Anselm Krüger Staff Smart Contract Developer

Boston, MA · anselm.kruger@gmail.com · +1 617-555-0173 · linkedin.com/in/anselmkruger

PROFILE SUMMARY

- **Staff Smart Contract Developer** with **13 years** in **security engineering and smart contracts**, now on **stablecoin and cross-chain transfer contracts** at **a regulated stablecoin issuer**.
- Works in **Solidity**, **Yul** and **Rust (Anchor)** with **Foundry**, **Certora Prover**, **Halmos** and **Echidna**, across **Ethereum, Arbitrum, Base, Avalanche C-Chain and Solana**.
- Strong in **formal specs for token accounting**, **upgrade and key management design** and **incident response**, and sets the security bar the contract teams ship against.
- Works with **compliance, treasury operations and key custody teams**, **4 external audit firms** and **exchange and wallet partners** during launches and drills.
- Chairs the **smart contract security review board**, mentors **5 senior engineers**, and wrote the **pre-audit standard** used across **4 contract teams**.

TECHNICAL SKILLS

Contract Languages:	Solidity, Yul, Rust (Anchor), Python, Go
Frameworks & Libraries:	Foundry, OpenZeppelin Contracts, Solady, Anchor, viem
Security & Static Analysis:	Slither with custom detectors, Semgrep, threat modeling
Fuzzing & Formal Tools:	Certora Prover, Halmos, Kontrol, Echidna, Medusa, Foundry invariant tests
Token & Proxy Standards:	ERC-20, EIP-712, ERC-2612, EIP-3009, transparent proxies, UUPS, ERC-7201
Chains & L2 Networks:	Ethereum, Arbitrum, Base, OP Mainnet, Avalanche C-Chain, Solana
Ops, Oracles & Monitoring:	Safe multisig, HSM signing, Hypernative, OpenZeppelin Monitor, Immunefi

EDUCATION

ETH Zurich — **M.Sc. in Computer Science** — Zurich, Switzerland · Sep 2011 to Aug 2013

WORK EXPERIENCE

Circle — **Staff Smart Contract Engineer** — Boston, MA · Feb 2020 to Present

- Led formal verification for the stablecoin token contracts with **58 Certora Prover rules** on supply, blocklist and minter allowance logic, run on every pull request before audit.
- Set the pre-audit standard 4 contract teams follow (threat model, invariant list, **Slither** and Semgrep gates), cutting high and medium findings per external audit from 11 to **2**.
- Designed the upgrade process for proxied token contracts on 9 chains, with HSM-backed multisig approvals, timelocks and storage layout diffs, shipping **31 upgrades** with no failed transactions.
- Wrote the on-chain incident runbook and ran quarterly pause drills with treasury and custody teams, bringing time from alert to paused minting from 45 minutes to **8 minutes**.
- Cut gas per transfer by **18%** on a new token contract version by packing blocklist and balance data into shared slots, checked with differential fuzz tests against the old version.

Kudelski Security — **Senior Security Engineer** — Lausanne, Switzerland · Sep 2013 to Jan 2020

- Audited Solidity contracts for **21 DeFi and token clients** from 2017 on, writing a working exploit test for every high-severity finding.
- Reviewed cryptographic code for finance and telecom clients, reporting **over 40 issues** in key handling and random number generation.
- Built the team's **Echidna** fuzzing harness for client Solidity code, used on **30 later engagements**.