

Mahdi Nejadgholi

+1(438)XXX-XXXX | xoredtwice@pm.me | xored.io | xoredtwice | xoredtwice

Skills

Web3 Full Stack Development, Smart Contract Code Audit, Decentralized Governance Models

Information Security E-Voting protocols, zk-SNARKs, Sigma-protocols, Multi-party Computation.

Software Development Python, Solidity, Brownie, Truffle, ZoKrates, Django, J2EE, LAMP, NoSql, Bash.

Applied Machine Learning Deep Learning Software Testing, Generative Models, Convolutional Neural Networks.

Experiences

Concordia University

RESEARCH ASSISTANT, WEB3 CODE AUDITOR, PART-TIME

- Audited various Web3 ERC20 tokens code to find financial misstatement risks.
- Conducted an analysis of smart contract code for implementation efficiency.
- Developed a semantic search engine tailored for public Web3 smart contracts.

Montreal, Canada

Nov 2022 - Present

AgoraVote

FULL-STACK DEVELOPER

- Full stack development of e-voting software using ElectionGuard.
- Conducted market analysis of active electronic voting and Web3 governance projects.

Montreal, Canada

Aug 2022 - present

CH3SS

FULL-STACK WEB3 DEVELOPER

- Designed and developed an efficient Chess logic for Ethereum Virtual Machine.
- Full stack development of a Proof-of-Concept fully on-chain chess gameplay.

Montreal, Canada

Nov 2021 - Present

VoteXX

DEVELOPER & RESEARCH ASSISTANT

- Designed and implemented Nullification protocol.
- Implemented VoteXX E-voting Crypto library.
- Developed a Systemization of Knowledge over E-voting academic literature using Topic Modeling and NLP techniques

XXNetwork

Mar 2020 - Nov 2022

HyperBlueCube Start-up

Co-FOUNDER AND R&D DIRECTOR

- Design and implementation of Customized BMS Devices.
- Conducted an extensive research over active attack vectors of IoT Wireless protocols.

Tehran, Iran

Oct 2014 - Mar 2018

Publications & Talks

VoteXX: A Solution to Improper Influence in Voter-Verifiable Elections

CRYPTOLOGY EPRINT ARCHIVE

WWW

2022

Introduction to Cryptocurrency

PRESENTED AT WEST VANCOUVER MEMORIAL LIBRARY

Vancouver, Canada

2021

Short Paper: Ballot secrecy for liquid democracy

6TH WORKSHOP ON ADVANCES IN SECURE ELECTRONIC VOTING

Grenada, US

2021

A Study of Oracle Approximations in Testing Deep Learning Libraries

34TH IEEE/ACM INTERNATIONAL CONFERENCE ON AUTOMATED SOFTWARE ENGINEERING (ASE)

San Diego, US

2019

Education

Concordia University

Montreal, Canada

MASTER OF APPLIED SCIENCE – INFORMATION SECURITY

2018 - 2022

- Research Topics
 - Coercion-resistant **E-Voting Protocols**.
 - Ballot Privacy in **Liquid Democracy**.
 - **Deep Learning** Frameworks' **Test Suite Analysis**.
- Courses
 - Foundations of Cryptography (Also T.A.)
 - Protocols and Network Security (Also T.A.)
 - Natural Language Analysis
 - Advanced Software Engineering Topics
 - Operating System Security
 - Software Measurement (Only T.A.)

Shahid Rajaei Teacher Training University (SRTTU)

Tehran, Iran

MASER OF SCIENCE – COMPUTER SCIENCE AND ENGINEERING

2013 - 2016

- Research Topics
 - **Classification** based on Virtual Force Field Simulation.
 - Deep Model **Transfer Learning** for Face Recognition.
- Courses
 - Machine Learning
 - Neural Networks
 - Meta-heuristic algorithms
 - Computational Geometry

Amirkabir University of Technology (AUT)

Tehran, Iran

BACHELOR OF SCIENCE – COMPUTER HARDWARE ENGINEERING

2007 - 2012

Coursera.org

World-Wide Web

COURSE CERTIFICATES

2016 - Present

- **Smart Contracts** – Digital Certificate: LGLQKZA5U6K7
provided by University at Buffalo
- **Blockchain Basics** – Digital Certificate: XVR9XUETH55H
provided by University at Buffalo
- **Machine Learning** – Digital Certificate: UHAPK2K78WQU
provided by Stanford University

Honors & Awards

- 2022 **Programme Accélération grant**, Centech Montreal, Canada
- 2021 **Cyber Security Summer School, “Online Voting” Certificate**, University of Tartu Tartu, Estonia
- 2019 **Harriet and Abe Gold Award**, Concordia University Montreal, Canada
- 2010 **1st Prize Winner**, @Home Robocup League, AUTCup Tehran, Iran
- 2009 **Member of Technical Committee**, 2nd Linux Festival, Amirkabir University Tehran, Iran
- 2008 **Undergraduate Grant**, Amirkabir University, Awarded to 1st ranked on 8th Khwarizmi Youth Festival. Tehran, Iran
- 2007 **1st Prize Winner**, 8th Khwarizmi Youth Festival, a competition for Iranian teenagers with innovative ideas. Designed and implemented a frame to convert non-touchscreen to touchscreen displays, Iran Patent ID : 82/A/009058 Tehran, Iran