

# Fan Long

University of Toronto, Computer Science Department  
40 St. George Street, BA3250  
Toronto, Ontario, Canada  
☎ +1 (416)-978-6055  
✉ fanl@cs.toronto.edu  
🌐 <http://www.cs.toronto.edu/~fanl/>

---

## Biographical Information

### Personal

Work Addr 40 St. George Street, BA3250, Toronto, ON, Canada  
Phone 416-978-6055

### Degrees

- October 2017 **Ph.D., Electrical Engineering and Computer Science,**  
*Massachusetts Institute of Technology*, Cambridge, MA.  
Thesis: Automatic Patch Generation via Learning from Successful Human Patches  
Advisor: Prof. Martin Rinard
- September 2012 **S.M., Electrical Engineering and Computer Science,**  
*Massachusetts Institute of Technology*, Cambridge, MA.  
Thesis: Automatic Input Rectification  
Advisor: Prof. Martin Rinard
- July 2010 **B.S., Computer Science, Tsinghua University**, Beijing, China.  
Enrolled in Tsinghua Xuetang Special Pilot CS Class (Directed by Prof. Andrew Yao)

### Employment

- July 2025 - **Associate Professor,**  
Present *University of Toronto, Computer Science Department (Cross Appointed by Electrical and Computer Engineering Department)*, Toronto, Ontario, Canada.
- September 2018 - June 2025 **Assistant Professor,**  
*University of Toronto, Computer Science Department*, Toronto, Ontario, Canada.

### Honours

- 2025 ACM SIGSOFT International Symposium on Software Testing and Analysis Most Influential Paper Award
- 2024 ACM/IEEE International Conference on Software Engineering Best Paper Award
- 2022 IEEE International Conference on Blockchain and Cryptocurrency Best Paper Award
- 2018 ACM SIGSOFT Dissertation Award
- 2018 MIT CSAIL Dissertation Award
- 2008 Silver Medal (6th place) and Asia Champion in ACM-ICPC World Finals.
- 2007 Gold Medal (1st place) in ACM-ICPC Changchun Regional.
- 2006 Gold Medal (3rd place) in 18th International Olympiad in Informatics.
- 2005 Gold Medal in 17th International Olympiad in Informatics.

---

## Academic History

### Research Interests

My areas of interest are software engineering, programming languages, security, and blockchains.

### Ongoing Project

2018-Present **Smart Contract Security in Blockchains:**

Design and implement new programming language concepts and tools to secure smart contracts in blockchain systems [9, 10, 18, 4, 6, 3, 2].

2018-Present **Blockchain Consensus Algorithms:**

The performance remains one of the most critical challenges of current blockchains. The goal is to design and implement new consensus algorithms together with end-to-end systems that can alleviate this performance limitation [19, 20].

2019-Present **Blockchain Gossip Network:**

As consensus protocols improved, the transaction propagation in the gossip network becomes the new performance bottleneck. The goal is to design and implement novel gossip network protocols to save bandwidth during transaction propagation [17, 8].

2020-Present **Blockchain Storage Protocol:**

Design and implement new blockchain storage protocols that enable faster read/write access and/or reduce the storage size of participants maintaining the blockchain state [11].

2021-Present **Transaction Execution Optimization:**

Design and implement novel techniques to optimize transaction executions in blockchain systems, including parallizing transaction executions [12, 14].

2020-Present **Accelerating Cryptographic Computations:**

Design and Implement GPU/special hardware solutions to accelerate cryptographic computations [13, 15].

### Previous Projects

2014-2018 **Automatic Patch Generation:**

Systematically analyzed previous patch generation techniques and identified several critical issues [23, 28]. Designed and implemented a series of automatic patch generation systems [24, 27, 28].

2013-2014 **Lightweight Error Recovery via Recovery Shepherd:**

Designed and implemented RCV [32], a lightweight dynamic program analysis and runtime system for enabling software applications to recover from fatal null-dereference and divide-by-zero errors.

2012-2014 **Sound Input Filtering for Integer Overflow Errors:**

Designed and implemented SIFT [31], the first sound input filter system for critical integer overflow errors.

2010-2012 **Automatic Input Rectification:**

Designed and implemented SOAP [34], the first automatic input rectification system that changes atypical inputs, instead of discarding them, to preserve desirable data in atypical but benign inputs.

2014-2015 **Automatic Code Transfer:**

Helped design and implement CodePhage [29], the first patch generation tool that transfers correct code across applications.

- 2014-2015 **Attacks on the Weakness of Control Flow Integrity:**  
Analyzed the imprecision of the control flow graphs (CFG) constructed by pointer analysis algorithms. The analysis enables control-jujutsu attacks on fine-grained control flow integrity (CFI) techniques that rely on such imprecise CFGs [25].
- 2012-2015 **Automatic Overflow Bug Finding:**  
Helped design and implement DIODE [30], a concolic execution tool that finds critical integer overflow errors at memory allocation sites.
- 2010-2013 **Automatic Program Generation from Natural Language:**  
Helped design and implement NL2P [33], a novel synthesis tool that automatically generates input parser programs from natural language descriptions of the input format.
- 2008-2009 **Automatic API Documentation Generation:**  
Designed and implemented Altair [37], a novel API documentation generation tool. It uses a combination of machine learning and program analysis techniques to generate cross-reference sections for API documents.
- 2008-2010 **Targeted Record and Replay for Debugging:**  
Designed and implemented iTarget [36], a lightweight record and replay system that enables targeted replay of specific components of a software application.
- 2008 **Model Checking of Distributed Systems**  
Helped implement MODIST [38], a model checking tool that automatically finds critical errors in real world large distributed systems.
- Research Awards
- 2024 Cong Wang Blockchain/AI Fund, \$334,525
- 2022-2024 MITACS Accelerate Grant with Bank of Canada, 2022 September, \$100,500
- 2020-2021 Model X from Bank of Canada, 2020 October, \$3,000
- 2020-2025 NSERC Discovery Grant, 2020 April, \$157,500
- 2019-2021 Connaught New Researcher Award, 2019 April, \$19,190

---

## Refereed Publications

- [1] Honghua Dong, Jiacheng Yang, Xun Deng, Yuhe Jiang, Gennady Pekhimenko, Fan Long, and Xujie Si. TypyBench: Evaluating LLM type inference for untyped Python repositories. In *Proceedings of the 42nd International Conference on Machine Learning*, volume 267 of *Proceedings of Machine Learning Research*, Vancouver, Canada, 13–19 Jul 2025. PMLR.
- [2] Zhiyang Chen, Ye Liu, Sidi Mohamed Beillahi, Yi Li, and Fan Long. Demystifying invariant effectiveness for securing smart contracts. *Proc. ACM Softw. Eng.*, 1(FSE):1–24, jul 2024.
- [3] Zhiyang Chen, Sidi Mohamed Beillahi, and Fan Long. Flashsyn: Flash loan attack synthesis via counter example driven approximation. In *Proceedings of the IEEE/ACM 46th International Conference on Software Engineering*, ICSE ’24, New York, NY, USA, 2024. Association for Computing Machinery.
- [4] Xun Deng, Sidi Mohamed Beillahi, Cyrus Minwalla, Han Du, Andreas Veneris, and Fan Long. Safeguarding defi smart contracts against oracle deviations. In *Proceedings of the IEEE/ACM 46th International Conference on Software Engineering*, ICSE ’24, New York, NY, USA, 2024. Association for Computing Machinery.
- [5] Chenxing Li, Sidi Mohamed Beillahi, Guang Yang, Ming Wu, Wei Xu, and Fan Long. LVMT: An efficient authenticated storage for blockchain. In *17th USENIX Symposium on*

*Operating Systems Design and Implementation (OSDI 23)*, pages 135–153, Boston, MA, July 2023. USENIX Association.

- [6] Xun Deng, Zihan Zhao, Sidi Mohamed Beillahi, Han Du, Cyrus Minwalla, Keerthi Nelaturu, Andreas Veneris, and Fan Long. A robust front-running methodology for malicious flash-loan defi attacks. In *2023 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS)*, pages 1–10, 2023.
- [7] Srisht Fateh Singh, Panagiotis Michalopoulos, Sidi Mohamed Beillahi, Andreas Veneris, and Fan Long. Möbius: an atomic state sharding design for account-based blockchains. In *2023 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, pages 1–9, 2023.
- [8] Mingxun Zhou, Liyi Zeng, Yilin Han, Peilun Li, Fan Long, Dong Zhou, Ivan Beschastnikh, and Ming Wu. Mercury: Fast transaction broadcast in high performance blockchain systems. In *IEEE INFOCOM 2023 - IEEE Conference on Computer Communications*, pages 1–10, 2023.
- [9] Zihan Zhao, Sidi Mohamed Beillahi, Ryan Song, Yuxi Cai, Andreas Veneris, and Fan Long. Sigvm: enabling event-driven execution for truly decentralized smart contracts. *Proc. ACM Program. Lang.*, 6(OOPSLA2), oct 2022.
- [10] Sidi Mohamed Beillahi, Eric Keilty, Keerthi Nelaturu, Andreas Veneris, and Fan Long. Automated Auditing of Price Gouging TOD Vulnerabilities in Smart Contracts. In *Proceedings of the 2022 International Conference on Blockchain and Cryptocurrency*. IEEE, 2022.
- [11] Jemin Andrew Choi, Sidi Mohamed Beillahi, Peilun Li, Andreas Veneris, and Fan Long. LMPTs: Eliminating storage bottlenecks for processing blockchain transactions. In *Proceedings of the 2022 International Conference on Blockchain and Cryptocurrency*. IEEE, 2022.
- [12] Peter Garamvolgyi, Yuxi Liu, Dong Zhou, Fan Long, and Ming Wu. Utilizing parallelism in smart contracts on decentralized blockchains by taming application-inherent conflicts. In *Proceedings of the 44th International Conference on Software Engineering, ICSE 2022, Pittsburgh, PA, USA, 2022*. ACM.
- [13] Ao Li, Bojian Zheng, Gennady Pekhimenko, and Fan Long. Automatic horizontal fusion for gpu kernels. In *2022 IEEE/ACM International Symposium on Code Generation and Optimization (CGO)*, pages 14–27, 2022.
- [14] Keerthi Nelaturu, Sidi Mohamed Beillahi, Fan Long, and Andreas Veneris. Smart contracts refinement for gas optimization. In *2021 3rd Conference on Blockchain Research Applications for Innovative Networks and Services (BRAINS)*, pages 229–236, 2021.
- [15] Ye Zhang, Shuo Wang, Xian Zhang, Jiangbin Dong, Xingzhong Mao, Fan Long, Cong Wang, Dong Zhou, Mingyu Gao, and Guangyu Sun. Pipezk: Accelerating zero-knowledge proof with a pipelined architecture. In *48th ACM/IEEE Annual International Symposium on Computer Architecture, ISCA 2021, Valencia, Spain, June 14-18, 2021*, pages 416–428. IEEE, 2021.
- [16] Yuxi Cai, Fan Long, Andreas Park, and Andreas Veneris. Engineering economics in the conflux network. In *2020 2nd Conference on Blockchain Research Applications for Innovative Networks and Services (BRAINS)*, pages 160–167, 2020.

- [17] Yilin Han, Chenxing Li, Peilun Li, Ming Wu, Dong Zhou, and Fan Long. Shrec: Bandwidth-efficient transaction relay in high-throughput blockchain systems. In *Proceedings of the 11th ACM Symposium on Cloud Computing*, SoCC '20, page 238252, New York, NY, USA, 2020. Association for Computing Machinery.
- [18] Ao Li, Andrew Jemin Choi, and Fan Long. Securing smart contract with runtime validation. In *Proceedings of the 41th ACM SIGPLAN Conference on Programming Language Design and Implementation*, PLDI 2020. ACM, 2020.
- [19] Chenxin Li, Peilun Li, Dong Zhou, Zhe Yang, Ming Wu, Wei Xu, Fan Long, and Andrew Yao. A decentralized blockchain with high throughput and fast confirmation. In *Proceedings of the 2020 USENIX Conference on USENIX Annual Technical Conference*, USENIXATC 2020. USENIX Association, 2020.
- [20] Peilun Li, Guosai Wang, Xiaoqi Chen, Fan Long, and Wei Xu. Gosig: A scalable and high-performance byzantine consensus for consortium blockchains. In *Proceedings of the 11th ACM Symposium on Cloud Computing*, SoCC '20, page 223237, New York, NY, USA, 2020. Association for Computing Machinery.
- [21] Fan Long, Peter Amidon, and Martin Rinard. Automatic inference of code transforms for patch generation. In *Proceedings of the 2017 11th Joint Meeting on Foundations of Software Engineering*, ESEC/FSE 2017, pages 727–739, New York, NY, USA, 2017. ACM.
- [22] Stelios Sidiroglou-Douskos, Eric Lahtinen, Anthony Eden, Fan Long, and Martin Rinard. Codecarboncopy. In *Proceedings of the 2017 11th Joint Meeting on Foundations of Software Engineering*, ESEC/FSE 2017, pages 95–105, New York, NY, USA, 2017. ACM.
- [23] Fan Long and Martin Rinard. An analysis of the search spaces for generate and validate patch generation systems. In *Proceedings of the 38th International Conference on Software Engineering*, ICSE 2016, pages 702–713, New York, NY, USA, 2016. ACM.
- [24] Fan Long and Martin Rinard. Automatic patch generation by learning correct code. In *Proceedings of the 43rd Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, POPL 2016, pages 298–312, New York, NY, USA, 2016. ACM.
- [25] Isaac Evans, Fan Long, Ulziibayar Otgonbaatar, Howard Shrobe, Martin Rinard, Hamed Okhravi, and Stelios Sidiroglou-Douskos. Control jujutsu: On the weaknesses of fine-grained control flow integrity. In *Proceedings of the 22Nd ACM SIGSAC Conference on Computer and Communications Security*, CCS 2015, pages 901–913, New York, NY, USA, 2015. ACM.
- [26] Brendan Juba, Christopher Musco, Fan Long, Stelios Sidiroglou-Douskos, and Martin C. Rinard. Principled sampling for anomaly detection. In *22nd Annual Network and Distributed System Security Symposium, NDSS 2015, San Diego, California, USA, February 8-11, 2015*, 2015.
- [27] Fan Long and Martin Rinard. Staged program repair with condition synthesis. In *Proceedings of the 2015 10th Joint Meeting on Foundations of Software Engineering*, ESEC/FSE 2015, pages 166–178, New York, NY, USA, 2015. ACM.
- [28] Zichao Qi, Fan Long, Sara Achour, and Martin Rinard. An analysis of patch plausibility and correctness for generate-and-validate patch generation systems. In *Proceedings of the 2015 International Symposium on Software Testing and Analysis*, ISSTA 2015, pages 24–36, New York, NY, USA, 2015. ACM.

- [29] Stelios Sidiroglou-Douskos, Eric Lahtinen, Fan Long, and Martin Rinard. Automatic error elimination by horizontal code transfer across multiple applications. In *Proceedings of the 36th ACM SIGPLAN Conference on Programming Language Design and Implementation*, PLDI 2015, pages 43–54, New York, NY, USA, 2015. ACM.
- [30] Stelios Sidiroglou-Douskos, Eric Lahtinen, Nathan Rittenhouse, Paolo Piselli, Fan Long, Deokhwan Kim, and Martin Rinard. Targeted automatic integer overflow discovery using goal-directed conditional branch enforcement. In *Proceedings of the Twentieth International Conference on Architectural Support for Programming Languages and Operating Systems*, ASPLOS 2015, pages 473–486, New York, NY, USA, 2015. ACM.
- [31] Fan Long, Stelios Sidiroglou-Douskos, Deokhwan Kim, and Martin Rinard. Sound input filter generation for integer overflow errors. In *Proceedings of the 41st ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, POPL 2014, pages 439–452, New York, NY, USA, 2014. ACM.
- [32] Fan Long, Stelios Sidiroglou-Douskos, and Martin Rinard. Automatic runtime error repair and containment via recovery shepherding. In *Proceedings of the 35th ACM SIGPLAN Conference on Programming Language Design and Implementation*, PLDI 2014, pages 227–238, New York, NY, USA, 2014. ACM.
- [33] Tao Lei, Fan Long, Regina Barzilay, and Martin C. Rinard. From natural language specifications to program input parsers. In *Proceedings of the 51st Annual Meeting of the Association for Computational Linguistics, ACL 2013, 4-9 August 2013, Sofia, Bulgaria, Volume 1: Long Papers*, pages 1294–1303, 2013.
- [34] Fan Long, Vijay Ganesh, Michael Carbin, Stelios Sidiroglou, and Martin Rinard. Automatic input rectification. In *Proceedings of the 2012 International Conference on Software Engineering*, ICSE 2012, pages 80–90. IEEE Press, 2012.
- [35] Zhenyu Guo, Dong Zhou, Haoxiang Lin, Mao Yang, Fan Long, Chaoqiang Deng, Changshu Liu, and Lidong Zhou. G2: A graph processing system for diagnosing distributed systems. In *Proceedings of the 2011 USENIX Conference on USENIX Annual Technical Conference*, USENIXATC 2011, pages 27–27, Berkeley, CA, USA, 2011. USENIX Association.
- [36] Ming Wu, Fan Long, Xi Wang, Zhilei Xu, Haoxiang Lin, Xuezheng Liu, Zhenyu Guo, Huayang Guo, Lidong Zhou, and Zheng Zhang. Language-based replay via data flow cut. In *Proceedings of the Eighteenth ACM SIGSOFT International Symposium on Foundations of Software Engineering*, FSE 2010, pages 197–206, New York, NY, USA, 2010. ACM.
- [37] Fan Long, Xi Wang, and Yang Cai. Api hyperlinking via structural overlap. In *Proceedings of the the 7th Joint Meeting of the European Software Engineering Conference and the ACM SIGSOFT Symposium on The Foundations of Software Engineering*, ESEC/FSE 2009, pages 203–212, New York, NY, USA, 2009. ACM.
- [38] Junfeng Yang, Tisheng Chen, Ming Wu, Zhilei Xu, Xuezheng Liu, Haoxiang Lin, Mao Yang, Fan Long, Lintao Zhang, and Lidong Zhou. Modist: Transparent model checking of unmodified distributed systems. In *Proceedings of the 6th USENIX Symposium on Networked Systems Design and Implementation*, NSDI 2009, pages 213–228, Berkeley, CA, USA, 2009. USENIX Association.

- [1] Zhiyang Chen, Sidi Mohamed Beillahi, and Fan Long. Flashsyn: Flash loan attack synthesis via counter example driven approximation. *arXiv preprint*, 2206.10708, 2022.
- [2] Andreas Veneris, Andreas Park, Fan Long, and Poonam Puri. Central bank digital loonie: Canadian cash for a new global economy. *SSRN*, 3770024, 2021.
- [3] Chenxing Li, Fan Long, and Guang Yang. Ghast: Breaking confirmation delay barrier in nakamoto consensus via adaptive weighted blocks. *arXiv preprint*, 2006.01072, 2020.
- [4] Ao Li and Fan Long. Detecting standard violation errors in smart contracts. *arXiv preprint*, 1812.07702, 2018.
- [5] Chenxing Li, Peilun Li, Dong Zhou, Wei Xu, Fan Long, and Andrew Chi-Chih Yao. Scaling nakamoto consensus to thousands of transactions per second. *arXiv preprint*, 1805.03870, 2018.

## Teaching and Supervision

### Undergraduate Courses

- CSC488: Compilers and Interpreters (2019 Fall, 2021 Winter, 2022 Winter, 2023 Winter, and 2024 Winter)
- CSC373: Algorithm Design, Analysis & Complexity (2019 Winter)
- CSC324: Principles of Programming Languages (2022 Winter and 2023 Winter)

### Graduate Courses

- CSC2125H: Blockchain Technology & Engineering (2018 Fall, 2019 Fall, 2021 Winter, 2022 Winter, 2023 Winter, and 2024 Winter)

### Research Supervision

- 2021 Sep - **Sidi Mohamed Beillahi, Postdoc**,  
Present working on blockchain systems and smart contract security,  
co-supervised with Andreas Veneris, where I am the primary supervisor.
- 2024 Jul - **Xun Deng, PhD Student, ECE**,  
Present co-supervised with Andreas Veneris, where I am the primary supervisor.
- 2023 Feb - **Zhiyang Chen, PhD Student**,  
Present Securing Smart Contracts with Dynamically Inferred Invariants
- 2023 Sep - **Jacky Zhou, Master Student**,  
Present Integrating MPC Capability for Smart Contracts in Blockchains
- 2023 May - **Vladyslav Nekriach, Master Student, ECE**,  
Present Heterogenous Blockchain Systems with Multiple Virtual Machines,  
co-supervised with Andreas Veneris, Where I am the primary supervisor.
- 2022 May - **Xun Deng, Master Student, ECE**,  
2024 Jun Utilize Generalized Frontrunning to Defend Smart Contract Attacks,  
co-supervised with Andreas Veneris, where I am the primary supervisor.
- 2021 Sep - **Zhiyang Chen, Master Student**,  
2023 Jan FlashSyn: Flash Loan Attack Synthesis via Counter Example Driven Approximation
- 2021 Sep - **Hossein Ghotbaddini, Master Student**,  
2023 Jan Parallelizing Blockchain Transaction Execution via Automatic Increment Detection

- 2021 Sep - **Srisht Fateh Singh, Master Student, ECE,**  
 2023 Jun Sustainable State Sharding and Token Liquidity Provision for the Blockchain Ecosystem, co-supervised with Andreas Veneris, where I am the primary supervisor.
- 2020 Sep - **Zihan Zhao, Master Student, ECE,**  
 2022 Jun SigVM: Enabling event-driven execution for autonomous smart contracts.
- 2019 Sep - **Andrew Jemin Choi, Master Student,**  
 2022 Jan LMPTs: Eliminating storage bottlenecks for processing blockchain transactions.
- 2018 Sep - **Ao Li, Master Student,**  
 2020 Jan Detecting Standard Violation Errors in Smart Contracts.
- 2018 Sep - **Yuxi Cai, Master Student, ECE,**  
 2020 Jun Decentralized Oracles and Network Economics in Modern Blockchain Systems, co-supervised with Andreas Veneris, where I am the secondary supervisor.
- 2018 Sep - **Keerthi Nelaturu, PhD Student, ECE,**  
 Present Smart Contract Verification, co-supervised with Andreas Veneris, where I am the secondary supervisor.
- 2022 Apr - **Zhanwen Tan, MScAC Student,**  
 Present High Performance Decentralized Storage System, I acted as his academic research supervisor for his internship project.
- 2019 Jan - **Yilin Han, MScAC Student,**  
 2020 Jan Shrec: Bandwidth Efficient Transaction Relay in High-throughput Blockchain Systems, I acted as his academic research supervisor for his internship project.
- 2020 Jan - **Ryan Song, Undergraduate Student,**  
 2020 Dec he worked together with Zihan Zhao on the SigVM project.
- 2020 Sep - **Xiaoxu Guo, PhD Student,**  
 2021 Sep she quited the program due to difficulties cuased by COVID
- Other Mentoring
- Master Thesis Committee/Reader: Mike Maksimov, Torin Viger, Nick Feng, Zachary Cetinic
- PhD Thesis Committee: Jeremy Ko, Bangtian Liu, Gengrui Zhang (ECE), Boyue Hu, Torin Viger
- External Co-Supervision: Peilun Li (2017-2021, Tsinghua University), Chenxing Li (2017-2022, Tsinghua University)

## Administrative Positions

### Committee Services

- 2021-2022 **Awards Committee**, *University of Toronto*, Computer Science Department.
- 2019-2022 **Undergraduate Admission Committee**, *University of Toronto*, Computer Science Department.
- 2019-2020 **Graduate Admission Committee**, *University of Toronto*, Computer Science Department.
- 2018-2019 **First Year Learning Committee**, *University of Toronto*, Computer Science Department.

### External Services



- PC
- **PLDI:** Programming Language Design and Implementation (2022, 2020, 2018)
  - **POPL:** Programming Language Design and Implementation (2022)
  - **ASE:** Automated Software Engineering (2022, 2020)
  - **ICBC:** International Conference on Blockchain and Cryptocurrency (2022, 2021, 2020, 2019)
- Reviewers
- **PLDI:** Programming Language Design and Implementation (2016 ERC)
  - External reviewers for top conferences and journals like POPL, ICSE, TOSEM, ESE, etc..