

# Jeremy Clark

**NSERC / Raymond Chabot Grant Thornton / Catalaxy  
Industrial Research Chair in Blockchain Technologies**

**Associate Professor**

Concordia Institute for Information Systems Engineering (CIISE)  
Concordia University

[j.clark@concordia.ca](mailto:j.clark@concordia.ca)

+1 (514) 848-2424 x5381

<https://users.encs.concordia.ca/~clark/>

# Employment

## Academic positions

- Associate Professor, Concordia Institute for Information Systems Engineering (CIISE), Concordia University. 1 Jun 2018 – present.
- Assistant Professor, Concordia Institute for Information Systems Engineering (CIISE), Concordia University. 1 Aug 2013 – 31 May 2018.

## Consulting

- Subject Matter Expert on Internet Voting Security (Consultant), City of Toronto, RFP 3405-13-3197. 28 Nov 2014 – 20 Sep 2015.

## Designations

- Professional Engineer. Professional Engineers of Ontario (PEO). 17 Dec 2018 — present.

# Academic Background

## Degrees

- Ph.D., Computer Science, University of Waterloo. Graduated: Jun 2011.
- M.A.Sc., Electrical Engineering, University of Ottawa. Graduated: Oct 2007.
- B.E.Sc., Computer Engineering, University of Western Ontario. Graduated: Apr 2004.

## Post-Doctorate

- Post Doctoral Fellow, School of Computer Science, Carleton University. 1 Jul 2011 – 1 Aug 2013.

## Awards & honours

- Excellence in Teaching Award, Junior Faculty Member. Concordia University, 2017.
- Postdoctoral Fellowships Program (PDF). Natural Sciences and Engineering Research Council of Canada (NSERC). 2011–2013
- Alumni Gold Medal (Top Graduating PhD Student). University of Waterloo. 2011
- Alexander Graham Bell Canada Graduate Scholarship (CGS). Natural Sciences and Engineering Research Council of Canada (NSERC). 2008–2011
- David R. Cheriton Graduate Scholarship. University of Waterloo. 2008–2011
- President's Graduate Scholarship. University of Waterloo. 2008-2011

- Ontario Graduate Scholarship (OGS). Declined. 2008
- Entrance Scholarship. University of Waterloo. 2007
- Grand Prize: Best Election System. “The Punchscan Voting System.” University Voting Systems Competition (VoComp). 2007
- Best Project in Department. “Real-Time Encryption using Cellular Automata.” University of Western Ontario Design Day Competition. 2004
- Honorable Mention. “Cellular Automata.” Ontario Engineering Competition. 2004

## Publications

### Summary

Type	Lifetime	While employed
Journals	6	4
Refereed Conference	37	17
Book Chapters	5	2

### Statistics

Citations, h-index and i10 index is based on Google Scholar. Google Scholar is automated and not necessarily fully accurate; however it gives representative results. Our field does not have organizations providing rigorous citation counting or metrics (e.g., impact factor).

Top-4 publications is the number of publications in (1) IEEE Symposium on Security and Privacy, (2) USENIX Security Symposium, (3) ACM Conference on Computer and Communications Security (CSS), and (4) Network and Distributed System Security (NDSS) Symposium. These are considered the best four venues for security research and are widely monitored. Concordia ranks third in Canada<sup>1</sup> by this metric (behind Waterloo, Carleton) and 121 worldwide.

Updated Fall 2019	Lifetime
Citations	3000
h-index	23
Top-4 publications	4

<sup>1</sup> <http://s3.eurecom.fr/~balzarot/notes/top4/index.html> [as of Fall 2018]

## Notes on the nature of the field

Unlike other fields, the most active venues for security research are **refereed conferences**, as opposed to refereed journals. Conferences are highly competitive. Top-4 conferences (defined above) like IEEE Symposium on Security & Privacy had an acceptance rate of 12% and 14% the two years I published there.

Given the competitive nature of the top tier conferences, second tier venues are often called **workshops**. Unlike in other fields, these are also rigorously peer reviewed venues for completed technical papers and are typically competitive. In our field, the term workshop denotes a venue that is specific to a narrow domain, as opposed to conferences and symposiums, which tend to accept a wide range of papers.

As one illustrative example, our well-publicized work on the Scantegrity voting system (see media below) appeared initially at a **workshop** (USENIX EVT/WOTE which is co-located with USENIX Security; a top-4). The following year, we published a fuller version of the paper in a **journal** (IEEE Transactions on Information Forensics and Security). The workshop version has been cited 125 times, while the journal version has been cited only 50 times.

## Refereed conference publications

### Abbreviations

*AR* = Acceptance rate

*LNCS XXXX* = Volume XXXX of Springer's Lecture Notes in Computer Science

C37	M Rahimian*, S Eskandari*, J. Clark. Resolving the Multiple Withdrawal Attack in ERC20 Tokens <i>2019 IEEE Workshop on Security &amp; Blockchains (IEEE S&amp;B)</i> .
C36	E. Mangipudi, K. Rao, J. Clark, A. Kate. Automated Penalization of Data Leakage using Crypto-augmented Smart Contracts. <i>2019 IEEE Workshop on Security &amp; Blockchains (IEEE S&amp;B)</i> .
C35	S. Eskandari*, M. Moosavi*, J. Clark. Transparent Dishonesty: front-running attacks on Blockchain. <i>Trusted Smart Contracts, Proceedings of Financial Cryptography and Data Security: FC Workshops, 2019</i> . LNCS 11599.
C34	M. Elsheikh, A. Youssef, J. Clark. Deploying PayWord on Ethereum. <i>Trusted Smart Contracts, Proceedings of Financial Cryptography and Data Security: FC Workshops, 2019</i> . LNCS 11599.
C33	V. Zhao, J. Choi, D. Demirag*, M. Mannan, K. Butler, E. Ayday, J. Clark. One-time programs made practical. <i>Proceedings of Financial Cryptography and Data Security (FC), 2019</i> . LNCS 11598.
C32	S. Eskandari*, A. Leoutsarakosg, T. Mursch, J. Clark. A first look a browser-based cryptojacking. <i>2018 IEEE Workshop on Security &amp; Blockchains (IEEE S&amp;B)</i> .
C31	C. Okoye*, J. Clark. Toward Cryptocurrency Lending. <i>Trusted Smart Contracts, Proceedings of Financial Cryptography and Data Security: FC Workshops, 2018</i> . LNCS 10958.

C30	M. Moosavi*, J. Clark. Ghazal: toward truly authoritative web certificates using Ethereum. <i>Trusted Smart Contracts, Proceedings of Financial Cryptography and Data Security: FC Workshops</i> , 2018. LNCS 10958.
C29	S. Eskandari*, J. Clark, M. Adham, V. Sundaresan. On the feasibility of decentralized derivatives markets. <i>Trusted Smart Contracts, Proceedings of Financial Cryptography and Data Security: FC Workshops</i> , 2017. LNCS 10323.
C28	N. Yang* and J. Clark. Practical Governmental Voting with Unconditional Integrity and Privacy. <i>VOTING, Proceedings of Financial Cryptography and Data Security: FC Workshops</i> , 2017. LNCS 10323.
C27	S. Eskandari*, J. Clark, A. Hamou-Lhadj. "Buy your Coffee with Bitcoin: Real-World Deployment of a Bitcoin Point of Sale Terminal." <i>Proceedings of the 13th IEEE International Conference on Advanced and Trusted Computing (Bitcoin Track)</i> , 2016.
C26	G. Dagher*, B. Bünz, J. Bonneau, J. Clark, D. Boneh. Provisions: Privacy-preserving proofs of solvency for Bitcoin exchanges. <i>Proceedings of the 22nd ACM Conference on Computer and Communications Security (CCS)</i> , 2015. AR: 19%.
C25	J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. Kroll, E. W. Felten. Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. <i>Proceedings of the 34th IEEE Symposium on Security and Privacy (IEEE SSP)</i> , 2015. AR: 14%. <u>Highest cited security paper from 2015</u>
C24	S. Eskandari*, D. Barrera, E. Stobert, J. Clark. A First Look at the Usability of Bitcoin Key Management. <i>Proceedings of the NDSS Workshop on Usable Security (USEC)</i> , 2015.
C23	D. Barrera, D. McCarney, J. Clark, P. C. van Oorschot. Baton: Certificate Agility for Android's Decentralized Signing Infrastructure. <i>Proceedings of the 7th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)</i> , 2014. AR: 26%.
C22	J. Bonneau, J. Clark, E. W. Felten, J. A. Kroll, A. Miller, A. Narayanan. On Decentralizing Prediction Markets and Order Books. <i>Proceedings of the 13th Annual Workshop on the Economic of Information Security (WEIS)</i> , 2014.
C21	M. Backes, J. Clark, P. Druschel, A. Kate, M. Simeonovski. Back-Ref: Accountability in Anonymous Communication Networks. <i>Proceedings of the 12th International Conference on Applied Cryptography and Network Security (ACNS)</i> , 2014. LNCS 8479. AR: 22%.
C20	J. Bonneau, A. Narayanan, A. Miller, J. Clark, J. A. Kroll, E. W. Felten. Mixcoin: Anonymity for Bitcoin with Accountable Mixes. <i>Proceedings of the 18th Conference on Financial Cryptography and Data Security (FC)</i> , 2014. LNCS 8437. AR: 22%
C19	F. Zagorski, R. Carback, D. Chaum, J. Clark, A. Essex, P. Vora. Remotegrity: Design and Use of an End-to-End Verifiable Remote Voting System. <i>Proceedings of the 11th International Conference on Applied Cryptography and Network Security (ACNS)</i> , 2013. AR: 23%.
C18	J. Clark and P. C. van Oorschot. SSL and HTTPS: Revisiting past challenges and evaluating certificate trust model enhancements. <i>Proceedings of the 34th IEEE Symposium on Security and Privacy (IEEE SSP)</i> , 2013. AR: 12%.

C17	D. McCarney, D. Barrera, J. Clark, S. Chiasson, and P. C. van Oorschot. Tapas: Design, implementation, and usability evaluation of a password manager. <i>Proceedings of the 2012 Annual Computer Security Applications Conference (ACSAC)</i> , 2012. AR: 19%.
C16	D. Barrera, J. Clark, D. McCarney, P. C. van Oorschot. Understanding and improving app installation security mechanisms through empirical analysis of Android. <i>Proceedings of the 2nd Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM)</i> , 2012. AR: 37%.
C15	A. Essex, J. Clark, and U. Hengartner. Cobra: Toward concurrent ballot authorization for internet voting. <i>Proceedings of the 2012 USENIX Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE)</i> , 2012. AR: 35%.
C14	J. Clark and A. Essex. CommitCoin: Carbon dating commitments with Bit-coin. <i>Proceedings of the 16th Conference on Financial Cryptography and Data Security (FC)</i> , 2012. LNCS 7397. AR: 33%.
C13	J. Clark and U. Hengartner. Selections: an internet voting system with over-the-shoulder coercion-resistance. <i>Proceedings of the 15th Conference on Financial Cryptography and Data Security (FC)</i> , 2011. LNCS 7035. AR: 35%.
C12	R. Carback, D. Chaum, J. Clark, J. Conway, A. Essex, P. S. Herrnson, T. Mayberry, S. Popoveniuc, R. L. Rivest, E. Shen, A. T. Sherman, P. L. Vora. Scantegrity II Municipal Election at Takoma Park: The First E2E Binding Governmental Election with Ballot Privacy. <i>Proceedings of the 19th USENIX Security Symposium</i> , 2010. AR: 15%.
C11	A. Essex, J. Clark, U. Hengartner, C. Adams. Eperio: Mitigating Technical Complexity in Cryptographic Election Verification. <i>Proceedings of the 2010 USENIX Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE)</i> , 2010. AR: 39%.
C10	J. Clark, U. Hengartner. On the Use of Financial Data as a Random Beacon. <i>Proceedings of the 2010 USENIX Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE)</i> , 2010. AR: 39%.
C09	A. T. Sherman, R. Carback, D. Chaum, J. Clark, A. Essex, P. S. Herrnson, T. Mayberry, S. Popoveniuc, R. L. Rivest, E. Shen, B. Sinha, P. L. Vora. Scantegrity Mock Election at Takoma Park. <i>Proceedings of the 4th International Conference on Electronic Voting (EVOTE)</i> , 2010.
C08	J. Clark, U. Hengartner, K. Larson. Not-So Hidden Information: Optimal Contracts for Undue Influence in E2E Voting Systems. <i>Proceedings of the Second IAVoSS International Conference on E-voting and Identity (Vote-ID)</i> , 2009, LNCS 5767.
C07	A. Essex, J. Clark, U. Hengartner, C. Adams. How to Print a Secret. <i>Proceedings of the 4th USENIX Workshop on Hot Topics in Security (HotSec)</i> , 2009. AR: 28%.
C06	D. Chaum, R. Carback, J. Clark, A. Essex, S. Popoveniuc, R. L. Rivest, P. Y. A. Ryan, E. Shen, A. T. Sherman. Scantegrity II: End-to-end verifiability for optical scan election systems using invisible ink confirmation codes. <i>Proceedings of the 2008 USENIX Electronic Voting Technology Workshop (EVT)</i> , 2008.
C05	J. Clark, U. Hengartner. Panic passwords: Authenticating under duress. <i>Proceedings of the 3rd USENIX Workshop on Hot Topics in Security (HotSec)</i> , 2008. AR: 32%.

C04	A. Essex, J. Clark, C. Adams. Aperio: High integrity elections for developing countries. <i>Proceedings of the IAVoSS Workshop on Trustworthy Elections (WOTE)</i> , 2008.
C03	J. Clark, P.C. van Oorschot, C. Adams. Usability of anonymous web browsing: An examination of Tor interfaces and deployability. <i>Proceedings of the Third Symposium On Usable Privacy and Security (SOUPS)</i> . ACM International Conference Proceedings Series, vol 229, 2007, pp. 41–51. AR: 31%.
C02	J. Clark, A. Essex, C. Adams. On the security of ballot receipts in E2E voting systems. <i>Proceedings of the IAVoSS Workshop on Trustworthy Elections (WOTE)</i> , 2007.
C01	A. Essex, J. Clark, R. T. Carback III, S. Popoveniuc. Punchscan in practice: An E2E election case study. <i>Proceedings of the IAVoSS Workshop on Trustworthy Elections (WOTE)</i> , 2007.

### Articles in journals & periodicals

J07	S. Ruoti, B. Kaiser, A. Yerukhimovich, J. Clark, R. Cunningham. Blockchain Technology: What is it good for? <i>Communications of the ACM</i> . 63(1):46-53. 2017. Invited.
J06	G. Dagher*, B. Fung, N. Mohammad, J. Clark. SecDM: Privacy-preserving Data Outsourcing Framework with Differential Privacy. <i>Knowledge and Information Systems</i> . Accepted: 2019
J05	A. Narayanan, J. Clark. Bitcoin's Academic Pedigree. <i>Communications of the ACM</i> . 60(12):36-45. 2017. Invited.
J04	E. Moher, J. Clark, A. Essex. Diffusion of voter responsibility: potential failings in E2E receipt checking. <i>USENIX Journal of Election Technology and Systems</i> . 3(1):1-17. 2014.
J03	J. Clark. Enhancing Anonymity: Cryptographic and statistical approaches for shredding our digital dossiers. <i>ACM Computing Reviews</i> . 2014. Invited.
J02	D. Chaum, R. Carback, J. Clark, A. Essex, S. Popoveniuc, R. L. Rivest, P. Y. A. Ryan, E. Shen, A. T. Sherman, P. L. Vora. (2009) Scantegrity II: End-to-End Verifiability by Voters of Optical Scan Elections Through Confirmation Codes. <i>IEEE Transactions on Information Forensics and Security</i> , 4(4):611-627.
J01	D. Chaum, A. Essex, R. T. Carback III, J. Clark, S. Popoveniuc and A. T. Sherman, P. Vora. Scantegrity: end-to-end voter verifiable optical-scan voting. <i>IEEE Security &amp; Privacy</i> , vol. 6, no. 3, pp. 40–46, May/June 2008.

### Under review/revision (selected)

R05	J. Clark, P. Van Oorschot, S. Ruoti, K. Seamons, D. Zappala. SoK: Securing Email. Last submitted to: <i>2020 IEEE Euro Symposium on Security and Privacy</i> .
R03	Y. Nasser, C. Okoye*, J. Clark, P.Y.A. Ryan. Blockchains and voting: somewhere between hype and a panacea. Last submitted to: <i>IEEE Internet Computing</i> .

R02	G. Dagher*, J. Clark, B. Fung. A Distributed and Publicly Verifiable Protocol for Set-Valued Data Release with Differential Privacy. Last submitted to: <i>Springer Journal of Information Security</i> .
-----	---

## Book chapters

B05	J. Clark. The Long Road to Bitcoin. Preface to: "Bitcoin and Cryptocurrency Technologies." <i>Princeton University Press</i> , 2016.
B04	R. Carback, D. Chaum, J. Clark, J. Conway, A. Essex, P. S. Herrnson, T. Mayberry, S. Popoveniuc, R. L. Rivest, E. Shen, A. T. Sherman, P. L. Vora. The Scantegrity Voting System and its Use in the Takoma Park Elections. Chapter 10 in: "Real-World Electronic Voting: Design, Analysis and Deployment." <i>CRC Press</i> , 2016.
B03	S. Popoveniuc, J. Clark, R. Carback, A. Essex, D. Chaum. Securing Optical-Scan Voting. Chapter in: "Toward Trustworthy Elections: New Directions in Electronic Voting." State of the Art Survey Series, <i>Springer</i> , 357–369. 2010.
B02	A. Essex, J. Clark, C. Adams. Aperio: High Integrity Elections for Developing Countries. Chapter in: "Toward Trustworthy Elections: New Directions in Electronic Voting." State of the Art Survey Series, <i>Springer</i> , 388–401. 2010.
B01	J. Clark, P. Gauvin, C. Adams. Exit Node Repudiation for Anonymity Networks. Chapter 22 in: "Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society." <i>Oxford University Press</i> . 399-415, 2009.

## Editorial activities

E02	A. Zohar, I. Eyal, V. Teague, J. Clark, A. Bracciali, F. Pintore, M. Sala (Editors). "Financial Cryptography and Data Security: FC Workshops 2017." Lecture Notes in Computer Science (LNCS) 10958. <i>Springer</i> , 2019.
E01	J. Clark, S. Meiklejohn, P.Y.A.Ryan, D. Wallach, M. Brenner, K. Rohloff (Editors). "Financial Cryptography and Data Security: FC Workshops 2016." Lecture Notes in Computer Science (LNCS) 9604. <i>Springer</i> , 2016.

## Funding

Year	Program	Agency	Amount	PI	Co-Applicants
2019	Industrial Research Chair	Natural Sciences and Engineering Research Council of Canada (NSERC)	\$1,380,000 over 5 years	Y	



Year	Program	Agency	Amount	PI	Co-Applicants
2017	Education and Good Governance Fund (EGGF)	Autorité des marchés financiers (AMF)	\$100K/year for 2 years	Y	Emilio Boulianne (JMBS)  Share: 50%
2016	Seed Grant	Centre for the Study of Democratic Citizenship (CDSC)	\$6831 once	N	Fenwick Mckelvey (Comm)  Share: 50%
2015	Contributions Program	Office of the Privacy Commissioner of Canada (OPC)	\$50K/year for 1 year	Y	Mohammad Mannan (CIISE)  Share: 50%
2015	Programme Établissement de nouveaux chercheurs universitaires	Fonds de recherche du Québec - Nature et technologies (FRQNT)	\$19K/year for 2 years	Y	
2015	Aid to Research Related Events, Exhibition, Publication and Dissemination Activities (ARRE) Program	Concordia University	\$5K once	Y	
2015	Individual Seed Program	Concordia University	\$7K once	Y	
2014	Discovery Grant (DG)	Natural Sciences and Engineering Research Council of Canada (NSERC)	\$24K/year for 5 years	Y	
2013	Start-Up Grant	Concordia University	\$50K once	Y	

## Research Centres and Network Membership

- Smart Cybersecurity Network (SERENE-RISC). Knowledge Mobilization Network, Networks of Centres of Excellence of Canada (NCE).
- Centre for the Study of Democratic Citizenship (CSDC).

## Evidence of Impact

### Invited Talks and Seminars (Selected)

- Elections Quebec. "Internet Voting," Citizen Jury. Nov 2, 2019.
- Blockchain at McGill. "Introduction to Blockchain for Non-Profits," Social Innovation: Int'l Development and Blockchain. 29 Mar 2019.

- Canada Mortgage and Housing Corporation (CMHC). "Blockchain Technologies: Landscape and Future Directions." 26 Feb 2019.
- CFA Montreal FinTech Rendez-vous. "Blockchain Technologies: Landscape and Future Directions." 7 Feb 2019.
- Loto-Quebec. "Blockchain lunch and learn." 22 Jan 2019.
- RISQ Colloquium. "Blockchain Technologies: Landscape and Future Directions." 29 Nov 2018.
- TriPAC Pension Advisory Committees. "Blockchain Technologies: Landscape and Future Directions." Treasury Board Secretariat. 21 Nov 2018.
- Defending Democracy: Confronting Cyber-Threats At Home And Abroad. "Liquid Democracy and Blockchains." October 26, 2018.
- Blockchain and National Security. "Blockchain Technology: National Security Use-Cases." Public Safety Canada, October 18, 2018.
- Montreal Police Pension Fund (ABRPPVM). "Blockchain Technology: Landscape & Future Directions." Invited speaker, September 22, 2018.
- BMO 13th Annual Real Estate Conference. "Blockchain Applications & Real-Estate." Panel, BMO Capital Markets. September 20, 2018.
- Blockchain Technology Symposium (BTS). "Blockchain Nuances: Lessons from Fintech use-cases." Invited talk, Fields Institute. September 18, 2018.
- GoSec. "Blockchain Technologies: Landscape and Future Directions." August 29, 2018.
- StartupFest. "Democracy Enhancing Technologies." CryptoFest. July 10, 2018.
- FintechQC. "Blockchain Nuances" Keynote, Desjardins Labs & UQAR, June 20, 2018.
- The Walrus LIVE. "The Future of Money" Panel Discussion with David Tax (TD) and Susan Prince (CBC). June 14, 2018.
- BMO ThinkSeries. "Blockchain Technologies: Landscape and Future Directions." June 12, 2018.
- Autorite des marches financiers (AMF). "Crypto Primer II." June 11, 2018.
- Canada Pension Plan Investment Board (CPPIB). "Blockchain Technologies." June 1, 2018.
- Security Revolution. "Blockchain Primer." SERENE-RISC, May 31, 2018.
- "Blockchain Technologies: Landscape and Future Directions." True North Science Bootcamp. May 25, 2018.
- Anticipating Future Trends and Managing Risks Program. "Blockchain Technologies: Landscape and Future Directions," HEC Paris and Concordia. May 10, 2018.
- Autorite des marches financiers (AMF). "Crypto Primer I." May 1, 2018.
- GC Blockchain Day. "Ledgers Past, Present and Future." Treasury Board Secretariat of Canada. April 23, 2018.
- "Workplace 2020." Management Consulting Club, Concordia. Panel. April 8, 2018.
- "Blockchain Technologies: Landscape and Future Directions." Canadian National Railway (CN). February 8, 2018.

- Kenneth Woods Portfolio Management Program. "Cryptocurrencies: An Investable Asset?" John Molson School of Business. January 23, 2018.
- "Provisions: Privacy-Preserving Proofs of Solvency." Newcastle University. December 7, 2017.
- "Democracy Enhancing Technologies: From Theory to Practice." CDSC Speaker Series. McGill, September 15, 2017.
- Hydro-Québec Symposium 3i. "Bitcoin & Blockchains: Landscape and Future Directions." Invited Speaker, Montreal,
- Privacy, Security and Trust (PST). "Bitcoin & Blockchains: Landscape and Future Directions." Keynote, Calgary, Aug 28, 2017.
- Metropolis 2017. "The Bitcoin & Blockchain Technology Landscape." June 28, 2017.
- Blockchain Meetup. "Zero Knowledge." District 3. May 4, 2017.
- Canada Music Week. "Blockchains: Smart Contracts and Media-Driven Crypto Currencies" Panel discussion, April 19, 2017.
- District 3. "The Future of Blockchain." Panel discussion, December 8, 2016.
- Symposium on Foundations & Practice of Security. "The Bitcoin & Blockchain Technology Landscape." Keynote presentation. Université Laval, October 26, 2016.
- P2P Financial Systems Workshop. "Blockchain nuances." Keynote presentation. UCL, September 8, 2016.
- Bank of Canada. "Bitcoin & Blockchains: Part 2." July 14, 2016.
- Anti-phishing working group (APWG) eCrime 2016. "Bitcoin: an impartial assessment of its use and potential for cybercrime." May 31, 2016.
- C.D. Howe. "Blockchain Technologies and the Future of Finance." May 30, 2016.
- ASIMM Colloque RSI. "Bitcoin & Blockchains: Tutorial," May 12, 2016.
- Bank of Canada. "Bitcoin & Blockchains: Landscape and Future Directions," May 11, 2016.
- National Research Council (NRC), "Security Training Course," Mar 22, 2016.
- MIT Bitcoin Expo. "Blockchain-based voting: potential and limitations," MIT, Mar 6, 2016.
- Bitcoin and Cryptocurrency Research Conference. "Altcoins," Center for Information Technology Policy (CITP), Princeton University, March 27, 2014.
- USENIX Summit on Hot Topics in Security (HotSec 2013). "Eroding Trust and the CA Debacle," August 13, 2013.
- CIISE Distinguished Seminar. "How to Carbon Date Digital Information," Concordia University, March 8, 2012.
- MITACS Digital Security Seminar Series. "Panic Passwords and their Applications," Carleton University, January 27, 2011.
- CACR Cryptography Seminar. "The First Governmental Election with a Voter Verifiable Tally: Experiences using Scantegrity II at Takoma Park," University of Waterloo, February 5, 2010.
- CACR Cryptography Seminar. "Selections: An Internet Voting System with Over-the-shoulder Coercion Resistance," University of Waterloo, December 3, 2010

- Information Technology and Innovation Foundation (ITIF) Forum: Future of Voting. “Panel Discussion,” Longworth House Office Building, Washington, D.C. March 6, 2008.
- CACR Cryptography Seminar. “Combating Adverse Selection in Anonymity Networks,” University of Waterloo, October 17, 2007.

## Expert Testimony & Public Interest Consultations

- House of Commons, Standing Committee on Finance. Testimony: Statutory Review of the Proceeds of Crime and Terrorist Financing Act. March 27, 2018.
- Investissement Quebec. Bitcoin & Blockchains: Landscape and Future Directions. January 15, 2018.
- Government of Canada (GC) Digital Target State Architecture and Direction. Blockchain working group. August 2017 — present.
- Karina Gould, Minister of Democratic Institutions (House of Commons, Canada). CDSC roundtable. August 30, 2017.
- Online Voting Roundtable: Electoral Futures in Canada. “Blockchain and Voting: Assessment & Critique.” Invited Speaker, University of Ottawa. September 26, 2016.
- Autorité des marchés financiers (AMF). “Blockchain nuances.” March 29, 2017.
- Royal Canadian Mounted Police (RCMP). Bitcoin brainstorming session (#2). Participant in roundtable. September 28, 2016.
- Royal Canadian Mounted Police (RCMP). Bitcoin brainstorming session. Participant in roundtable. July 5, 2016.
- Formation régionale de la Cour du Québec. “Bitcoin: Introduction & Implications,” May 9, 2015.
- 2013–2014 City of Toronto. Subject Matter Expert on Internet Voting Security and Cryptography (RFP No. 3405-13-3197).
- Senate of Canada, Standing Committee on Banking, Trade and Commerce. Testimony: Study on the use of digital currency. April 3, 2014.
- City of Edmonton: Citizen Jury on Internet Voting. “Security Risks Related to Internet Voting,” Centre for Public Involvement/University of Alberta, November 23–25, 2012.

## Standards Committees

- Technical Committee, “SMC/ISO/TC 307: Blockchain and electronic distributed ledger technologies.” Member of Mirror Committee. *Standards Council of Canada*, Sept 2016—present.

## Press & Media (Selected)

- “Banks Claim They're Building Blockchains. They're Not.” *Investopedia*, July 13, 2018
- “The evolution of cryptojacking.” *CryptoInsider*, March 20, 2018
- “The Ethics Of Cryptojacking: Rampant Malware Or Ad-Free Internet?” *CoinTelegraph*, March 16, 2018.
- “One of the Biggest Coinhive Users Made \$7.69 In 3 Months.” *Motherboard*, March 14, 2018.

- “Attack Or Business Opportunity?: Academics Question Ethics Of Coinhive Cryptojacking.” *CoinTelegraph*, March 10, 2018.
- “How much should I regret not buying Bitcoin?” Gizmodo, January 29, 2018.
- Interview on Bitcoin regulation. *CBC Radio One*, December 5, 2017.
- “How blockchain-based payment is changing the cannabis industry,” *IBM thinkLeaders*, June 21, 2017.
- “Ottawa explores potential of ‘blockchain,’ billed as next-generation Internet tech.” *Toronto Star*, Feb 28, 2017.
- “Block the vote: Could Blockchain Technology Cybersecure Elections?” *Forbes*, Aug 30, 2016.
- “He’s Bitcoin’s Creator, He Says, but Skeptics Pounce on His Claim,” *New York Times*, May 2, 2016.
- “Logged out, but still out there,” *Globe and Mail*, Feb 19, 2016.
- “Princeton University releases first draft of bitcoin textbook,” *CoinDesk*, Feb 10, 2016.
- “The top 10 cryptocurrency research papers of 2015,” *CoinDesk*, Dec 27, 2015.
- “Canada’s Internet Voting Problem,” *SC Magazine*, Feb 2015 issue.
- “Latest Internet voting reports show failures across the board,” *Al Jazeera America*, Feb 8, 2015
- “How Block Chain Technology Could Usher in Digital Democracy,” *CoinDesk*, June 16, 2014.
- “Can Bitcoin Help Predict the Future?,” *CoinDesk*, May 24, 2014.
- “Heartbleed and sentinels of the net,” *Montreal Gazette*, Apr 21, 2014.
- “PROFESSOR: There Is A Big, Gaping Flaw In The New Satoshi Study,” *Business Insider*, Mar 28, 2014.
- “2014 Federal Budget Calls Bitcoin A Terrorist, Crime ‘Risk’ ,” *Huffington Post*, Feb 12, 2014.
- “Bitcoin: How its core technology will change the world,” *New Scientist*, Feb 5, 2014.
- “More than money, bitcoin’s real value lies in its algorithms,” *InfoWorld*, Jan 12, 2014.
- “U. researchers develop Bitcoin prediction market,” *Daily Princetonian*, Jan 5, 2014.
- “This Princeton professor is building a Bitcoin-inspired prediction market,” *The Verge*, Nov 29, 2013
- “Montreal’s Bitcoin Embassy bridges gap between digital currency and real world,” *Montreal Gazette*, Nov 29, 2013.
- “Bitcoin online currency gets new job in web security,” *New Scientist*, Jan 11, 2012.
- “Secure, verifiable voting: Cryptography, invisible ink, and other voting magic,” *Imprint*, Nov 6, 2009.
- “Scantegrity: Voters Test New Transparent Voting System,” *Huffington Post*, Nov 5, 2009.
- “Maryland Voters Test New Cryptographic Voting System,” *Wired News*, Nov 4, 2009.
- “Voters try out new security system,” *UW Daily Bulletin*, Nov 3, 2009.
- “E-voting system lets voters verify their ballots are counted,” *Computerworld*, Nov 3, 2009.

- “First Test for Election Cryptography,” *Technology Review*, Nov 2, 2009.
- “Mock election tests new voting system,” *Gazette.net*, April 15, 2009.
- “Geek the Vote 2012: What Election Tech Will Look like 4 Years From Now,” *Popular Mechanics*, Nov 4, 2008.
- “Canadian voting machine technology enters American political scene,” *CBC.ca*, Oct 28, 2008.
- “New Voter Counter System Uses Encrypted Codes, Invisible Ink,” *Voice of America*, Oct 24, 2008.
- “A Really Secret Ballot,” *The Economist*, Oct 22, 2008.
- “Class voting hacks prompt call for better audits,” *MSNBC*, Oct 20, 2008.
- “Clean Elections,” *Communications of the ACM*, October 2008.
- “Protecting Your Vote With Invisible Ink,” *Discover Magazine*, Oct 2008.
- “Flawless Vote Counts,” *Technology Review*, Sept/Oct 2008.
- “Shift Back to Paper Ballots Sparks Disagreement,” *Morning Edition*, Mar 7, 2008.
- “Down for the Count,” *ACM netWorker*, Mar 2008.
- “The future of voting IT,” *Government Computer News*, Mar 10, 2008.
- “A Damaging Paper Chase In Voting,” *Washington Post*, Sept 8, 2007.
- “Punchscan Wins VoComp 2007,” *As It Happens (CBC)*, August 23, 2007.
- “US/Canada Team Wins Voting Competition,” *Threat Level (Wired)*, July 19, 2007.
- “Electronic Democracy,” *Digital Planet (BBC)*, Jan 29, 2007.
- “Making Every E-vote Count,” *IEEE Spectrum*, Jan 2007.

## Concordia Promotional Activities


- Thinking Out Loud. “Bitcoin & Cryptocurrency,” Podcast, Episode 14. 27 Feb 2018.
- “Back to the future — reclaiming the internet” Distinguished Alumni Speaker Series with Fay Arjomandi. September 22, 2018.
- “This is Concordia. Now. “Bitcoin and cryptocurrency.” Conversation with Alan Shepherd. April 11, 2018.
- “X EXPLAINED: What you need to know about internet cookies.” Concordia Video. March 29, 2018.
- This Is Concordia. Now. “Jeremy Clark talks Bitcoin and cryptocurrency.” Conversation with Sudha Krishnan (CBC Montreal). February 22, 2018.
- Next-Gen. Now. “The Campaign for Concordia.” Promotional video with on-screen interview. November 24, 2017.
- Capstone Magazine. “Cyberattacks: everything you need to know.” Fall 2016.
- Concordia Alumni Association. “Everyone knows your birthday: How secure is your password Hint: not very!” New York City, May 16, 2017.
- Thinking Out Loud. “One Vote,” The Futurecast podcast, Episode 4. April 12, 2017.

- Next-gen. Now. “My Name is Jeremy Clark.” Website feature. March 1, 2017.
- Concordia University Magazine. “Guardians of the IT galaxy.” February 9, 2017.
- Thinking Out Loud. “Connecting your tech future,” conversation with Nora Young (CBC), Concordia University. March 1, 2016.
- Breakfast Talk. “Heartbleed & other CIISE Research,” Concordia University. May 6, 2014.

## Concordia University Magazine

- Winter 2019 - Picture & text, page 55.
- Fall 2018 - Picture & text, page 60.
- Spring 2018 - Picture & text, page 9.
- Spring 2018 - Picture & text, page 54.
- Fall 2017 - Picture & text, page 61-62.
- Winter 2017 - Picture & text, page 24.
- Spring 2016 - Picture & text, page 14-15.
- Winter 2016 - Picture & text, page 15.

## Highly Qualified Personnel

Name	State	Dates	Research Topic	Papers	Co-Supervisor
Mehdi Nejadgholi	MASc	2019/F-	Blockchain technology		
Corentin Thomasset	MASc	2019/F-	Blockchain technology		D. Barrera (Carleton), J. Fernandez (Polytechnique)
Reza Rahimian	PhD	2018/F- Part Time	Blockchain technology	C37	
Mahsa Moosavi	PhD	2018/S-	Blockchain technology	C30, C35	
Elizabeth Stobert	PDF 	2018/W- 2018/F	Usable security	C24	
Didem Demirag	PhD	2018/W-	Blockchain technology	C33	
Shayan Eskandari	PhD	2017/F-	Blockchain technology	C24, C27, C29, C32, C35, C37	

Name	State	Dates	Research Topic	Papers	Co-Supervisor
Chidinma Okoye	MASc 🎓	2016/S - 2017/F	“New applications of blockchain technology to voting and lending”	C31, R03	
Mahsa Moosavi	MASc 🎓	2015/F - 2018/W	“Rethinking Certificate Authorities: Understanding and decentralizing domain validation”	<i>See above</i>	
Michael Colburn	MASc 🎓	2014/F - 2018/S	“Short-Lived Signatures”	<i>See above</i>	
Abhimanyu Khanna	MASc 🎓	2014/F - 2017/S	“Towards Usable and Fine-grained Security for HTTPS with Middleboxes”		M. Mannan (CIISE)
Nan Yang	PhD	2014/S-	Theory of cryptography	C28	C. Crépeau (McGill)
Shayan Eskandari	MASc 🎓	2013/F - 2016/W	“Real world deployability and usability of Bitcoin”	<i>See above</i>	W. Hamou-Lhadj (ECE)
Gaby Dagher	PhD 🎓	2013/F - 2015/F	“Toward secure and privacy-preserving data sharing and integration”	C26, J06	B. Fung (McGill)

My graduated students have gone onto faculty positions (Boise State University) and positions in industry (BitAccess, KMPG, Deloitte).

## Teaching

### Courses Taught

Year/Term	Course	Class Size	Evaluation*
2017/2	INSE 6110: Foundations of Cryptography	79	1.22
2017/2	INSE 6630: Recent Developments in Information Systems Security	35	1.71
2016/4	INSE 6150: Security Evaluation Methodologies	59	1.13
2016/2	INSE 6150: Security Evaluation Methodologies	63	1.09
2016/2	INSE 6110: Foundations of Cryptography	79	1.32
2015/4	COMP 249: Object Oriented Programming II	50	1.44
2015/4	INSE 6150: Security Evaluation Methodologies	86	1.15
2015/2	INSE 6110: Foundations of Cryptography	76	1.24



Year/Term	Course	Class Size	Evaluation*
2014/4	COMP 249: Object Oriented Programming II	93	1.81
2014/4	INSE 6150: Security Evaluation Methodologies	86	1.41
2014/2	INSE 6110: Foundations of Cryptography	69	1.55
2013/4	INSE 6150: Security Evaluation Methodologies	46	1.73
2013/2	INSE 6110: Foundations of Cryptography	21	1.11

- Evaluation is for Question 20: “Overall, the professor is an effective teacher.” Score is from 1.00 (best) to 5.00 (worst).

## Teaching Awards

- Teaching Excellence Award, Junior Faculty, ENCS, Concordia University, 2017.

## External Courses/Lectures (Selected)

- “Improving usability and trust for moving Bitcoin adoption forward,” MAS.S65 - Blockchain Technologies, Massachusetts Institute of Technology (MIT). Guest lecture, 4 Nov 2015.
- “History of cryptocurrencies,” Bitcoin and Cryptocurrency Technologies, Princeton University. Guest lecture, online (Coursera), recorded in Sep 2015.
- COMP 4109: Applied Cryptography, Carleton University. Course, Winter 2013.

## Service to the University

Year	Committee
2018—	Concordia University Faculty Tribunal Pool
2018—	ENCS Blended/Online Pedagogy Committee
2017—	ENCS Elections Committee
2015—	CIISE PR/Website [Co-Chair]
2013—	CIISE Seminar Committee
2014–2016	Concordia University Faculty Tribunal Pool
2014–2015	CIISE Website Committee (merged with PR above)
2013–2015	CIISE PR Committee (merged with Website above)

# Graduate Student Committees

Year	Number					
	MASc Defence	PhD Seminar	PhD Comp.	PhD Proposal	PhD Defence	Chair
2018				1	2	
2017	3	2		1	1	
2016			2	1	1	
2015		1	3			1
2014		1				1
2013	3		1	1		

## External PhD Examiner

- Patrick McCorry, Newcastle University, UK, 2017
- Giulia Alberini, McGill, 2015
- Jérôme Dossogne, Université libre de Bruxelles, Belgium, 2015

# Academic Service

## Program Chairs

Year	Conference
2018	Workshop on Advances in Secure Electronic Voting (VOTING)
2017	The Smart Cybersecurity Network: Spring 2017 Workshop (SERENE-RISC)
2016	3rd Workshop on Bitcoin and Blockchain Research (BITCOIN)

## Editorial Boards

Year	Journal
2013–2016	USENIX Journal of Election Technologies (USENIX JETS)

## Program Committees (Selected)

<b>Year</b>	<b>Conference</b>
2019	Financial Cryptography and Data Security (FC)
2018	APWG Symposium on Electronic Crime Research (eCrime)
2018	Symposium on Usable Privacy & Security (SOUPS)
2018	IEEE Security & Privacy on the Blockchain (IEEE S&B)
2018	Workshop on Bitcoin Research (BITCOIN)
2018	Financial Cryptography and Data Security (FC)
2017	APWG Symposium on Electronic Crime Research (eCrime)
2017	Workshop on Advances in Secure Electronic Voting (VOTING)
2017	Workshop on Bitcoin Research (BITCOIN)
2017	Financial Cryptography and Data Security (FC)
2016	RSA Conference: Cryptographer's Track (CT-RSA)
2016	ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM)
2016	IEEE Advanced and Trusted Computing (Bitcoin track)
2016	Workshop on Advances in Secure Electronic Voting (VOTING)
2016	Workshop on Bitcoin Research (BITCOIN)
2016	Financial Cryptography and Data Security (FC)
2015	International Conference on E-Voting and Identity (VoteID)
2015	Workshop on Bitcoin Research (BITCOIN)
2014	Annual Computer Security Applications Conference (ACSAC)
2014	Conference on Privacy, Security and Trust (PST) – Privacy Theme.
2014	Workshop on Bitcoin Research (BITCOIN)
2013	VoteID (see above)
2012	USENIX Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE) [became USENIX JETS in 2013]
2011	USENIX EVT/WOTE (see above)

### Journal & External Reviews (Most Recent Year / Selected)

<b>Most Recent Year</b>	<b>Journal / Conference</b>
2020	IEEE Security and Privacy Magazine
2017	IEEE Computer
2017	IEEE Transactions on Dependable Secure Computing (TDSC)
2016	ACM Computing Surveys
2016	ACM Conference on Computer and Communications Security (CCS)
2015	IEEE Symposium on Security and Privacy (Oakland)
2015	Networks and Distributed Systems Security Symposium (NDSS)
2014	IEEE Transactions on Information Forensics and Security (TIFS)
2013	ACM Transactions on Information and Systems Security (TISSEC)
2013	USENIX Security Symposium
2013	EUROCRYPT

### Reviews for Funding Agencies (Most Recent Year)

<b>Most Recent Year</b>	<b>Agency</b>
2020	MITACS
2019	Natural Sciences and Engineering Research Council of Canada (NSERC)
2019	FRQ-NT
2019	Alberta Innovates
2017	Office of the Privacy Commissioner (Contributions Program)