Jason Richmond Teutsch

Phone: +1 (858) 224-2364
Email: jt@truebit.io
Personal web: https://people.cs.uchicago.edu/~teutsch/
Project web: https://truebit.io

Positions held

TrueBit
Founder — 2017–

National University of Singapore
Senior Research Fellow in School of Computing — 2015–2016

Fulbright Fellow to Israel — 2013, 2014–2015

Penn State University
Postdoc in Computer Science & Engineering — 2012–2013

Johns Hopkins University
Human Language Technology Center Of Excellence
Associate Staff Scientist — 2011–?

Ruprecht-Karls-Universität Heidelberg
Postdoc at Institut für Informatik — 2010–2011

Center for Communications Research
Research Staff — 2008–2010

RAND Corporation
Postdoctoral Fellow — 2007–2008

UCLA
Visiting Scholar in Mathematics — 2007–2008

University of Chicago
Teaching Assistant in Computer Science — 2005–2006

Indiana University
Associate Instructor in Mathematics — 2001–2004

Fulbright Fellow to Hungary — 2000–2001

Education

Indiana University
PhD, mathematics — 2007
Doctoral Minor, music composition
Certificate in Logic, Language, and Computation

University of Chicago
CIC Traveling Scholar in computer science — 2005–2007

Pomona College
BA, classical guitar & pure mathematics — 2000

Budapest Semesters in Mathematics — Fall 1998

Research interests cryptocurrencies, distributed systems security, game theory, shortest computer programs, and algorithmic randomness.

Talks

[1]	Stanford Blockchain Collective	Mar. 2018
[2]	Stanford Security Lunch	Feb. 2018
[3]	SF Ethereum Developers Meetup	Dec. 2017
[4]	Token Summit II	Dec. 2017
[5]	Devcon3 (Cancún)	Nov. 2017
[6]	Crypto Economics Security Conference (Berkeley)	Oct. 2017
[7]	USENIX Security Symposium (Vancouver)	Aug. 2017
[8]	UAB Mathematics Colloquium	Oct. 2016
[9]	UAB CIS Seminar	Sept. 2016
[10]	University of North Texas CSE	Mar. 2016
[11]	Financial Cryptography and Data Security (Barbados)	Feb. 2016
[12]	Chinese Academy of Sciences Institute of Software	Oct. 2015
[13]	Computability, Complexity, and Randomness (Heidelberg)	June 2015
[14]	MIT Lincoln Laboratory	Sept. 2014
[15]	Computability, Complexity, and Randomness (Singapore)	June 2014
[16]	Computability, Complexity, and Randomness (Moscow)	Sept. 2013
[17]	National University of Singapore CS Theory and Logic seminars	Apr. 2013
[18]	Johns Hopkins CS Theory Seminar	Feb. 2013
[19]	Center for Computing Sciences–Bowie	Feb. 2013
[20]	Universidad de Los Andes Math Colloquium	Feb. 2013
[21]	UCSD CSE Theory Seminar	Feb. 2013
[22]	Joint Mathematics Meetings (San Diego)	Jan. 2013
[23]	National Security Agency	Aug. 2012
[24]	Computability, Complexity, and Randomness (Cambridge, UK)	July 2012
[25]	Reed College Math Colloquium	June 2012
[26]	Penn State University Logic Seminar	Mar. 2012
[27]	University of Louisville Math Colloquium	Jan. 2012
[28]	UCSD Randomness & Complexity Seminar	Jan. 2012
[29]	Computability, Complexity and Randomness (Cape Town)	Feb. 2011
[30]	National University of Singapore Logic Seminar	Jan. 2011
[31]	Bar-Ilan Probability Seminar	Jan. 2011
[32]	Hebrew University CS Theory Seminar	Dec. 2011
[33]	Ben-Gurion University Computer Science Colloquium	Dec. 2010
[34]	Ruprecht-Karls-Universität Heidelberg, Institut für Informatik	Nov. 2010
[35]	Logic, Computability and Randomness (South Bend)	May 2010
[36]	Computability in Europe (Heidelberg)	June 2009
[37]	Okinawa Institute of Science and Technology	Mar. 2008
[38]	Center for Communications Research–La Jolla	Jan. 2008
[39]	University of Delaware Computer & Information Sciences	Nov. 2007
[40]	UCLA Logic Colloquium	Nov. 2007
[41]	National University of Singapore Logic Seminar	July 2007
[42]	National Security Agency	Jan. 2007
[43]	University of Chicago Logic Seminar	Nov. 2006
[44]	University of Chicago Theory of Computing Seminar	Nov. 2005
[45]	Indiana University Logic Seminar	Nov. 2004
[46]	IMA Program in Coding and Cryptography (South Bend)	June 2004

Grants and awards

Wanxiang Blockchain Labs Sponsorship Program
"TrueBit: a verification and storage solution for blockchains"
PI with Christian Reitwießner, $10,000 — 2016

Fulbright fellowship to Israel — 2013, 2014-2015

Fulbright fellowship to Hungary — 2000–2001

Blanchard Prize in [music] Composition from Pomona College — May 2000

American Recorder Society & Canto Antiguo workshop grants — Summer 1998

Work visits

Chinese Academy of Sciences travel grant — Sept.–Oct. 2015

Institute for Computational and Experimental Research in Mathematics
travel grant — Aug. 2014

National University of Singapore: Institute for Mathematical Sciences
+ Center for Quantum Technologies + Mathematics Department — 5–6/2014

National University of Singapore (NUS) — 4/2013, 1/2011, 2–3/2010, 6–8/2007

Newton Institute and Assocation for Symbolic Logic travel grants — July 2012

American Institute of Mathematics travel grant — Aug. 2007

Nanyang Technical University travel grant — Aug. 2007

NSF quantum computing fellowship — Summer 2003

Joint Program in Survey Methodology Junior Fellow — Summer 1999

Pomona College Summer Undergraduate Research Program — Summer 1998

Referee work

Computability
Computability in Europe (CiE)
Games and Economic Behavior
IEEE Conference on Computational Complexity (CCC)
IEEE Symposium on Foundations of Computer Science (FOCS)
IEEE Transactions on Information Theory
IEEE Transactions on Information Forensics & Security
Information and Computation
Information Processing Letters
Innovations in Computer Science (ITCS)
International Journal of Foundations of Computer Science
Journal of the ACM
Journal of Computer and System Sciences
Journal of Information Security and Applications
Journal of Symbolic Logic
Ledger
Logical Methods in Computer Science
Symposium on Mathematical Foundations of Computer Science (MFCS)
Symposium on Theory of Computing (STOC)
Theoretical Computer Science

Program committees

1st and 2nd Workshop on Trusted Smart Contracts
Crypto Economics Security Conference (CESC) 2017, 2018
ETHWaterloo Hackathon (Judge)

References

- Ken Ehrenberg, *University of Surrey*
- Lance Fortnow, *Georgia Tech* (PhD advisor)
- Sanjay Jain, *National University of Singapore*
- Prateek Saxena, *National University of Singapore* (postdoc supervisor)
- Steve Simpson, *Vanderbilt University*
- Frank Stephan, *National University of Singapore*
- Christian Reitwießner, *Ethereum Foundation*

JOURNAL PAPERS

[1] Jason Teutsch, Michael Straka, and Dan Boneh. Retrofitting a two-way peg between blockchains.

[2] Jason Teutsch. On decentralized oracles for data availability.

[3] Jason Teutsch, Vitalik Buterin, and Christopher Brown. Interactive coin offerings. (submitted).

[4] Jason Teutsch and Christian Reitwießner. A scalable verification solution for blockchains.

[5] Sanjay Jain and Jason Teutsch. Enumerations including laconic enumerators. *Theoretical Computer Science*, 700:89–95, 2017.

[6] Sanjay Jain, Frank Stephan, and Jason Teutsch. Closed left-r.e. sets. *Computability*, 6(1):1–21, 2017.

[7] George Barmpalias, Andrew Lewis-Pye, and Jason Teutsch. Lower bounds on the redundancy in computations from random oracles via betting strategies with restricted wagers. *Information and Computation*, 251:287–300, December 2016.

[8] Jason Teutsch and Marius Zimand. On approximate decidability of minimal programs. *ACM Transactions on Computational Theory*, 7(4):17:1–17:16, August 2015.

[9] Greg Clark and Jason Teutsch. Maximizing T-complexity. *Fundamenta Informaticae*, 139(1):1–19, 2015.

[10] Jason Teutsch. Short lists for shortest descriptions in short time. *Computational Complexity*, 23(4):565–583, December 2014.

[11] Frank Stephan and Jason Teutsch. Things that can be made into themselves. *Information and Computation*, 237:174–186, October 2014.

[12] Randall Dougherty, Jack H. Lutz, Daniel R. Mauldin, and Jason Teutsch. Translating the Cantor set by a random real. *Transactions of the American Mathematical Society*, 366:3027–3041, 2014.

[13] Jason Teutsch. A savings paradox for integer-valued gambling strategies. *International Journal of Game Theory*, 43(1):145–151, February 2014.

[14] Wolfgang Merkle and Jason Teutsch. Constant compression and random weights. *Computability*, 1(2):153–169, 2012.

[15] Bjørn Kjos-Hanssen, Frank Stephan, and Jason Teutsch. Arithmetic complexity via effective names for random sequences. *ACM Transactions on Computational Logic*, 13(3):24:1–24:18, August 2012.

[16] Frank Stephan and Jason Teutsch. An incomplete set of shortest descriptions. *The Journal of Symbolic Logic*, 77(1):291–307, March 2012.

[17] Adam Chalcraft, Randall Dougherty, Chris Freiling, and Jason Teutsch. How to build a probability-free casino. *Information and Computation*, 211:160–164, February 2012.

[18] Laurent Bienvenu, Frank Stephan, and Jason Teutsch. How powerful are integer-valued martingales? *Theory of Computing Systems*, 51(3):330–351, October 2012. Special issue for CiE 2010.

[19] Sanjay Jain, Frank Stephan, and Jason Teutsch. Index sets and universal numberings. *Journal of Computer and System Sciences*, 77(4):760–773, July 2011.

[20] Frank Stephan and Jason Teutsch. Immunity and hyperimmunity for sets of minimal indices. *Notre Dame Journal of Formal Logic*, 49(2):107–125, 2008.

[21] Jason Teutsch. On the Turing degrees of minimal index sets. *Annals of Pure and Applied Logic*, 148:63–80, September 2007.

Conference papers

[1] Loi Luu, Yaron Velner, Jason Teutsch, and Prateek Saxena. SmartPool: Practical Decentralized Pooled Mining. In *26th USENIX Security Symposium (USENIX 17)*, pages 1409–1426, Vancouver, BC, 2017. USENIX Association.

[2] Yaron Velner, Jason Teutsch, and Loi Luu. Smart contracts make Bitcoin mining pools vulnerable. In *Financial Cryptography and Data Security (BITCOIN 2017)*, pages 298–316. Springer Cham, 2017. To appear in *4th Workshop on Bitcoin and Blockchain Research*.

[3] Jason Teutsch, Sanjay Jain, and Prateek Saxena. When cryptocurrencies mine their own business. In *Financial Cryptography and Data Security: 20th International Conference (FC 2016) Christ Church, Barbados*, pages 499–514. Springer Berlin / Heidelberg, 2017.

[4] Loi Luu, Jason Teutsch, Raghav Kulkarni, and Prateek Saxena. Demystifying incentives in the consensus computer. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (CCS 2015)*, pages 706–719, New York, NY, USA, 2015. ACM.

[5] Nirupama Talele, Jason Teutsch, Robert Erbacher, and Trent Jaeger. Monitor placement for large-scale systems. In *Proceedings of the 19th ACM Symposium on Access Control Models and Technologies (SACMAT 2014)*, pages 29–40, New York, NY, USA, 2014. ACM.

[6] Wolfgang Merkle, Frank Stephan, Jason Teutsch, Wei Wang, and Yue Yang. Selection by recursively enumerable sets. In *Theory and Applications of Models of Computation (TAMC 2013)*, volume 7876 of *Lecture Notes in Computer Science*, pages 144–155. Springer, Berlin / Heidelberg, 2013.

[7] Nirupama Talele, Jason Teutsch, Trent Jaeger, and Robert F. Erbacher. Using security policies to automate placement of network intrusion prevention. In *Engineering Secure Software and Systems (ESSoS 2013)*, volume 7781 of *Lecture Notes in Computer Science*, pages 17–32. Springer, Berlin / Heidelberg, 2013.

[8] Divya Muthukumaran, Sandra Rueda, Nirupama Talele, Hayawardh Vijayakumar, Trent Jaeger, Jason Teutsch, and Nigel Edwards. Transforming commodity security policies to enforce Clark-Wilson integrity. In *Proceedings of the 28th Annual Computer Security Applications Conference (ACSAC 2012)*, December 2012.

[9] Wolfgang Merkle and Jason Teutsch. Constant compression and random weights. In *29th International Symposium on Theoretical Aspects of Computer Science (STACS 2012)*, volume 14 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 172–181, Dagstuhl, Germany, 2012.

[10] Sanjay Jain, Frank Stephan, and Jason Teutsch. Closed left-r.e. sets. In *Theory and Applications of Models of Computation (TAMC 2011)*, volume 6648 of *Lecture Notes in Computer Science*, pages 218–229. Springer, Berlin / Heidelberg, 2011.

[11] Laurent Bienvenu, Frank Stephan, and Jason Teutsch. How powerful are integer-valued martingales? In *Programs, Proofs, Processes (CiE 2010)*, volume 6158 of *Lecture Notes in Computer Science*, pages 59–68. Springer-Verlag, Berlin / Heidelberg, 2010.

[12] Sanjay Jain, Frank Stephan, and Jason Teutsch. Index sets and universal numberings. In *Mathematical Theory and Computational Practice (CiE 2009)*, volume 5635 of *Lecture Notes in Computer Science*, pages 270–279. Springer-Verlag, Berlin / Heidelberg, 2009.

[13] Pascal O. Vontobel, Roxana Smarandache, Negar Kiyavash, Jason Teutsch, and Dejan Vukobratovic. On the minimal pseudo-codewords of codes from finite geometries. In *Proceedings of IEEE International Symposium on Information Theory (ISIT 2005)*, pages 980–984, Adelaide, Australia, 2005.

Miscellaneous

[1] Sanjay Jain, Prateek Saxena, Frank Stephan, and Jason Teutsch. How to verify computation with a rational network. 2016.

[2] Jason Teutsch and Marius Zimand. A brief on short descriptions. *SIGACT News*, 47(1):42–67, March 2016.

[3] Robert F. Erbacher, Trent Jaeger, Nirupama Talele, and Jason Teutsch. Directed Multicut with linearly ordered terminals. 2014.

[4] Jason Teutsch. Review of Algorithmic Randomness and Complexity by Downey and Hirschfeldt. *SIGACT News*, 44(1):25–28, March 2013.

[5] Jason R. Teutsch. *Noncomputable Spectral Sets*. PhD thesis, Indiana University, 2007.

Music Compositions

- NFL Combo (2015), *montage of television music*
- Mimarom (2010), *niggun*
- Cats (2007), *carillon solo*
- Wedding Dance (2005), *clarinet and guitar*
- Dog Food and Harp (2004), *harp solo*
- Gnithon Sessop (2004?), *massive orchestra with double chorus and soloists*
- Two Portraits of a Mexican Woman Named Gordita and one of her Amicable and Fluffy Chinchilla (2003), *flute, clarinet, viola, cello, trumpet, trombone*
- Rose, Sheep, and Lilly (2003), *alto, triangle, timpani*
- Psalm (2003), *bases, viola, piano*
- Toolik (2002), *electronic medium*
- Intuitive Action (2002), *choir and percussion*
- Berlin-Mexico (2001), *harp solo*
- And Also a Dog (2001), *electronic medium*
- Synthesis #3 (2001), *piano solo*
- L, the U, and E (2000), *sopranos and piano*
- Suite for Guitar and String Quartet #2: *American Landscapes* (2000)
- Suite for Guitar and String Quartet #1 (1999)
- Four Paintings by Salvador Dalí (1999), *guitar solo*
- Prelude and two Dances (1998?), *guitar solo*
- Nähe des Geliebten (1996), *tenor and piano*
- Reconstrution of Truth (1997), *piano 4-hands*
- Deconstruction of Truth (1997), *piano solo*
- Cascades (1997?), *recorder solo*
- Swamp monster (1997), *bird/recorder, frog/violin, algae/cello, monster/clarinet, bug/piano*
- Blueberry Rag (1997), *piano solo*

Foreign Languages	Hebrew, Hungarian, Spanish

Solo	Cambridge to Manchester (UK)	July 2012
Bicycle	Québec on a Friday, 400 km	Sept. 2011
Tours	Pacific Coast	To Be Continued / June 2008
	Kingdom of Cambodia, 650 km	July/Aug. 2007
	Sister Bay–Postville–Nauvoo, 1200 mi.	July 2006
	Around Lake Michigan, 1700 mi.	July 2004
	The Southeastern US, 3000 mi.	July 2003
	Philly to Cleveland, 500 mi.	June 2000
	Other rides:	
	BBC Double Century Ride	6/14/2003
	Bicycle Ride Across Georgia, 342 mi.	1995
	Northern California, 900 mi.	1993
	Blue Ridge Parkway, 469 mi.	1992