Sanket Kanjalkar

☎ 217-721-7898 | ✉ sanket1729@gmail.com | github.com/sanket1729 | linkedin.com/in/sanket1729 | Seattle, WA

Personal Profile

Rust software engineer with 5+ years of industry experience in security and cryptography, backed by a strong academic publication record. Proficient in rust, applied cryptography, zero-knowledge proofs, bitcoin, distributed systems, peer-to-peer systems, blockchain, and smart contract scripting, prioritizing practical applications and dev-tooling.

Skills Rust, C++, C, bitcoin, python, sage, applied cryptography, ZKPs, distributed systems, Hadoop, RabbitMQ, Spring, Java, SQL.

Work Experience

Cryptographic Engineer | Blockstream Research

Seattle, WA | 2020 - ongoing | 3 years

Scripting team lead:

- **Miniscript:** Ideated, designed and implemented a language for bitcoin script from scratch. With a concise and intuitive syntax-*Miniscript* simplifies script development, wallet fee estimation, and enhances security and has seen **complete ecosystem wide adoption**.
  - Adopted by bitcoin core project used by more than **95%** of all bitcoin network participants.
  - Collaborated with industry-leading wallet providers, including Ledger, Coldcard, and Jade, to seamlessly integrate Miniscript into their platforms, expanding its reach and accessibility to over **4 million users**.
  - Created a compiler software that surpasses expert hand-optimized scripts in terms of fee incurred. This eliminated the need of hiring experts and reduced development time **from days to <1ms** resulting in significant cost savings for users.
- **Bitcoin script extensions:** Increasing the expressiveness of bitcoin script.
  - Spearheaded research and design of a **formally provable** smart contract language called *Simplicity*, eliminating hacks prevalent in crypto-currency ecosystem.
  - Improved developer rust tooling that shortened the implementation time by **25x**. This tooling enabled previously thought impossible use-cases like complex financial smart contracts such as options and limit orders.
  - Co-authored **15+** tutorials, papers, and engineering blog posts explaining the new work of Blockstream research.

Open source rust projects:

- Maintainer of multiple popular open-source Rust crates like rust-bitcoin, rust-miniscript, and rust-secp256k1, with a cumulative download count exceeding **10 million** on crates.io.
- Mentored 6+ bitcoin summer of code projects over the course of three summers.

Zero knowledge proof(ZKP) projects:

- Developed Bulletproof++, a novel zero knowledge(ZK) proof system saving over 60% transaction fees. Implemented C89 complaint constant-time code that offers **400%** increase in prover/verifier performance.
- Improved auditable Multi-Party Computation (MPC) by incorporating Zero-Knowledge Proofs (ZKPs), resulting in a threefold enhancement over existing approaches. Published findings at ***IEEE Europe S&P 2021*** workshop.

Distributed Systems Projects:

- Orchestrated the successful deployment and implementation of taproot network upgrade on a robust liquid peer-to-peer network comprising hundreds of nodes and assets valued over $100 million.
- Uncovered privacy flaws in Lightning Network's distributed system implementation, revealing balance information. Published at ***Financial Crypto 2021***.

Invited Talks:

- Featured speaker at prominent technical conferences, including The Bitcoin Conf, IC3, Advancing bitcoin, MIT Bitcoin Conf, delivering talks and leading developer workshops.

Software Engineer | Samsung Electronics

Seoul, Korea, 2016-2018 | 2 years

- Spearheaded the end-to-end design and development of a Threat Intelligence System for Samsung Smart TVs, encompassing over **10,000** devices globally, enabling quick response to new and unknown threats.
- Single-handedly designed, implemented, and managed a distributed system that processed 100k weekly security reports, utilizing RabbitMQ, the Spring framework, and PostgreSQL/Hibernate.
- Automated nearly instant threat detection saving response time from over multiple days to a few minutes.

Education

University of Illinois, Urbana-Champaign

Champaign, IL

MS in Computer Science | GPA 4.0/4.0 | **A+** in all courses *Aug 2018 - May 2020*

- Published masters thesis in applied cryptography on Multi-party computation(MPC) and zero-knowledge proofs.
- Received a bug bounty of **15,000 USD** for responsible disclosure of bugs to more than 26 open-source cryptocurrency projects affecting over 2 billion dollars marketcap. Bug report covered in prominent media and translated into several languages.
- Key courses: consensus systems(A+), applied cryptography(A+), network security(A+), Machine learning(A+), Formal methods(A+).

IIT Bombay

Mumbai, MH, India

Btech in Computer Science | GPA 8.99/10.0 *Aug 2012 - May 2016*

- IIT Joint Entrance Exam 2012: Ranked **29** out of 1.3 million candidates.
- Winner of coding, logic, and chess general championships. Recipient of Hostel Color award.