

# Jason Richmond Teutsch

---

Phone: +1 (858) 224-2364

Personal web: <https://people.cs.uchicago.edu/~teutsch/>

Email: [jt@truebit.io](mailto:jt@truebit.io)

Project web: <https://truebit.io>

---

POSITIONS	<b>TrueBit</b>	
HELD	Founder	2017–
	<b>National University of Singapore</b>	
	Senior Research Fellow in School of Computing	2015–2016
	<b>Fulbright Fellow to Israel</b>	2013, 2014–2015
	<b>Penn State University</b>	
	Postdoc in Computer Science & Engineering	2012–2013
	<b>Johns Hopkins University</b>	
	<b>Human Language Technology Center Of Excellence</b>	
	Associate Staff Scientist	2011–?
	<b>Ruprecht-Karls-Universität Heidelberg</b>	
	Postdoc at Institut für Informatik	2010–2011
	<b>Center for Communications Research</b>	
	Research Staff	2008–2010
	<b>RAND Corporation</b>	
	Postdoctoral Fellow	2007–2008
	<b>UCLA</b>	
	Visiting Scholar in Mathematics	2007–2008
	<b>University of Chicago</b>	
	Teaching Assistant in Computer Science	2005–2006
	<b>Indiana University</b>	
	Associate Instructor in Mathematics	2001–2004
	<b>Fulbright Fellow to Hungary</b>	2000–2001
EDUCATION	<b>Indiana University</b>	
	PhD, <a href="#">mathematics</a>	2007
	Doctoral Minor, <a href="#">music composition</a>	
	Certificate in <a href="#">Logic, Language, and Computation</a>	
	<b>University of Chicago</b>	
	<a href="#">CIC Traveling Scholar</a> in computer science	2005–2007
	<b>Pomona College</b>	
	BA, classical guitar & pure mathematics	2000
	<b>Budapest Semesters in Mathematics</b>	Fall 1998

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

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

- [1] Jason Teutsch. On decentralized oracles for data availability. (submitted).
- [2] Jason Teutsch, Vitalik Buterin, and Christopher Brown. Interactive coin offerings. (submitted).
- [3] Jason Teutsch and Christian Reitwießner. A scalable verification solution for blockchains. (submitted).
- [4] Sanjay Jain and Jason Teutsch. [Enumerations including laconic enumerators](#). *Theoretical Computer Science*, 700:89–95, 2017.
- [5] Sanjay Jain, Frank Stephan, and Jason Teutsch. [Closed left-r.e. sets](#). *Computability*, 6(1):1–21, 2017.
- [6] 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.
- [7] Jason Teutsch and Marius Zimand. [On approximate decidability of minimal programs](#). *ACM Transactions on Computational Theory*, 7(4):17:1–17:16, August 2015.
- [8] Greg Clark and Jason Teutsch. [Maximizing T-complexity](#). *Fundamenta Informaticae*, 139(1):1–19, 2015.
- [9] Jason Teutsch. [Short lists for shortest descriptions in short time](#). *Computational Complexity*, 23(4):565–583, December 2014.
- [10] Frank Stephan and Jason Teutsch. [Things that can be made into themselves](#). *Information and Computation*, 237:174–186, October 2014.
- [11] 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.
- [12] Jason Teutsch. [A savings paradox for integer-valued gambling strategies](#). *International Journal of Game Theory*, 43(1):145–151, February 2014.
- [13] Wolfgang Merkle and Jason Teutsch. [Constant compression and random weights](#). *Computability*, 1(2):153–169, 2012.
- [14] 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.
- [15] Frank Stephan and Jason Teutsch. [An incomplete set of shortest descriptions](#). *The Journal of Symbolic Logic*, 77(1):291–307, March 2012.
- [16] Adam Chalcraft, Randall Dougherty, Chris Freiling, and Jason Teutsch. [How to build a probability-free casino](#). *Information and Computation*, 211:160–164, February 2012.
- [17] 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.
- [18] Sanjay Jain, Frank Stephan, and Jason Teutsch. [Index sets and universal numberings](#). *Journal of Computer and System Sciences*, 77(4):760–773, July 2011.

- [19] Frank Stephan and Jason Teutsch. [Immunity and hyperimmunity for sets of minimal indices](#). *Notre Dame Journal of Formal Logic*, 49(2):107–125, 2008.
- [20] 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. To appear in *4th Workshop on Bitcoin and Blockchain Research (BITCOIN 2017)*.
- [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*
  - Reconstruction 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
	<a href="#">Sister Bay-Postville-Nauvoo</a> , 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
	<i>Other rides:</i>	
	<a href="#">BBC Double Century Ride</a>	6/14/2003
	<a href="#">Bicycle Ride Across Georgia</a> , 342 mi.	1995
	Northern California, 900 mi.	1993
	<a href="#">Blue Ridge Parkway</a> , 469 mi.	1992