction to Generalized Abstract Data Types

COURSES

λ-Calculus and Reasonable Cost Models | UBA

2019 Buenos Aires, Argentina

DeepSpec Summer School | Princeton University

2018 New Jersey, United States of America

Introduction to basic and algebraic Topology | UNR

2018 Rosario, Argentina

Haskell's Type System/GHC and its extensions | ECI

2018 Río Cuarto, Argentina

FlexibleContexts, FlexibleInstances, GADTs, Phantom Types, RankNPoly, DataKinds, MultiParamTypeClasses, FunctionalDependencies, TypeFamilies.

Introduction to Category Theory and Agda | UNR

2016 Rosario, Argentina

Interactive Theorem Proving | UBA

2014 Buenos Aires, Argentina

Introduction to Coq. Natural deduction, Curry-Howard correspondence and Lambda Calculus.

Introduction to Type Theory in Agda | UNR

2011 Rosario, Argentina

PUBLICATIONS

Journal Articles

- M. Capretto, **M. Ceresa**, A. Fernández Anta, A. Russo, and C. Sánchez, "Improving blockchain scalability with the setchain data-type," *Distrib. Ledger Technol.*, Oct. 2023, Just Accepted. DOI: 10.1145/3626963.
- **M. Ceresa** and M. Jaskelioff, "Effectful improvement theory," *Sci. Comput. Program.*, vol. 217, p. 102 792, 2022. DOI: 10.1016/j.scico.2022.102792.
- G. Grieco, **M. Ceresa**, A. Mista, and P. Buiras, "Quickfuzz testing for fun and profit," *Journal of Systems and Software*, vol. 134, pp. 340–354, 2017. DOI: 10.1016/j.jss.2017.09.018.

Conference Proceedings

- M. Capretto, **M. Ceresa**, A. F. Anta, A. Russo, and C. Sánchez, "Setchain: Improving blockchain scalability with byzantine distributed sets and barriers," in *IEEE International Conference on Blockchain, Blockchain 2022, Espoo, Finland, August 22-25, 2022*, IEEE, 2022, pp. 87–96. DOI: 10.1109/BLOCKCHAIN55522.2022.00022.
- M. Capretto, **M. Ceresa**, and C. Sanchez, "Transaction monitoring of smart contracts," in *Runtime Verification*, T. Dang and V. Stolz, Eds., Cham: Springer International Publishing, 2022, pp. 162–180, ISBN: 978-3-031-17196-3.
- **M. Ceresa** and C. Sánchez, "Multi: A Formal Playground for Multi-Smart Contract Interaction," in *4th International Workshop on Formal Methods for Blockchains (FMBC 2022)*, Z. Dargaye and C. Schneidewind, Eds., ser. Open Access Series in Informatics (OASIcs), vol. 105, Dagstuhl, Germany: Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2022, 5:1–5:16, ISBN: 978-3-95977-250-1. DOI: 10.4230/OASIcs.FMBC.2022.5.
- **M. Ceresa**, F. Gorostiaga, and C. Sánchez, "Declarative stream runtime verification (hlola)," in *Programming Languages and Systems*, B. C. d. S. Oliveira, Ed., Cham: Springer International Publishing, 2020, pp. 25–43, ISBN: 978-3-030-64437-6.
- G. Grieco, **M. Ceresa**, and P. Buiras, "Quickfuzz: An automatic random fuzzer for common file formats," in *Proceedings of the 9th International Symposium on Haskell, Haskell 2016, Nara, Japan, September 22-23, 2016*, G. Mainland, Ed., ACM, 2016, pp. 13–20. DOI: 10.1145/2976002.2976017.