

Gabriel Coutinho de Paula

gcdepaula@protonmail.com
https://www.gcdepaula.com/
github.com/GCdePaula/
ethresear.ch/u/gcdepaula
x.com/GCdePaula_

About me

My work has taken me from programming languages to Ethereum. I design protocols that hold in adversarial environments, and I build the systems that run them.

Three examples. I co-authored Dave, a peer-reviewed, permissionless and Sybil-resistant fraud-proof algorithm. Dave came after our earlier primitive proved too slow to settle under sustained attack. I built the proof system securing a Stage-2 rollup on Ethereum mainnet. And I shipped a high-throughput, low-latency app-specific sequencer that preserves censorship resistance and settlement. All of it open-source, and argued out in public.

The systems were raised rather than architected top-down. I learned this discipline during my Master's in programming languages under Professor Roberto Ierusalimschy, creator of Lua, a programming language raised the same way.

Experience

Cartesi

Research Lead — Jan 2025 — present
Lead Blockchain Researcher & Engineer — Oct 2021 — Dec 2024
Software Engineer (part-time) — Jun 2020 — Sep 2021

I set research priorities and coordinate the work of a small research team, and have managed and mentored engineers, alongside research, writing, and shipping software. Owned the proof-system roadmap from research concept to live mainnet; now doing the same for the sequencing layer.

Algorithm Design & Adversarial Analysis Co-authored the *Dave algorithm* (peer reviewed, ACM), a permissionless, Sybil-resistant dispute-resolution primitive. Built the threat models it rests on: censorship budgets, resource-exhaustion vectors, and Sybil coordination.

Proof System Implementation Implemented PRT end-to-end, on-chain and off: the Solidity dispute engine (a multi-level bisection game that narrows a disputed execution down to the single RISC-V instruction where parties diverge) and the Rust client that drives it. This code secures Cartesi's Honeypot, a Stage-2 rollup tracked by L2BEAT and operated as a public mainnet break-it bounty.

Sequencing Designed, built, and deployed Cartesi's app-specific *sequencer*, preserving proof-system compatibility and L1 forced inclusion. Live on Sepolia. Benchmarks: >14K signed transfers/sec (unsaturated), 12 ms processing latency, 50 MB peak memory. Sub-cent per operation at mainnet costs, with fees designed to deter spam.

Public Research Analyses on ethresear.ch that drew technical responses from researchers at Offchain Labs, OP Labs, L2BEAT and RISC Zero, and helped shape the later discussion of fraud-proof trade-offs. Presented at Devcon SEA 2024; debated at EthCC 2024.

Papers

Dave: a decentralized, secure, and lively fraud-proof algorithm — Jan 2026
ACM Distributed Ledger Technologies Fraud-proof algorithm achieving 1-of-N security with low participation costs: settlement delay and defender effort scale logarithmically in Sybils; adversary expenditure grows exponentially relative to defender effort.

A Foreign Function Interface for Pallene — Oct 2022
Brazilian Symposium on Programming Languages (SBLP)
Designed and implemented C interoperability for Pallene, using the C compiler to check function bindings and support C macros. Best Non-Student Paper Award. PDF.

Education

Computer Science, M.Sc.

PUC-Rio 2019 — 2021

Advisor Professor Roberto Ierusalimschy.

Thesis A Foreign Function Interface for Pallene — C interoperability that marks exactly where safety ends. Dissertation and paper (Best Non-Student Paper Award, SBLP).

Focus Programming language theory, virtual machines, compiler design; formal specification of cross-language interfaces.

Computer Engineering, B.Eng.

PUC-Rio 2012 — 2018

Research Middleware for IoT, Prof. Markus Endler; Computational chemistry, Prof. Bruno Horta.

Internship Apple Developer Academy; four-time Apple WWDC scholarship winner.

Teaching Signals & Systems TA, four semesters.

Essays

Best of Both Worlds? A Measured Review of Non-Interactive ZK Fraud Proofs Sep 2025

Essay and discussion Analyzed how censorship, Sybil attacks, and competition for proving rewards affect security, progress, and participation costs under an explicit threat model. Drew responses from RISC Zero/Boundless and L2BEAT.

The Dave Algorithm — Triumphing over Sybils with a Laptop and a Small Collateral Feb 2025

Essay and discussion Explained the algorithm's mechanisms and practical trade-offs, including why a single honest validator can defend against many coordinated adversaries. The discussion includes a detailed technical exchange with cryptographer Victor Shoup (then Offchain Labs).

Enforceable Human-Readable Transactions Feb 2025

Essay and discussion Proposed cryptographically binding human-readable descriptions to transactions, reducing reliance on front ends to explain what users are signing.

Fraud Proofs Are Broken, but we can fix them Apr 2024

Essay and discussion Examined security, settlement-time, and participation-cost trade-offs in the designs proposed at the time, including our own. Drew responses from OP Labs and from Ed Felten (Offchain Labs), and helped shape the subsequent discussion of the fraud-proof trilemma.

Scaling Content: How to truly tackle blockchain's scalability problem Jan 2022

Personal blog Examined how software ecosystems preserve knowledge through abstractions, and argued for RISC-V execution environments to make that existing software available to Ethereum.

Talks

The Dave Algorithm Nov 2024

Devcon SEA presentation video & slides.

Proof It Debate Jul 2024

Modular Security (EthCC Brussels) debate with Justin Drake, Ed Felten, John Adler and Mark Tyneway; moderated by Luca Donno.

Modular Security Interview Jul 2024

The Defiant with Luca Donno.

We Need To Talk About Fraud Proofs Apr 2024

TheRollup podcast.

Permissionless Refereed Tournaments, a new fraud-proof primitive Nov 2023

L2Days (Devconnect Istanbul) presentation.