Praveensankar Manimaran

PhD Research Fellow

praveema@ifi.uio.no

+4796741397

Oslo, Norway

https://praveen.xyz/

github.com/praveensankar/

linkedin.com/in/praveen000/

Bio

Praveensankar Manimaran is a PhD Research Fellow at the University of Oslo, Norway working on Verifiable Credentials (VCs) and Blockchain Technologies. Praveen's research focuses on privacy issues in the revocation and verification of VCs. Praveen has expertise in Smart Contracts, Zero-Knowledge Proofs, BBS Signatures, Bloom Filters, and Merkle Tree Accumulators.

Education

Ph.D. - Informatics, *University of Oslo* 2020 Oct – 2024 Oct
Oslo, Norway

- Research in **Verifiable Credentials** and **Blockchain Technologies**
- Identified important privacy problems in VCs's revocation and verification, developed novel solutions using latest techniques such as Merkle Tree Accumulators and BBS Signatures, implemented prototypes to showcase the feasibility and published the research findings.
- 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
- Supervisors: Roman Vitenberg, Leander Jehl
- Collaborators: Thiago Garrett, Mayank Raikwar, Arlindo F. Conceição

M.Tech. - Computer Science and Engineering, 2018 Jul – 2020 Jun
National Institute of Technology Puducherry Karaikal, India

- CGPA: 9.82, **Gold Medalist**

B.E. - Computer Science and Engineering, *PSG College of Technology* 2012 Jul – 2016 May

Publications

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

- Prevoke presents privacy issues in revoking VCs and presents a solution based on Bloom Filters, Merkle Tree Accumulators, and Smart Contracts.
- Prevoke also proposes a novel two-phase verification technique to optimize the efficiency of VCs' verification. Most of the valid VCs would go through efficient and fast verification. Only revoked VCs and a handful of valid VCs would go through expensive verification.

Understanding Decentralized Identity: From Federated to Self-Sovereign Identity Management Systems, *ACM Computing Surveys (Under Review)* 2024

- Provides a generic model to analyse the architecture of IMSs
- Using the generic model, analyze a) IOTA Id, b) Indy, and c) eIDAS.
- Discusses the differences between these IMSs using a novel taxonomy

Addressing traceability of revocation status of Verifiable Credentials,
(Work in Progress)

- Utilises Zero-Knowlege Proofs to address traceability problem

Projects

Prevoke, *Proof of Concept implementation*

- **Components**: 1) Issuer, 2) Holder, 3) Verifier, 4) Smart Contract, 5) Golang and Smart Contract interactions, and 6) mock VC data model based on W3C Specifications.
- **Workflows:** 1) issuance, 2) revocation, 3) VP construction and sharing, and 4) VP verification
- **Languages:** Golang, Solidity

Professional Experience

Software Engineer, *Accolite Software India Pvt Ltd* 2016 Jul – 2017 Mar

- Worked on web development using technologies associated with .NET frameworks and angularjs.

Skills

Verifiable Credentials	●●●●●	Blockchain	●●●●●
Research	●●●●●	Golang	●●●●○
Privacy	●●●●○		

References

Dr. Roman Vitenberg, *Professor*, University of Oslo, Norway
romanvi@ifi.uio.no

Dr. Leander Nikolaus Jehl, *Associate Professor*, University of Stavanger, Norway
leander.jehl@uis.no

Dr. Thiago Garrett, *Postdoctoral Fellow*, University of Oslo, Norway
thiagoga@ifi.uio.no

Dr. Mayank Raikwar, *Postdoctoral Fellow*, University of Oslo, Norway
mayankr@ifi.uio.no