Gabriel Coutinho de Paula

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

About me

I design adversary-resilient algorithms and implement them end-to-end, from formal threat models to production smart contracts and off-chain systems.

The method runs from theory to production. I co-authored the Dave algorithm (a dispute-resolution primitive with a proven exponential cost asymmetry against Sybil adversaries) after our earlier primitive proved too slow to settle under sustained attack. Dave cut the delay constant by an order of magnitude.

And I designed, built, and deployed Cartesi's app-specific sequencer: low-latency, high-throughput rollup infrastructure that preserves proof-system compatibility and L1 forced inclusion.

I developed this discipline (iterating between design, adversarial analysis, and low-level implementation) during my Master's in programming languages under Professor Roberto Ierusalimschy, creator of the Lua programming language.

Experience

Cartesi

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

Owned the proof system roadmap and drove it 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 novel dispute-resolution primitive that is permissionless and Sybil resistant. Built the threat models it rests on: censorship budgets, resource-exhaustion vectors, Sybil coordination. Designed Cartesi's app-specific *sequencer* that preserves a rollup's two core security guarantees: settlement (proof system compatible) and censorship resistance (L1 forced inclusion).

Protocol 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. Shipped the *sequencer* (live on Sepolia): >14K signed transfers/sec (unsaturated), 12 ms processing latency, 50 MB peak memory; sub-cent per operation (mainnet costs), with fees designed to make spam economically infeasible.

Public Research Discourse Published analyses on ethresear.ch that shaped how the L2 community evaluates fraud-proof trade-offs, drawing technical responses from cryptographer Victor Shoup (NYU; then Offchain Labs), OP Labs, and L2BEAT. Debated Justin Drake (Ethereum Foundation), Ed Felten (Princeton, Arbitrum co-founder), John Adler (Fuel, Celestia), and Mark Tyneway (Optimism) with Luca Donno (L2BEAT) as moderator at EthCC. Presented at *Devcon SEA 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 costs scale exponentially.

A Foreign Function Interface for Pallene — Oct 2022
Brazilian Symposium on Programming Languages (SBLP)
Won Best Non-Student Paper Award

Education

Computer Science, M.Sc.

PUC-Rio 2019 — 2021

Advisor Professor Roberto Ierusalimschy.
Thesis A Foreign Function Interface for Pallene, thesis and paper (Best Non-Student Paper Award, SBLP).
Focus Programming Language Theory, Virtual Machines, Compiler Design. Formal specification of cross-language interfaces — reasoning precisely about system behavior under composition.

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
Ethresearch and personal blog Formal analysis of non-interactive ZK fraud proofs under adversarial conditions; drew responses from RISC Zero/Boundless and L2BEAT.

The Dave Algorithm — Triumphing over Sybils with a Laptop and a Small Collateral Feb 2025
Ethresearch and personal blog Companion post to the Dave paper; drew a detailed technical exchange with cryptographer Victor Shoup (NYU; then Offchain Labs).

Enforceable Human-Readable Transactions Feb 2025
Ethresearch and personal blog Proposed cryptographically binding human-readable descriptions to transactions, countering front-end spoofing like the $1.5B Bybit hack. Engaged Micah Zoltu and the Ethereum security community.

Fraud Proofs Are Broken, but we can fix them Apr 2024
Ethresearch and personal blog Established the safety/promptness/decentralization trilemma for permissionless fraud proofs. Drew responses from Ed Felten and OP Labs.

Scaling Content: How to truly tackle blockchain's scalability problem Jan 2022
Personal blog Argued for RISC-V execution environments to give Ethereum access to decades of existing software, anticipating the ecosystem's current renewed interest in RISC-V execution.

Talks

The Dave Algorithm Dec 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.