# Sanket Kanjalkar


CONTACT INFORMATION

Second Year Student, Master of Science(Expected Graduation: May-2020) sanket1729@gmail.com
Department of Computer Science +1-217-721-7898; sanket1729.github.io
University of Illinois at Urbana-Champaign https://www.linkedin.com/in/sanket1729


INTERESTS

Bitcoin and **Blockchains**, Applied Cryptography, Computer Security, Machine Learning

EDUCATION

**University of Illinois at Urbana-Champaign** 4.0/4.0
Master of Science, Computer Science, 2018-2020 **A+** in **all** courses
**Indian Institute of Technology (IIT), Bombay, India** 8.99/10
B.Tech with Honors, Computer Science and Engineering, 2012-16

PUBLICATION

I can't believe it's not Stake: Resource exhaustion attacks on Proof of Stake currencies;
*S. Kanjalkar*, Y.Li, J.Kuo, A. Miller; (**Financial Crypto'19, St.kitts**) pdf

RELEVANT WORK EXPERIENCE

**Blockstream Reseach** | Research Intern *May'19 - Aug'19*

- Research and development of Minisript, a new language for writing bitcoin scripts allowing automated static analysis
- Implemented an open source library written in **rust** which allows smooth interoperation between wallets from different vendors

**University of Illinois at Urbana-Champaign** | Graduate Research Assistant *Aug'18 - Present*

- Lead a project to responsibly disclose resource exhuastion vulnerabilities affecting 26+ currencies having a total of 2.6 B USD market cap. *Aug'18-Jan'19*
- Evaluating the security and privacy of lightning network, an off-chain Layer-2 scaling solution for bitcoin against denial of service and payment inference attacks *Dec'19 - Present*
- Teaching assistant for Applied Cryptography (*Fall '19*) and Intro to CS (*Fall' 18*)

**SAMSUNG KOREA** | Software Eng, Seoul HQ, Korea, DTV Security *Aug'16 - June'18*

- **Software development:** Designed a distributed system from scratch via **Enterprise Architect** and implementated it across multiple machines with rpc support via **rabbitMQ**, **Spring** framework for webservers, **postgreSQL/hibernate** for database with **CI/TDD**.
- **Data Analytics:** Automated Weekly Security Status report generation based on analytics on TV security reports from tens of thousands of Smart TVs worldwide.
- **Devops/Reliability:** Ensured smooth deployment, maintainance and high availability of 15 systems in production.

**SAMSUNG KOREA** | Research Intern, Visual Display *May - Jul '15*

- Performed qualitative research on methods to determine a trust metric using Machine Learning for an IoT(Internet of Things) device in an IoT ecosystem. Recieved Pre-placement Offer.

SELECTED PROJECTS

**Undergraduate Dissertation** | IIT Bombay, July'15-Mayc'16
Static Analysis of programs for checking malicious behavior using clustering techniques on control flow graphs of programs.

**SVM in Zero Knowledge** | UIUC, Aug-Dec'18
Designed and implemented a Zero knowledge application where any prover can convince the verifier that the SVM classifier accuracy without revealing any **secret** weights used in the classifier.

**Vandalism detection using car OBD port** | Carsense Technologies, Jun-Aug'16
Implemented logic for detecting vandalism, towing and gps location tracking on STM32 IC in ***low level C*** for an embedded device connected to OBD port of the car.

TECHNICAL SKILLS

**Programming**: **Rust**, C, C++, Java EE, Python, Shell, Matlab, SQL
**Frameworks/Tools**: Spring, Enterprise Architect, Hibernate, PyTorch, RabbitMQ

RELEVANT COURSES

(Grad)Applied Cryptography(**A+**), Computer Security(**A+**), ML(**A+**), Formal methods(**A+**)
(Undergrad) Data Structures/Algo, Graph Theory, Linear Optimization, AI, Reinforcement learning

ACHIEVEMENTS

- Awarded **15,000$** by the QTUM foundation for responsible disclosure of security vulnerability.
- Recieved full scholarship **(4000$)** to attend the workshop of **Programming Blockchain**
- Co-organizer of Seoul Bitcoin Meetup with over 2200 members. Conducted tens of technical presentations on bitcoin and 1 hands on developer workshop about Bitcoin Scripts *2016-2018*
- Secured All India Rank 29 in IIT-JEE *2012*