Kyle Den Hartog

Email: resume@kyledenhartog.com
Cell Phone: +64 (027) 297-1753
Website: https://kyledenhartog.com
GitHub: https://github.com/kdenhartog

Professional Experience:

Senior Software Engineer **July 2019 - Present**

MATTR, Auckland, New Zealand

- Collaborated with a team of 4 to 6 to produce and review high quality code with test driven development and agile project management in Typescript while utilizing core technologies like Node.js, Express, and Postgres
- Acted as a subject matter expert and a contributor to many architectural decisions of MATTR products through architecture reviews of design specification produced by principal and senior engineers on our engineering team
- Contributed to Phase 1 development of the Department of Homeland Security Silicon Valley Innovation Program contract with a team of 4 to build web based react web applications for exchanging verifiable credentials
- Conducted public talks at industry conferences as an industry expert representing MATTR as a software engineer and standards contributor
- Tracked, triaged, and summarized important movements in over 10 draft standards in the decentralized identity ecosystem for engineering and product leaders on our team so that we could competitively assess feature priorities
- Mentored and conducted training exercises to upskill our engineering department of 15+ developers about the domain specific technologies used in the decentralized identity ecosystem. This includes summaries of JSON-LD and the semantic web, JOSE, cryptography, blockchains, smart contracts, and layer 2 scaling solutions
- Promoted good security practices within the organization acting as a subject matter expert for cryptography and cryptographic key management. This includes designing and architecting our internal key management service to securely store and use the private key used to issue millions of NZ covid passes for the NZ Ministry of Health
- Additionally authored our internal cryptography policy and reviewed additional information security framework policies based on NZISM v3.4 in order to meet SOC2 compliance requirements
- Built proof of concepts to experiment with new functionality and keep MATTR on the cutting edge of technological updates in the space including offline credential concepts used to improve privacy for millions
- Maintained the JSON-LD BBS+ Signatures open source library relied upon by over 30 different projects
- Discovered and responsibly disclosed a cryptographic twist attack in the most widely used javascript implementation of secp256k1 which has 13 million downloads weekly and was reported under CVE-2020-28498

Blockchain Software Engineer

Evernym, Draper, UT **December 2017 - February 2019**

- Collaborated with community software architects and developers to formalize multiple community technical standards one of which was a standard message encryption format derived from JSON Web Encryption
- Contributed to the development of decentralized identifier (DIDs) authentication and authorization protocols using digital signature cryptography and zero knowledge proofs throughout the decentralized identity community
- Researched several blockchain based identity projects to determine viability of interoperability with Sovrin which led to a public partnership between Ontology and Evernym
- Mentored an intern for 6 months helping him architect and develop the first Hyperledger Indy python reference agent which
- Created and maintained the Indy-Dev repository which improved the onboarding experience for developers to test the Hyperledger Indy-SDK from hours to minutes through the use of a common docker development environment
- Researched academic papers to identify cryptographic protocols that would help with the design of a p2p encryption protocol which led to the development of the DIDCommV1 protocol and Hyperledger Aries
- Represented Evernym as a contributor to the formation of the Hyperledger Aries project

Information Security Engineer

ProCircular Inc., Iowa City, IA **May 2016 - May 2017**

- Wrote scripts, automated workflows, and improved business process efficiency to decrease vulnerability assessment times by 57.4%
- Efficiently conducted vulnerability assessments, external penetration tests, web application testing assessments, and red team engagements to help the company reach profitability within 6 months
- Executed from concept to delivery a program for executive training on cybersecurity awareness in 3 months
- Delivered on time custom client reports with documented analysis of findings, vulnerabilities, exploits, gaps, risks, and recommendations that could be easily interpreted by clients with a diverse set backgrounds

Kyle Den Hartog

Email: resume@kyledenhartog.com Cell Phone: +64 (027) 297-1753
Website: https://kyledenhartog.com GitHub: https://github.com/kdenhartog

Open Source Software Contributions

Typescript

- implemented xchacha20poly1305 cipher in typescript available on github under the stablelib repository
- Contributed to JSON-LD BBS+ Signatures
- optimized the ion-sdk library maintained by Microsoft at DIF which was thread blocking in node.js while trying to generate a proof of work hash for their spam prevention mechanism

Rust

- developed in a rust library with over 300 github stars a method to easily encrypt, sign, decrypt and verify messages while retaining provenance of the message using the JWE and JWS standards (DIDCommV1)
- Assisted development of libsovtoken plugin for Indy-SDK which enabled payment functionality for use with Indy Plenum token plugin

Python

- Contributed nearly 5,000 lines of tests and refactors to the development of a token plugin for Indy Plenum
- Made a python3 client API to communicate with the DIF universal resolver to resolve DIDs from blockchains

Java

- Built a password manager using AES encryption and SHA512 hashing with open-source libraries
- Implemented a one-time-pad encryption scheme and RC4 stream cipher scheme in a graduate cryptography class

Relevant Technologies used

Node.js, Typescript, Jest, Postgres DB, Redis DB, Express, React, Lerna, Rust, Cryptography, Blockchain, Smart Contracts, Docker, AWS, HTML, Javascript, Open ID Connect (OIDC), Identity and Access Management (IAM), Web Assembly (WASM), Github Actions, CI/CD, test automation, Git, Github, REST, data structures, algorithms, full-stack Development

Standards Development

- W3C Decentralized Identifiers working group, MATTR representative and implementer
- W3C Verifiable Credentials Working Group, MATTR representative and V1.1 specification editor
- IETF draft-denhartog-pairing-curves-jose-cose-00, author
- IETF draft-looker-jwm-01, reviewer
- Various additional W3C CCG work items
- Decentralized Identity Foundation Sidetree WG, MATTR representative and contributor
- Open ID Connect SIOP V2, early contributor (while at DIF)

Group Affiliations:

W3C Verifiable Credentials working group, Editor (v1.1)	May 2021 - Present
Decentralized Identity Foundation, Technical Steering Committee	June 2021 - Present
Decentralized Identity Foundation, DID-Auth WG Chair	November 2017 - Present
Hyperledger Global Forum, Indy Agent Speaker	December 2018
Hyperledger, Technical Ambassador	June 2018 - March 2020

Education:

University of Iowa, Iowa City, IA May 2017
Bachelor of Arts in Computer Science