

# Praveensankar Manimaran

## PhD Research Fellow

✉ praveema@ifi.uio.no ☎ +919500552237 🔗 <https://praveen.xyz/>

🐙 [github.com/praveensankar/](https://github.com/praveensankar/) 🌐 [linkedin.com/in/praveen000/](https://www.linkedin.com/in/praveen000/)

### Bio

Praveensankar Manimaran is a PhD Research Fellow at the University of Oslo, Norway, working on Verifiable Credentials and Zero-Knowledge Proofs. Praveen has expertise in developing new research directions, designing, developing, and implementing solutions for complex research problems.

### Education

<b>Ph.D. - Informatics</b> , <i>University of Oslo</i>	2020 Oct – Present
<b>M.Tech. - Computer Science and Engineering</b> , <i>National Institute of Technology Puducherry</i> • CGPA: 9.82, <b>Gold Medalist</b>	2018 Jul – 2020 Jun
<b>B.E. - Computer Science and Engineering</b> , <i>PSG College of Technology</i>	2012 Jul – 2016 May

### Professional Experience

<b>PhD Research Fellow</b> , <i>University of Oslo, Norway</i> • Research in <b>Verifiable Credentials, Zero-Knowledge Proofs, Blockchain Technologies</b> • Worked as a teaching assistant for the following courses: IN5020 - Distributed Systems (2022, 2023), IN5420 - Distributed Blockchain Technologies (2022, 2023). • Installed and maintained Norway's EBSI pilot node (2022-2023). • <b>Advisors:</b> Roman Vitenberg, Leander Jehl • <b>Collaborators:</b> Thiago Garrett, Mayank Raikwar, Arlindo F. Conceição	2020 Oct – 2024 Oct
<b>Software Engineer</b> , <i>Accolite Software India Pvt Ltd</i> ✉ • Worked on web development and used technologies associated with the .NET framework.	2016 Jul – 2017 Mar

### Publications

<b>zkToken: Empowering Holders to Limit Revocation Checks for Verifiable Credentials</b> , ( <a href="https://arxiv.org/html/2509.11934v1">https://arxiv.org/html/2509.11934v1</a> ) • Formalizes the privacy issuer of traceability of revocation status in the verifiable credentials system. • Proposes <i>zkToken</i> , a revocation protocol that uses a custom-built Zero-Knowledge Proof circuit to address the privacy issue. • <i>zkToken</i> outperforms existing protocols in terms of required bandwidth for issuers and holders.	
---	--

## Decentralization Trends in Identity Management: From Federated to Self-Sovereign Identity Management Systems, (Computer Science Review, Volume 58, 2025)

- Reviews Federated and Self-Sovereign Identity systems from a conceptual point of view.
- Proposes a generic framework for Identity systems and analyzes the architectures and workings of (a) IOTA Id, (b) Indy, and (c) eIDAS v1.0.
- Highlights differences in decentralization and privacy strategies across these systems.

## Prevoke: Privacy-Preserving Configurable Method for Revoking Verifiable Credentials, 2024 IEEE International Conference on Blockchain (Blockchain)

- *Prevoke* presents key privacy challenges in the revocation protocol and proposes a novel solution that utilizes Merkle Tree Accumulators, BBS Signatures, Bloom Filters and Smart Contract.
- *Prevoke* also proposes a two-phase verification protocol that optimizes the performance of verification. Most of the valid credentials go through fast verification. Only revoked and a handful of valid credentials would go through slow verification.

## Research Adoption

### EBIP: Secure Privacy-Preserving Revocation of Verifiable Credentials, [<https://hub.ebsi.eu/ebips>]

- Discloses a security vulnerability in EBSI's Dynamic Status List, a revocation protocol for verifiable credentials that addresses the privacy issue of holder's traceability.
- Adopts **zkToken**, a ZKP-based revocation protocol developed during my PhD.

## Projects


### zkToken, Implementation

2024 Aug – 2025 May

- Implemented *zkToken* and integrated *zkToken* into an in-built VC ecosystem.
- Built a custom ZKP circuit based on Groth16 ZKP scheme using the gnark library.
- Benchmarked the performance of *zkToken* and an existing protocol to perform the comparison.
- **Languages:** Golang, Solidity
- The GitHub repository will be shared upon request, as the research paper is not yet published.

### Prevoke, Implementation

2023 Aug – 2024 Jul

- Implemented *Prevoke* and integrated *Prevoke* into an in-built VC ecosystem.
- **Workflows:** 1) issuance, 2) revocation, 3) VP construction and sharing, and 4) VP verification.
- In addition, deployed a Smart Contract on a Private Blockchain using Ganache, hosted in NREC.
- The entities are hosted as servers and geographically distributed via NREC.
- **Results:** Analyzed the performance, latency, and cost of *Prevoke* for different workloads.
- **Languages:** Golang, Solidity, Python
- **Github repo:** <https://github.com/praveensankar/Prevoke> .