

Luu The Loi (Loi Luu)

CONTACT INFORMATION	System Security Lab Com 2, Base 1-02, School of Computing National University of Singapore	Phone: (+65) 93443602 Web: http://www.comp.nus.edu.sg/~loiluu E-mail: loiluu@comp.nus.edu.sg
RESEARCH INTERESTS	My research interests are cryptocurrency and consensus protocols, but I am also broadly interested in research problems in Security and Distributed System. Currently I am focusing on designing secure and scalable cryptocurrencies and consensus protocols in distributed systems.	
EDUCATION	<ul style="list-style-type: none">• National University of Singapore, Singapore Ph.D., Computer Science, Fall 2014 - Present<ul style="list-style-type: none">• Advisor: Dr. Prateek Saxena• Univ. of Engineering and Technology, Vietnam National Univ., Hanoi, Vietnam B.S., Computer Science, Fall 2009-June 2013<ul style="list-style-type: none">• GPA: 3.62/4.0, Honor Programme, Highest Distinction• Thesis: “Implement Breath First Search and Experiment with Search Algorithms on KLEE”• Thesis advisors: Dr. Hoang T. Anh	
PEER-REVIEWED PUBLICATION	<ol style="list-style-type: none">1. Loi Luu, Viswesh Narayanan, Chaodong Zheng, Kunal Baweja, Seth Gilbert, Prateek Saxena. A Secure Sharding Protocol For Blockchains. <i>The 23rd ACM Conference on Computer and Communications Security (CCS’16)</i> (Acceptance rate 16.5%).<ul style="list-style-type: none">• Commercialized and Deployed at an (undisclosed) financial institution in Aug 20162. Loi Luu, Duc-Hiep Chu, Hrishi Olickel, Prateek Saxena, Aquinas Hobor. Making Smart Contracts Smarter. <i>The 23rd ACM Conference on Computer and Communications Security (CCS’16)</i> (Acceptance rate 16.5%).<ul style="list-style-type: none">• The paper is well recieved by the community. See this Reddit post.• On the news: CoinDesk.3. Loi Luu, Jason Teutsch, Raghav Kulkarni and Prateek Saxena. Demystifying incentives in the consensus computer. <i>The 22nd ACM Conference on Computer and Communications Security (CCS’15)</i> (Acceptance rate 19.4%).<ul style="list-style-type: none">• The paper has influenced the future design of Ethereum cryptocurrency. See this blog post.• Great discussion about the paper on Reddit.4. Loi Luu, Ratul Saha, Inian Parameshwaran, Prateek Saxena and Aquinas Hobor. On Power Splitting Games in Distributed Computation: The Case of Bitcoin Pooled Mining, <i>The 28th IEEE Computer Security Foundations Symposium (CSF’15)</i> (Acceptance rate 34.3%).5. Loi Luu, Shweta Shinde, Prateek Saxena and Brian Demsky. A Model Counter for Constraints Over Unbounded Strings, <i>The 35th annual ACM SIGPLAN conference on Programming Language Design and Implementation (PLDI’14)</i> (Acceptance rate 18.1%).6. Loi Luu, . Smart Contracts Make Bitcoin Mining Pools Vulnerable. To appear at the <i>4th Workshop on Bitcoin and Blockchain Research (BITCOIN’17)</i>.	

PREPRINTS &
PAPER UNDER
SUBMISSION

1. [Loi Luu](#), Yaron Velner, Jason Teutsch, Prateek Saxena . SMARTPOOL: Practical Decentralized Pooled Mining. Cryptology ePrint Archive, Report 2017/019. January 2017.
 - Launched as a community [project](#).
2. [Loi Luu](#), Viswesh Narayanan, Kunal Baweja, Chaodong Zheng, Seth Gilbert, Prateek Saxena. SCP: A Computationally-Scalable Byzantine Consensus Protocol For Blockchains. Cryptology ePrint Archive, Report 2015/1168. November 2015.

POSTER

1. Hoon Wei Lim, [Loi Luu](#), Shruti Tople and Prateek Saxena, WeShare: A Coercion-Resistant and Scalable Storage Cloud, *36th IEEE Symposium on Security and Privacy*.

TALKS

1. SmartPool: Decentralized Mining Pools Using Smart Contracts, [European Ethereum Development Conference](#), Paris, February 2017.
2. Ethereum and Smart Contracts, [Winter School on Cryptocurrency and Blockchain Technologies](#), Shanghai, January 2017.
3. Making Smart Contracts Smarter, [Ethereum Devcon2](#), Shanghai, September 2016.
4. SCP: A Computationally-Scalable Byzantine Consensus Protocol, [ScalingBitcoin, Hong Kong](#), December 2015.
5. On the incentive compatibility of Bitcoin & Cryptocurrency, [ADSC Singapore](#), 30 July 2015.
6. Dropping your cake and eating it too: Profiting in Bitcoin pools by withholding blocks, [Tetcon, Ho Chi Minh city](#), January 2015.

PROFESSIONAL
EXPERIENCE

1. Cofounder, SmartPool project Jan 2017 - Present
SmartPool.io
2. Scientific advisor for several financial institutions April 2016 - November 2016
Anquan Capital
3. Research Assistant Jul 2013 - Aug 2014
National University of Singapore
4. Co-founder and software developer Nov 2011 - Jan 2013
truongnha.com, an open-source school management system for high schools in Vietnam

SELECTED
HONORS
AND AWARDS

- **Microsoft Research Asia Graduate Fellowship** 2016
- **President Graduate Fellowship** 2014-Present
National University of Singapore.
- **Distinguished Academic Achievement Award** 2013
Vietnam National University (Awarded to the best students from the college).
- **Best Thesis Award** 2013
Vietnam National University, (Awarded to the best 5 student theses from the college).
- **GE Foundation Scholar Leadership** 2010
(Awarded by General Electric Foundation to the best 10 students in Vietnam).
- **Third Prize ACM-ICPC Asian Regional Contest, Vietnam** 2010
- **Third Prize National Olympiad in Informatics for Students, Vietnam** 2008

REFERENCES

Dr. Prateek Saxena (advisor)
Assistant Professor
School of Computing
National University of Singapore
Email: prateeks@comp.nus.edu.sg

Dr. Aquinas Hobor (collaborator)
Assistant Professor
NUS School of Computing & Yale-NUS College
National University of Singapore
Email: hobor@comp.nus.edu.sg