PX

16

DECLARATION OF ARVIND NARAYANAN
PURSUANT TO 28 U.S.C. § 1746

I, Arvind Narayanan, hereby state that I have personal knowledge of the facts set forth below and am competent to testify about them. If called as a witness, I could and would testify as follows:

1. I am over 18 years old. I live in New York City, New York.

2. I am an Assistant Professor of Computer Science at Princeton University. I earned a Ph.D. in computer science from the University of Texas at Austin. A true and correct copy of my curriculum vitae is attached to this declaration as **Attachment ("Att.") A**.

3. I have been researching and teaching courses and delivering lectures on Bitcoin for over two years. I currently teach a course on Bitcoin and cryptocurrency technologies which I believe to be the first university course devoted to the computer science behind Bitcoin. The course contains several portions specifically about mining.

4. I am the recipient of the National Science Foundation's (NSF) Award #1421689 "TWC: Small: Addressing the challenges of cryptocurrencies: Security, anonymity, stability" which I believe to be the first US government research grant for Bitcoin and cryptocurrency research. I have co-authored several peer-reviewed publications on Bitcoin with other leading computer scientists. I have been invited to speak about Bitcoin at a variety of academic and industry events, including the 2014 Real World Cryptography conference and the 2014 Hashers United Conference.

5. **The Bitcoin network.** Bitcoin is a digital currency with no central issuing authority. It was introduced as a whitepaper in 2008 and open-source software in 2009 by one Satoshi Nakamoto, whose true identity (or identities) is unknown. The Bitcoin software and peer-to-peer network of "nodes" collectively maintain a digital ledger that records all

transactions. Once a Bitcoin transaction is sent out to the network, it typically gets recorded in the ledger in the next update, which occurs about every 10 minutes, on average.

6. **Mining.** Bitcoin's key innovation is ensuring that the nodes cannot equivocate about which transactions are in the ledger — otherwise, the system would not have any value or meaning as a currency. To achieve this, only some nodes, called miners, are allowed to update the ledger. While anyone may become a miner, there is a price of admission — solving computationally hard "mining puzzles." As a reward for the work of maintaining the ledger, miners are rewarded in newly minted bitcoins. These rules are encoded into the software and collectively enforced by the existing nodes and miners. Any miner that violates these rules will be ignored by the other miners and effectively becomes separated from the Bitcoin network.

7. **Increasing difficulty of mining.** Crucially, the mining reward is a fixed number of bitcoins for every ledger update (at the present time, roughly 25 bitcoins every 10 minutes). Miners are in a contest with each other to collect these rewards. Thus, as more miners enter the network and as miners utilize more powerful hardware, the puzzles automatically become harder and harder to solve so that the mining reward can be issued at a constant rate. For most of Bitcoin's existence, the difficulty level of these puzzles (measured by computational effort required) has grown at an astonishing rate. For example, over the course of year 2013 it grew about 500-fold, representing a doubling in difficulty every 41 days.

8. One reason for such rapid growth is that miners have repeatedly switched to new types of computer chips for mining. Each new type is increasingly specifically tailored to Bitcoin mining and increasingly efficient at it. The newest type, Application-Specific Integrated Circuit (ASIC), is only capable of mining bitcoins (and other derivative cryptocurrencies that operate on the same technology); it is generally worthless for any other computational task.

9. **The miner's costs and revenues.** Assuming that difficulty doubles steadily every two months, a given piece of mining equipment, even if it represents the newest and most efficient technology when the miner purchases it, will rapidly erode in value. If it was switched on in January, by March it would only generate 50% of the mining revenue per day as it did at first. By May, it would only generate 25%, and by July, only 12.5%, at which point, it would likely be considered obsolete. Given that the equipment incurs costs, such as the cost of electricity to operate, after a point, the miner will be unable to generate any profits using it, as costs will exceed revenues. Electricity costs can be substantial -- for example, Defendants' BitForce MiniRig product consumes 1,250 watts, about as much as a large air-conditioning window unit.

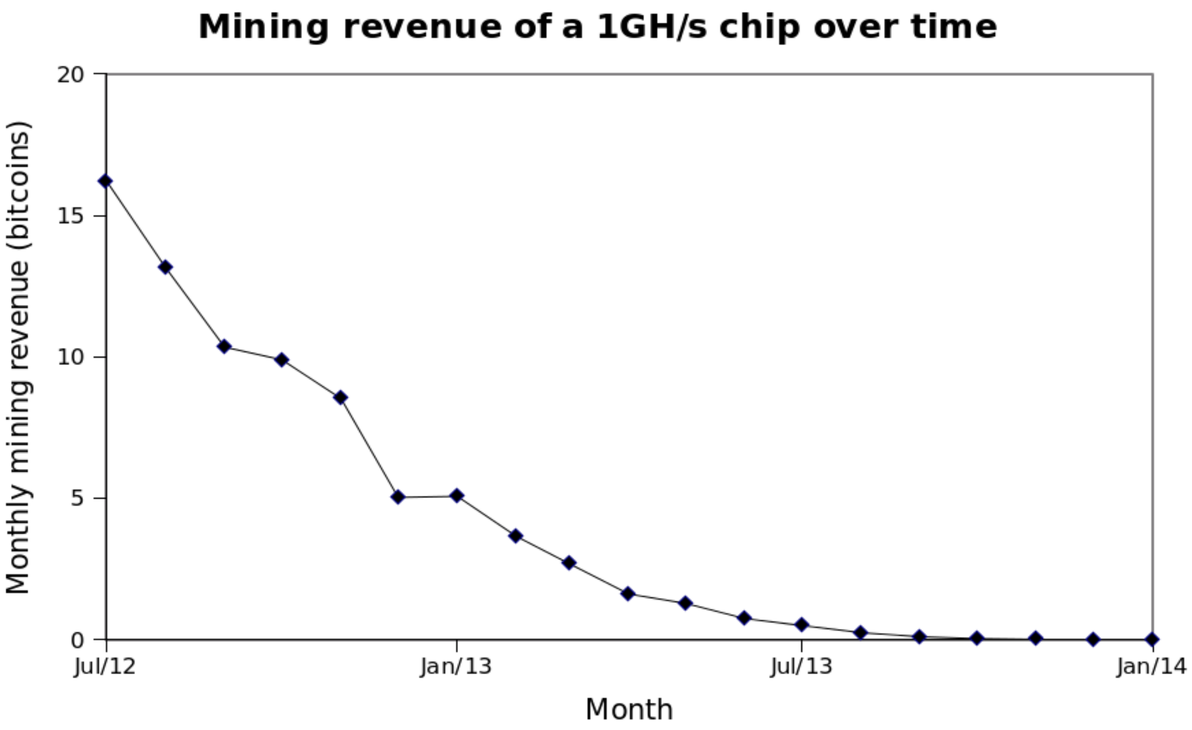
10. The miner's fundamental challenge is to acquire equipment early enough in the technology lifecycle to maximize its operational lifetime. If he succeeds, he will be able to use it for long enough — typically, a few months — to recoup the cost of the hardware investment and make an overall profit.

11. **Retrospective calculation of profitability.** It is possible to calculate exactly how much revenue a piece of mining equipment would have generated before its obsolescence if it had been first operated on a given date. To perform this calculation, I needed to know the speed of the hardware, measured in gigahashes per second (GH/s), as well as historical data on the growth of difficulty of the mining puzzles. I downloaded the historical data from the website blockchain.info.

12. Using this data, I computed a table that tracks the depreciation of mining equipment over time. To compute each day's entry in the table, I first calculate the 24-hour mining reward based on the per-block reward and divide the result by that day's network hash

rate (expressed in GH/s). The table takes into account the fact that the mining reward halved from 50 bitcoins per 10-minute block to 25 bitcoins per 10-minute block in November 2012 in accordance with a pre-specified formula in the Bitcoin Network software.

13. For each day starting January 2009 to the present time, the table describes how much revenue in bitcoins a fixed piece of mining equipment (whose speed is 1GH/s) would generate. The figure below summarizes the information in this table for the period of interest. The information in the table is available upon request.



14. **Impact of BitForce shipping delays.** Defendants advertised their initial line of BitForce ASIC machines as shipping in October 2012. I analyzed the impact of delays on the "BitForce Jalapeno" machines; the results are essentially identical for the other BitForce machines in terms of the impact of shipping delays on depreciation in percentage terms.

15. According to my table, the lifetime mining revenues (LMR) for a Jalapeno machine (whose advertised speed and power consumption are 4.5 GH/s and 4.5 watts, respectively) that was hypothetically delivered in October 2012 and first operated on October 31, 2012 is ฿ 134.9. The LMR is calculated by adding the daily mining revenues specified in the table, starting from October 31, 2012, and multiplying the result by 4.5 to account for the machine's speed.

16. For a Jalapeno machine first operated on Sep 30, 2013, the LMR measured in bitcoin is ฿ 0.514. This represents a 263-fold depreciation.

17. On Nov 28 2013, Defendants posted on their website that all the orders for BitForce mining had been shipped. For a Jalapeno machine first operated on November 28, 2013, the LMR is ฿ 0.170. This represents a 793-fold depreciation.

18. If Defendants had shipped a large number of machines on time and customers had begun to operate them in October 2012, this would have increased the total mining power of the Bitcoin network, increasing the mining difficulty and in turn lowering the LMR of each machine delivered. If 20,000 additional Jalapeno machines (or the equivalent in mining power thereof) had been added to the network on October 31, 2012, then the LMR of each shipped Jalapeno machine would be ฿ 36.6. I did not have access to precise data on the volume of pre-orders and the breakdown of these orders between the different machines, but regardless of the precise volume and breakdown, the essential conclusion remains the same: on-time shipping of orders would have diminished the LMR, but by a ratio that is far less than the depreciation caused by the shipping delays.

19. Similar calculations hold for the other BitForce machines. For the "Single SC" with a speed of 40 GH/s, LMR on October 31, 2012, would be ฿ 1,199. If a large volume of

orders (amounting to the mining power specified above) had been delivered at that date, the LMR would be ฿ 325. Delayed delivery on November 28, 2013 decreases the LMR to ฿ 1.512. The corresponding numbers for the "MiniRig SC" with a speed of 1,000 GH/s are ฿ 29,980, and ฿ 8,134, and ฿ 37.8 respectively.

20. *Summary of shipping delay analysis*: a hypothetical consumer who pre-ordered and received a BitForce Jalapeno machine in October 2012 would be able to realize a LMR of between ฿ 134.9 and about ฿ 36.6 depending on how many *other* consumers received similar machines. Instead, consumers experienced shipping delays and received machines with an LMR of between ฿ 0.514 and ฿ 0.170, representing a depreciation of roughly 71-fold in the best case and roughly 800-fold in the worst case.

21. **Effect of pool mining.** Since there is only one ledger update and reward payout roughly every 10 minutes, an individual miner, depending on his mining power, may only be able to win a reward once in several days or months. When he does win, however, the reward is substantial – ฿ 25 is about USD 10,000 at today's exchange rate. This is somewhat analogous to buying lottery tickets. To minimize unpredictability and ensure a steady revenue stream, most miners join "mining pools" that allow them to hedge risk by pooling together their computing power and splitting any reward in proportion to mining power contributed.

22. All findings I present are unaffected by a consumer's decision to join a pool or mine by himself. Pool mining does not change a miner's expected or average revenue except for a small fee of a few percent that may be charged by the pool operator; it merely decreases the day-to-day or month-to-month variation in these revenues.

23. **Analysis of Monarch machines.** In August 2013 Defendants began taking pre-orders of Monarch machines starting at $2,499 with an advertised speed of 700 GH/s and power

consumption of 471 W. Given today's mining difficulty and exchange rate, such a machine currently generates a revenue of USD 3.36/day and costs USD 1.13 to operate assuming a power cost of 10 cents/KWh, which is the US average.

24. A hypothetical consumer who received a 700 GHz Monarch machine by end of 2013, as advertised, and who first operated it on January 1, 2014, would be able to mine ฿ 15.6 using it. By end of 2013, ASIC technology was already so widespread in the market that even shipment of a large volume of Monarch orders would not have significantly affected this figure. However, a consumer who received and first operated a Monarch machine on Aug 31, 2014 would realize a revenue of ฿ 0.787, representing a 20-fold depreciation.

25. Under the implausibly optimistic assumption that the mining difficulty remains constant at the current level, such a machine would break even in slightly over three years (if it had been purchased for $2,499).

26. If the mining difficulty continues to compound at the rate that it has over the past year, a Monarch machine will reach obsolescence in under four months from the present time, generating about USD 240 in mining revenue (and incurring USD 132 in electricity costs).

27. Under the somewhat optimistic assumption that mining difficulty increases linearly (rather than compounding) at the same rate as the last six months, the machine would reach obsolescence in a little over two years, generating USD 1,265 in mining revenue (and incurring USD 1,007 in electricity costs).

28. Thus, a customer of a Monarch machine will not come close to recouping his hardware investment in the most plausible scenarios of the network's evolution.

29. **Bitcoin mining calculator.** Defendants used the third-party "TP's Bitcoin Calculator" in their advertising. This calculator allows consumers to estimate the expected daily

profit, break-even time, and other variables of interest, but under the assumption that mining difficulty (and exchange rate) will remain constant. As historical data shows, this assumption is highly unrealistic. As a result, the calculator presents consumers with exceedingly optimistic estimates of revenue and profitability.

30. For example, on Nov 28, 2013 — the date when Defendants posted that all BitForce orders had been shipped — the calculator would have shown a break-even time of merely 51 days for any of these machines. In reality, the machines were rapidly depreciating in value, nearing obsolescence, and would never break even if switched on on that date.

31. Defendants' Facebook post about this calculator mentions break-even time which is fundamentally about future revenues.

32. **Testing of products.** Defendants' products must interoperate with the Bitcoin peer-to-peer network which follows a complex software protocol. However, the details of this protocol are not implemented in Defendants' hardware product. Rather they are handled by a software controller which runs on a regular computer. Only the mining puzzle is computationally difficult and needs to be executed by Defendant's products.

33. The mining puzzle derives its difficulty from the fact that it requires performing the same calculation (called a "hash function") over and over again with different inputs. This hash function is in fact a mathematical formula that is independent of, and long predates, the Bitcoin protocol. I therefore know of no technological reason why ASIC mining hardware must be tested on the live Bitcoin network.

34. Furthermore, even if testing on the live network were necessary, there is a way to ensure that it does not affect the network: simply modify the software to only verify that the hardware solved the mining puzzles correctly but not broadcast the solved puzzles to the rest of

the network. Existing mining software such as BFGMiner (bfgminer.com) seems to already support a similar feature ("benchmark mode").

Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury that the statements made in this declaration are true and correct.

Executed this 19th day of November, 2014, in Princeton, NJ.

Arvind. N.

Arvind Narayanan

Att. A

Arvind Narayanan

[redacted]

http://randomwalker.info/

Assistant Professor, Computer Science & CITP, Princeton University.
Affiliate Scholar, Center for Internet and Society, Stanford Law School.

1. *Education and work history*

- Assistant Professor, Computer Science & CITP, Princeton University (Sep 2012-present).
- Postdoctoral fellow, Computer Science Department, Stanford University (Jun 2009-Aug 2012).
- Ph.D., Computer Science, The University of Texas at Austin, 2009. Advisor: Vitaly Shmatikov.
- Summer internship. SRI International, Palo Alto CA 2007.
- Summer internship. Microsoft Research, Mountain View CA 2006.
- M.Tech, Computer Science, Indian Institute of Technology, Madras, India. Dual degree, 1999-2004.
- B. Tech, Computer Science, Indian Institute of Technology, Madras, India. Dual degree, 1999-2004.

2. *Research*

My research interests are information privacy and security with a strong side-interest in technology policy. My current threads of research are web privacy and transparency, Bitcoin and cryptocurrencies, and big data and privacy. In the past I have worked on demonstrating flaws in privacy and anonymization techniques as well as designing and implementing privacy-enhancing systems.

3. *Students*

- Christian G. Eubank. MSE, 2012 – 2014.
- Steven Goldfeder. Ph.D. track, 2013 –
- Steven Englehardt. Ph.D. track, 2013 –
- Peter Zimmerman. MSE track, 2013 –

4. *Publications*

Thesis

- Arvind Narayanan. *Data Privacy: The Non-Interactive Setting*. University of Texas at Austin Dissertation Series. Proquest, UMI Dissertation Publishing, 2011.

Book chapter

- Arvind Narayanan, Vitaly Shmatikov. *Uncircumventable Enforcement of Privacy Policies via Cryptographic Obfuscation*. In "Digital Privacy: Theory, Technologies and Practices". Editors: A. Acquisti, S. Di Vimercati, S. Gritzalis, and C. Lambrinoudakis. Auerbach Publications 2007.

Journals

- Arvind Narayanan, Shannon Vallor.
  Why software engineering courses should include ethics coverage.
  Communications of the ACM, 2014.
- Yaniv Erlich, Arvind Narayanan.
  Routes for breaching and protecting genetic privacy.
  Nature Reviews Genetics, 2014.
- Jonathan Mayer, Arvind Narayanan.
  Privacy Substitutes.
  66 Stanford Law Review Online 89. 2013.
- Solon Barocas, Seda Guerses, Arvind Narayanan, Vincent Toubiana.
  Unlikely Outcomes? A Distributed Discussion on the Prospects and Promise of Decentralized Personal Data Architectures.
  Institute of Network Cultures Reader series 2013.
- Arvind Narayanan.
  What Happened to the Crypto Dream?
  IEEE Security and Privacy Magazine 2013.
- Arvind Narayanan, Kannan Srinathan, C. Pandu Rangan.
  Perfectly Reliable Message Transmission.
  Information Processing Letters 100:1, pages 23–28, 2006.

Proceedings of conferences

- Gunes Acar, Christian Eubank, Steven Englehardt, Marc Juarez, Arvind Narayanan, Claudia Diaz.
  The Web never forgets: Persistent tracking mechanisms in the wild.
  ACM Conference on Computer and Communications Security (CCS) 2014.
- Jeremy Clark, Joseph Bonneau, Edward W. Felten, Joshua A. Kroll, Andrew Miller, Arvind Narayanan.
  On Decentralizing Prediction Markets and Order Books.
  Workshop on the Economics of Information Security (WEIS) 2014.
- Joseph Bonneau, Arvind Narayanan, Andrew Miller, Jeremy Clark, Joshua A. Kroll, Edward W. Felten.
  Mixcoin: Anonymity for Bitcoin with accountable mixes.
  Financial Cryptography 2014.
- Arvind Narayanan.
  Privacy technologies: An annotated syllabus.
  HotPETS 2013.

- Christian Eubank, Marcela Melara, Diego Perez-Botero, Arvind Narayanan.
  Shining the Floodlights on Mobile Web Tracking — A Privacy Survey.
  Web 2.0 Security & Privacy (W2SP) 2013.
- Suman Jana, Arvind Narayanan, Vitaly Shmatikov.
  A Scanner Darkly: Protecting User Privacy from Perceptual Applications.
  In IEEE Security and Privacy 2013. **Winner of the 2014 Privacy Enhancing Technologies Award.**
- Claude Castelluccia and Arvind Narayanan.
  Privacy Considerations of Online Behavioural Tracking.
  European Network and Information Security Agency (ENISA) expert report, 2012.
- Arvind Narayanan, Vincent Toubiana, Solon Barocas, Helen Nissenbaum, Dan Boneh.
  A Critical Look at Decentralized Personal Data Architectures.
  Data Usage Management on the Web (DUMW) workshop 2012.
- Arvind Narayanan, Hristo Paskov, Neil Gong, John Bethencourt, Richard Shin, Emil Stefanov, Dawn Song.
  On the Feasibility of Internet-scale Author Identification.
  IEEE Security & Privacy 2012.
- Arvind Narayanan, Elaine Shi, Benjamin I. P. Rubinstein.
  Link Prediction by De-anonymization: How We Won the Kaggle Social Network Challenge.
  International Joint Conference on Neural Networks (IJCNN) 2011.
- Joseph A. Calandrino, Arvind Narayanan, Ann Kilzer, Edward W. Felten, Vitaly Shmatikov.
  You Might Also Like: Privacy Risks of Collaborative Filtering.
  IEEE Security & Privacy 2011.
- Arvind Narayanan, Narendran Thiagarajan, Mugdha Lakhani, Mike Hamburg, Dan Boneh.
  Location Privacy via Private Proximity Testing.
  Network and Distributed Systems Security Symposium (NDSS) 2011. **Distinguished paper award.**
- Arvind Narayanan, Vitaly Shmatikov.
  Myths and Fallacies of Personally Identifiable Information.
  Communications of the ACM, June 2010.
- Arvind Narayanan, Vincent Toubiana, Dan Boneh, Helen Nissenbaum and Solon Barocas.
  Adnostic: Privacy Preserving Targeted Advertising.
  Network and Distributed Systems Security Symposium (NDSS) 2010.
- Arvind Narayanan, Vitaly Shmatikov.
  De-anonymizing Social Networks.
  IEEE Security & Privacy 2009.
- Arvind Narayanan, Vitaly Shmatikov.
  Robust De-anonymization of Large Sparse Datasets.
  IEEE Security & Privacy 2008. **Winner of the 2008 Privacy Enhancing Technologies Award**.
- Arvind Narayanan, Ilya Mironov.
  Domain Extensions for Random Oracles: Beyond the Birthday-paradox Bound.
  Proceedings of the ECRYPT Hash Workshop 2007.

- Arvind Narayanan, Vitaly Shmatikov.
  Obfuscated Databases and Group Privacy.
  ACM Conference on Computer and Communications Security (CCS) 2005.
- Arvind Narayanan, Vitaly Shmatikov.
  Fast Dictionary Attacks on Passwords Using Time-Space Tradeoff.
  ACM Conference on Computer and Communications Security (CCS) 2005.
- Kannan Srinathan, Arvind Narayanan, C. Pandu Rangan.
  Optimal Perfectly Secure Message Transmission.
  Advances in Cryptology – CRYPTO 2004.
- Vinod Vaikuntanathan, Arvind Narayanan, Kannan Srinathan, C. Pandu Rangan, Kwangjo Kim.
  On the power of Computational Secret Sharing.
  Indocrypt 2003.
- Arvind Narayanan, C. Pandu Rangan, Kwangjo Kim.
  Practical Pay TV Schemes.
  Australasian Conference on Information Security and Privacy (ACISP) 2003.

Position papers and expert commentary

- Arvind Narayanan, Edward W. Felten, Joanna Huey.
  A precautionary approach to big data privacy. 2014.
- Arvind Narayanan, Edward W. Felten.
  No silver bullet: De-identification still doesn't work. 2014.
- Claude Castellucia, Arvind Narayanan.
  Privacy considerations of online behavioural tracking.
  European Network and Information Security Agency (ENISA) special report 2012.
- Jonathan Mayer, Arvind Narayanan, Sid Stamm.
  Do Not Track: A Universal Third-Party Web Tracking Opt Out.
  IETF Internet Draft. 2011.

5. *Selected press*

- *Browser 'Fingerprints' Help Track Users*.
  BBC News, Jul 22, 2014
- *Meet the Online Tracking Device That Is Virtually Impossible to Block*.
  ProPublica, Jul 21, 2014
- *Browser Cookies: How They Could Be Undermining Your Privacy*.
  CBC News, Apr 08, 2014
- *Those Prying Eyes*.
  Princeton Alumni Weekly, Jan 08, 2014
- *Can I Get Some Privacy?*
  Stanford Magazine, Mar 11, 2013
- *Arvind Narayanan Isn't Anonymous, and Neither Are You*.
  WIRED, Jun 18, 2012

- *The End of Anonymous Commenting*.
  On the Media (NPR), Mar 02, 2012.
- *The Privacy Challenge in Online Prize Contests*.
  NYTimes Bits blog, May 21, 2011
- *Do Not Track Me Online, Please*.
  CBC News, Mar 22, 2011
- *How Privacy Vanishes Online, a Bit at a Time*.
  New York Times, Mar 17, 2010
- *Netflix Cancels Contest Plans and Settles Suit*.
  NYT bits blog, Mar 12, 2010
- *Social Sites Dent Privacy Efforts*.
  BBC News, Mar 27, 2009

6. *Teaching*

- Fall 2014-15.
  COS 597E. Advanced Topics in Computer Science: Bitcoin and cryptocurrency technologies.
- Spring 2014.
  COS 598B. Advanced Topics in Computer Science: Privacy Technologies.
- Fall 2013-14.
  COS 432: Information Security.
- Spring 2013.
  COS 226: Data Structures and Algorithms. Co-taught with Dr. Josh Hug.
- Fall 2012-13
  COS 597D. Advanced Topics in Computer Science: Privacy Technologies.
  FRS 125. Freshman Seminar: Friending, Following, Finding. Co-taught with Prof. Andrea LaPaugh.

7. *Research grants*

- NSF Award #1421689. *Addressing the challenges of cryptocurrencies: Security, anonymity, stability*. 2014-2017.

8. *Program Committees*

- IEEE Security & Privacy (Oakland) 2015.
- Privacy Enhancing Technologies Symposium (PETS) 2014.
- Workshop on the Economics of Information Security (WEIS) 2014.
- Financial Cryptography 2014.
- Hot Topics in Privacy Enhancing Technologies (HotPETs) 2013.
- World Wide Web Conference (Security, Privacy, Trust, and Abuse) 2013.
- IEEE Security & Privacy (Oakland) 2013.
- W3C "Do Not Track and Beyond" Workshop 2012.
- IEEE Security & Privacy (Oakland) 2012.

- Security and Social Networking (SESOC) workshop 2012.
- Privacy Enhancing Technologies Symposium (PETS) 2012.
- Workshop on Artificial Intelligence and Security (AISEC) 2011.
- ACM Conference on Computer and Communications Security (CCS) 2011.
- USENIX Workshop on Health Security and Privacy (HealthSec) 2011.
- Privacy Enhancing Technologies Symposium (PETS) 2011.

9. Conferences organized

- Web Transparency and Accountability Conference. Princeton University, March 2014.
  Co-organizer: Solon Barocas.
- Bitcoin and Cryptocurrency Research Conference. Princeton University, March 2014.
  Co-organizer: Edward Felten.
- "Accelerate Genomic Research with Privacy Protections" workshop. Banbury Center, Dec 2013.
  Co-organizers: Yaniv Erlich, Bob Kain.

10. Advisory Boards and Award Committees

- Council for Big Data, Ethics and Society.
  (Advisory council for NSF Big Data projects, funded by an NSF EAGER.)
- Privacy Enhancing Technologies Award Committee, 2014.
- Stanford Cookie Clearinghouse Advisory Board.
- Heritage Health Prize Advisory Board.
  ($3MM machine-learning prize for improving healthcare predictions.)
- NIH Distinguished Advisory Board for Silent Spring Institute–Harvard–Brown grant (R01 ES021726):
  "Data Sharing and Privacy Protection in Digital-Age Environmental Health Studies."

11. Awards

- 2014 Privacy Enhancing Technologies Award.
- 2008 Privacy Enhancing Technologies Award.
- MCD Fellowship at UT Austin, 2004.
- Silver medal at the International Mathematical Olympiad (IMO) 1999.