

Zak Blacher

Security Architect, Engineering-focused

✉ resume@chalkzebra.com

📍 San Francisco

📄 gitlab.com/zblach

🌐 linkedin.com/in/zakblacher

🐙 github.com/zblach

WORK EXPERIENCE

Security Tech Lead, C= Block, Inc (square)

12/2022 - Present

San Francisco, CA

- security leadership & engineering direction
- developed crypto & operations strategy
- established CI/CD, development best-practices
- owned corporate integration w/ security teams

Director of Security skiff.org

12/2020 - 08/2022

San Francisco, CA

end-to-end encrypted collaboration suites

- designed API strategy for cryptographic primitives
- established code review process & culture
- coordinated external pentesting / certification / roadmap
- lead engineering direction, design & threat modelling

Staff Software Eng., Security Engineering coinbase

06/2017 - 10/2020

San Francisco, CA

- cold storage tech lead (2017-2019)
- initial architect for custody and staking products
- designed & built multi-hop message integrity systems
- product lead - top-of-funnel tokenization
- code bootcamp and intern mentor
- internal security & software architecture consultant
- provided employee security onboarding & education
- embedded engineering & security consultation

Sr. Software Engineer, Security Features fitbit

10/2016 - 06/2017

San Francisco, CA

- built upgradeable user authentication systems
- developed user-privacy design features

Trust Engineer, Security Infrastructure LinkedIn

01/2015 - 10/2016

Mountain View, CA

- developer of the internal service-to-service auth systems
- partner for developer security education
- third-party software vendor assessment

Engineer, Payments Integration Rails Amazon.com

08/2013 - 10/2014

Seattle, WA

- camt053 & iso20022 banking partner integration
- SRE & devops, large-scale java engineering

July 05, 2023

SKILLS & COMPETENCIES

python

golang

software engineering

security engineering

mentorship

applied cryptography

developer education

operations analysis

software architecture

threat modelling

OPEN SOURCE CONTRIBUTIONS

argon2-jvm – API compatibility fixes & testing

openssl – x509 validation bug fixes

sudo – excision of flawed crypto library dependency

EDUCATION

Masters of Mathematics (Computer Science) University of Waterloo

09/2011 - 08/2013

Waterloo, Ontario

- Differential Privacy

- Applied Security

Magister Nätverkssäkerhet (Security) Karlstads Universitet

08/2009 - 09/2010

Karlstad, Värmland

- Filesystem Forensics

- Cryptography & Privacy

Honors Bachelor of Science (Networking & Security) University of Windsor

09/2006 - 08/2011

Windsor, Ontario

TALKS / PUBLICATIONS / PATENTS

Blockchains 101 @Blockchain McGill (11/2021)

keynote speaker - blockchain mechanisms w/ examples

"Why You Need a Physical Vault to Secure Digital Currency"

<https://www.wired.com/story/coinbase-physical-vault-to-secure-a-virtual-currency/>

"Offline Storage System and Method of Use"

USPTO: 20210019971A1 @ coinbase

"Systems and methods for re-using cold storage keys"

USPTO: 20210119781A1 @ coinbase

"Transcending Cloud Limitations by Obtaining Inner Piece"

novel limit-bypass exploits against cloud storage APIs @ DEFCON 21

"A Study of NTFS Cluster-Slack Retention Characteristics"

Masters Thesis: Filesystem forensics research for FIVES working group