Mahdi **Nejadgholi**

+1(438)***-**** | mahdi@xored.io | xored.io | xoredtwice | xoredtwice

Skills

Applied Cryptography	Post-Quantum Cryptography • SNARKs • MPC Protocols • E-voting protocols • Symbolic proofs
Decentralized Web	DeFi protocol design • Smart-contract audit • Governance models • Full-stack development
Applied Machine Learning	Deep Learning software testing • Prompt engineering • NLP pipeline design
Development Stack	Bash • Python • Rust • Solidity • Java • Mathematica • JS • Circom • GNARK

Experiences

Xored Innovations — *Montreal, Canada*

Sole Proprietorship - Applied Cryptography services — *January 2024 - Present*

- Conducted security audits on multiple Web3 smart contracts to detect cryptographic weaknesses.
- Served as a contractor for multiple companies, delivering applied cryptographic design and implementation services.

Parity Financials Inc. — *UK (Remote)*

Blockchain Researcher — *Jan 2024 - Nov 2025*

- Delivered customized proof-of-concept implementations based on recent DeFi research papers, including ZkLedger (2019), Aiges (2023), and Cicada (2024).
- Designed financial mechanisms such as Delivery-versus-Payment (DvP) and on-chain auction systems, for auditable, privacy-preserving banking.
- Conducted pre-production smart contract audits to ensure security and compliance.
- Performed in-depth research on state-of-the-art DeFi protocols and products.
- Gained hands-on experience with post-quantum cryptography and zero-knowledge protocols.

Concordia University — *Montreal, Canada*

Research Assistant, Web3 Code Auditor — *Nov 2022 - Nov 2023*

- Audited various Web3 ERC20 tokens code to find financial misstatement risks.
- Conducted an analysis of smart contract code for implementation efficiency.

AgoraVote — *Montreal, Canada*

Full-stack Developer — *Aug 2022 - Dec 2023*

- Full stack development of e-voting software using ElectionGuard.
- Conducted market analysis of active electronic voting and Web3 governance projects.
- Held a 1500-voter voting event for CSN-FSSS, SPBTPA (category 3).

Education

Concordia University — *Montreal, Canada*

Master of Applied Science – Information Systems Engineering – GPA: 3.94 — *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.)** | Software Measurement **(Only T.A.)**
  Operating System Security | Natural Language Analysis | Advanced Software Engineering Topics

Shahid Rajaee Teacher Training University — *Tehran, Iran*

Maser of Science – Computer Science and Engineering – GPA: 3.1 — *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 — *Tehran, Iran*

Bachelor of Science – Computer Hardware Engineering — *2007 - 2012*

Publications & Talks

Rayls II: Fast, Private, and Compliant CBDCs — *Rome, Italy*
Financial Cryptography — *2025*

Revisiting Silent Coercion — *Nancy, France*
E-Vote-ID — *2025*

VoteXX: A Solution to Improper Influence in Voter-Verifiable Elections — *Virtual*
E-Vote-ID — *2022*

Ballot secrecy for liquid democracy — *Grenada, US*
6th Workshop on Advances in Secure Electronic Voting - **First Author** — *2021*

A Study of Oracle Approximations in Testing Deep Learning Libraries — *San Diego, US*
34th IEEE/ACM International Conference on Automated Software Engineering (ASE) - **First Author** — *2019*

Introduction to Cryptocurrency — *Vancouver, Canada*
Presented at West Vancouver Memorial Library - **Sole Speaker** — *2021*

Honors & Awards

2025 **Concordia University Graduate Doctoral Fellowship**, Concordia University — *Montreal, Canada*
2025 **Concordia International Tuition Award of Excellence**, Concordia University — *Montreal, Canada*
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*

Extra

Simply a Node — *YouTube*
Full-stack creator — *Sep 2025 - Present*

- Explaining the core ideas behind cryptography through clear visualizations and engaging narration.
- Bridging the gap between natural language and formal mathematical notation.

CH3SS — *Montreal, Canada*
Full-stack developer — *Nov 2022 - Present*

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