

Tejaswa Rastogi

Blockchain Security Engineer

✉ razzor@ciphershastra.com

 linkedin.com/in/razzor

Dedicated and passionate Blockchain Security Engineer with a strong commitment to safeguarding digital assets and systems. Adept at identifying vulnerabilities and crafting robust security solutions. Loves creating CTF challenges to sharpen skills and foster a culture of cybersecurity awareness. Enthusiastic about the intricacies of cryptography and its application in blockchain security. Committed to advancing the field through continuous learning and innovative problem-solving.

Experience

Blockchain Security Engineer | ADI Foundation

June 2026 - Present

- Conduct in-house code reviews across multiple codebases to find and remediate vulnerabilities
- Lead blockchain security audits and guide secure development practices for dApps and smart contracts
- Define application security policies, procedures, and engineering guidelines for the organisation
- Own incident response and security triage for blockchain-related events

Lead Security Engineer (Blockchain) | Reckong Tech

Sep 2025 - May 2026

- Conduct end-to-end security reviews for smart contracts and ZK circuits while establishing company-wide security policies.
- Develop custom tools and internal security libraries to harden the development lifecycle and mitigate vulnerabilities.
- Manage high-stakes external audits with top-tier firms, overseeing technical remediation and serving as the primary security liaison.
- Engineer competitive security solutions and present novel research at global conferences

Security Engineer | Matter Labs/zkSync

March 2024 - August 2025

- Perform Security Reviews on existing and new smart contracts and circuits.
- Research and Engineer competitive solutions/tools to improve the security landscape with testing and formal verification.
- Lead external audits and communications
- Share any new research at security conferences

Security Auditor | ConsenSys Diligence

June 2022 - Feb 2024

- Perform Security Audits on Complex Protocols.
- Help the auditee team to adopt a better and more secure system design.
- Research and Contribute to the in-house security tools.
- Research new attack vectors, and share the knowledge with fellow auditors in the team.
- Speak at leading security conferences sharing any new research or building relations with new protocols.

Blockchain Smart Contract Auditor | QuillAudits

May 2021 - June 2022

- Conduct Smart Contract Audits: Manual Review, Functional/Automated/Fuzz Testing
- Client Interactions: Providing suggestions to resolve the issues reported during an audit
- Interviews: Take interviews for new joiners in order to bring new talent in.

Infosec Instructor | TSPL's Explorium

Jul 2018 - May 2019

- Prepare and Deliver lectures to students on topics such as programming, networking, cyber-security, and software design.
- Plan, Evaluate, Revise curricula, course content, course materials, and method of instruction
- Collaborate with colleagues to address teaching and research issues.
- Maintain computer equipment used in instruction

Education

Bachelors in Computer Science | Mithibai College - Mumbai University

2014 - 2017

- CGPA: 6.7/7.0

Certifications

- | | |
|--|---------------|
| • Certified Ethical Hacker EC-Council | October 2020 |
| • Blockchain Security Infosec | August 2020 |
| • Autopsy Digital Forensics Basis Technology | June 2020 |
| • CCNA CyberOps CISCO | March 2018 |
| • Python3 Sololearn | August 2017 |
| • Network Devices Cybrary | August 2017 |
| • Cross-Site Scripting Cybrary | August 2017 |
| • MTA: Security Fundamentals Microsoft | November 2016 |

Entrepreneur Journey

- | | |
|---|------|
| ● Created CipherShastra | 2021 |
| • An open source platform to help everyone learn Smart Contract Security by solving CTF like challenges | |
| ● Founded Unchained | 2021 |
| • An international conference aiming to promote Blockchain Security | |
| ● Founded RazzorSec | 2019 |
| • A community aiming to bring more and more enthusiasts into the evolving world of Blockchain Security | |

Professional Talks

- **ZK Verifiers Exposed: Lessons from Real Bugs and Fixes** | ETHTaipei 2025
- **Quantum Robust Ethereum: What's Next?** | Web3Conf Goa 2024
- **Phishing Smart Contracts for Fun & Profit** | c0c0n 16
- **Not So Famous Attack Vectors in the World of Smart Contract Security** | ETHDubai, Nullc0n Berlin
- **Detecting Price Manipulation Attacks** | SANS Blockchain Security Summit 2022
- **Preventing Sandwich Attacks with Recurrent and Recursive Zero Knowledge Proofs** | DEFCON 29
- **Post Quantum Cryptography & 5G Security** | Nullc0n 2021
- **Verifiable Delay Functions for Preventing DoS/DDoS Attacks on Ethereum2.0** | DEFCON 28
- **Modifying Jigsaw to Evade ML Malware Classifiers** | Red Team Security Summit 2020

Some Public Reports

- [Linea Plonk Verifier](#)
- [Linea Message Service & ZK Rollup | Canonical Token Bridge](#)
- [Forta Delegated Staking](#)
- [Gearbox Finance V2](#)
- [YoloRekt](#)
- [Nord Advisory, Nord Finance, Nord Loan](#)
- [Pi Protocol](#)

Currently Learning

- [Rust | Intermediate](#)
- [Applied Cryptography | Beginner](#)