July 5, 2023
A more recent version may be available here:
https://www.pulpspy.com/cv/cv.pdf

Jeremy Clark

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

Associate Professor
Concordia Institute for Information Systems Engineering (CIISE)
Concordia University

j.clark@concordia.ca
+1 (514) 848-2424 x5381
https://pulpspy.com

Table of Contents

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.

Professional designations

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

Consulting work

- Subject matter expert on undisclosed digital asset subject, *Susman Godfrey LLP*. November 2022—present.
- Subject matter expert on undisclosed cryptocurrency subject, *Williams & Connolly LLP*. January 2018—March 2018.
- Subject matter expert on internet voting security, *City of Toronto*, RFP 3405-13-3197. November 2014 – September 2015.

Advisory boards

- Canadian Blockchain Supply Chain Association (CBSCA), Advisory Board, 2019—present.
- 3iQ Digital Asset Management, Advisory Board, 2017—2021.

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

Unlike other fields, the most active venues for security research are **refereed conferences**, as opposed to refereed journals. Given the competitive nature of the top tier conferences, mid-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 broad 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 206 times, while the journal version has been cited only 114 times.

Type	Lifetime	While employed
Journals	10	8
Refereed Conferences	48	28
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).

Updated Fall 2022	Lifetime
Citations	7439
h-index	27

Refereed conference publications

Abbreviations

**Supervised student* *AR = Acceptance rate* *Rank = Core2021*

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

C48	A. Arun, J. Bonneau, J. Clark. Short-lived zero-knowledge proofs and signatures. *28th Annual International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT)*, 2022. [Rank: A]
C47	D. Demirag*, M. Namazi, E. Ayday, J. Clark. Privacy-Preserving Link Prediction. *17th DPM International Workshop on Data Privacy Management*, 2022.
C46	D. Chaum, R.T. Carback, J. Clark, C. Liu, M. Nejadgholi*, B. Preneel, A.T. Sherman, M. Yaksetig, F. Zagorski, B. Zhang. VoteXX: A Solution to Improper Influence in Voter-Verifiable Elections. *Seventh International Joint Conference on Electronic Voting (E-VOTE-ID)*, 2022.
C45	M. Salehi*, J. Clark, M. Mannan. Not so immutable: Upgradeability of Smart Contracts on Ethereum. *WTSC*, *Proceedings of Financial Cryptography and Data Security: FC Workshops,* 2022.
C44	M. Moosavi*, J. Clark. Lissy: Experimenting with on-chain order books. *WTSC*, *Proceedings of Financial Cryptography and Data Security: FC Workshops,* 2022.
C43	D. Demirag*, J. Clark. Opening sentences in academic writing: How security researchers defeat the blinking cursor. *ACM Technical Symposium on Computer Science Education (SIGCSE TS)*, 2022. [Rank: A]
C42	S. Eskandari*, M. Salehi*, W. C. Gu, J. Clark. SoK: Oracles from the Ground Truth to Market Manipulation. *ACM Advances in Financial Technology*, 2021
C41	M. Salehi*, J. Clark, M. Mannan. Red-Black Coins. *DeFi*, *Proceedings of Financial Cryptography and Data Security: FC Workshops,* 2021.
C40	D. Demirag*, J. Clark. Absentia: secure function evaluation on Ethereum. *WTSC*, *Proceedings of Financial Cryptography and Data Security: FC Workshops,* 2021.
C39	M. Nejadgholi*, N. Yang*, J. Clark. Ballot secrecy for liquid democracy. *VOTING*, *Proceedings of Financial Cryptography and Data Security: FC Workshops,* 2021.
C38	J. Clark, P.C. van Oorschot, S. Ruoti, K. Seamons, D. Zappala. Securing Email. *Proceedings of Financial Cryptography and Data Security (FC),* 2021. [Rank: A]
C37	M Rahimian*, S Eskandari*, J. Clark. Resolving the Multiple Withdrawal Attack in ERC20 Tokens. *2019 IEEE Workshop on Security & Blockchains (IEEE S&B)*.
C36	E. Mangipudi, K. Rao, J. Clark, A. Kate. Automated Penalization of Data Leakage using Crypto-augmented Smart Contracts. *2019 IEEE Workshop on Security & Blockchains (IEEE S&B)*.
C35	S. Eskandari*, M. Moosavi*, J. Clark. Transparent Dishonesty: front-running attacks on Blockchain. *Trusted Smart Contracts*, *Proceedings of Financial Cryptography and Data Security: FC Workshops*, 2019. LNCS 11599.
C34	M. Elsheikh, J. Clark, A. Youssef. Deploying PayWord on Ethereum. *Trusted Smart Contracts*, *Proceedings of Financial Cryptography and Data Security: FC Workshops*, 2019. LNCS 11599.

C33	V. Zhao, J. Choi, D. Demirag*, M. Mannan, K. Butler, E. Ayday, J. Clark. One-time programs made practical. *Proceedings of Financial Cryptography and Data Security (FC)*, 2019. LNCS 11598. [Rank: A]
C32	S. Eskandari*, A. Leoutsarakosg, T. Mursch, J. Clark. A first look a browser-based cryptojacking. *2018 IEEE Workshop on Security & Blockchains (IEEE S&B)*.
C31	C. Okoye*, J. Clark. Toward Cryptocurrency Lending. *Trusted Smart Contracts*, *Proceedings of Financial Cryptography and Data Security: FC Workshops*, 2018. LNCS 10958.
C30	M. Moosavi*, J. Clark. Ghazal: toward truly authoritative web certificates using Ethereum. *Trusted Smart Contracts*, *Proceedings of Financial Cryptography and Data Security: FC Workshops*, 2018. LNCS 10958.
C29	S. Eskandari*, J. Clark, M. Adham, V. Sundaresan. On the feasibility of decentralized derivatives markets. *Trusted Smart Contracts*, *Proceedings of Financial Cryptography and Data Security: FC Workshops*, 2017. LNCS 10323.
C28	N. Yang* and J. Clark. Practical Governmental Voting with Unconditional Integrity and Privacy. *VOTING*, *Proceedings of Financial Cryptography and Data Security: FC Workshops,* 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." *Proceedings of the 13th IEEE International Conference on Advanced and Trusted Computing (Bitcoin Track),* 2016.
C26	G. Dagher*, B. Bünz, J. Bonneau, J. Clark, D. Boneh. Provisions: Privacy-preserving proofs of solvency for Bitcoin exchanges. *Proceedings of the 22nd ACM Conference on Computer and Communications Security (CCS)*, 2015. [Rank: A+] AR: 19%
C25	J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. Kroll, E. W. Felten. Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. *Proceedings of the 34th IEEE Symposium on Security and Privacy (IEEE SSP)*, 2015. [Rank: A+] AR: 14%. 3rd highest cited security paper from 2015
C24	S. Eskandari*, D. Barrera, E. Stobert, J. Clark. A First Look at the Usability of Bitcoin Key Management. *Proceedings of the NDSS Workshop on Usable Security (USEC)*, 2015.
C23	D. Barrera, D. McCarney, J. Clark, P. C. van Oorschot. Baton: Certificate Agility for Android's Decentralized Signing Infrastructure. *Proceedings of the 7th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*, 2014.
C22	J. Bonneau, J. Clark, E. W. Felten, J A. Kroll, A. Miller, A. Narayanan. On Decentralizing Prediction Markets and Order Books. *Proceedings of the 13th Annual Workshop on the Economic of Information Security (WEIS)*, 2014.
C21	M. Backes, J. Clark, P. Druschel, A. Kate, M. Simeonovski. Back-Ref: Accountability in Anonymous Communication Networks. *Proceedings of the 12th International Conference on Applied Cryptography and Network Security (ACNS)*, 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. *Proceedings of the 18th Conference on Financial Cryptography and Data Security (FC)*, 2014. LNCS 8437. [Rank: A] 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. *Proceedings of the 11th International Conference on Applied Cryptography and Network Security (ACNS)*, 2013. AR: 23%.
C18	J. Clark and P. C. van Oorschot. SSL and HTTPS: Revisiting past challenges and evaluating certificate trust model enhancements. *Proceedings of the 34th IEEE Symposium on Security and Privacy (IEEE SSP)*, 2013. [Rank: A+] 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. *Proceedings of the 2012 Annual Computer Security Applications Conference (ACSAC)*, 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. *Proceedings of the 2nd Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM)*, 2012. AR: 37%.
C15	A. Essex, J. Clark, and U. Hengartner. Cobra: Toward concurrent ballot authorization for internet voting. *Proceedings of the 2012 USENIX Electronic Voting Technology Workshop/ Workshop on Trustworthy Elections (EVT/WOTE)*, 2012. AR: 35%.
C14	J. Clark and A. Essex. CommitCoin: Carbon dating commitments with Bit- coin. *Proceedings of the 16th Conference on Financial Cryptography and Data Security (FC)*, 2012. LNCS 7397. [Rank: A]
C13	J. Clark and U. Hengartner. Selections: an internet voting system with over-the- shoulder coercion-resistance. *Proceedings of the 15th Conference on Financial Cryptography and Data Security (FC)*, 2011. LNCS 7035. [Rank: A]
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. *Proceedings of the 19th USENIX Security Symposium, 2010*. [Rank: A+] AR: 15%.
C11	A. Essex, J. Clark, U. Hengartner, C. Adams. Eperio: Mitigating Technical Complexity in Cryptographic Election Verification. *Proceedings of the 2010 USENIX Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE)*, 2010.
C10	J. Clark, U. Hengartner. On the Use of Financial Data as a Random Beacon. *Proceedings of the 2010 USENIX Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE)*, 2010.
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. *Proceedings of the 4th International Conference on Electronic Voting (EVOTE)*, 2010.

C08	J. Clark, U. Hengartner, K. Larson. Not-So Hidden Information: Optimal Contracts for Undue Influence in E2E Voting Systems. *Proceedings of the Second IAVoSS International Conference on E-voting and Identity (Vote-ID)*, 2009, LNCS 5767.
C07	A. Essex, J. Clark, U. Hengartner, C. Adams. How to Print a Secret. *Proceedings of the 4th USENIX Workshop on Hot Topics in Security (HotSec)*, 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. *Proceedings of the 2008 USENIX Electronic Voting Technology Workshop (EVT)*, 2008.
C05	J. Clark, U. Hengartner. Panic passwords: Authenticating under duress. Proceedings of the 3rd USENIX Workshop on Hot Topics in Security (HotSec), 2008. AR: 32%.
C04	A. Essex, J. Clark, C. Adams. Aperio: High integrity elections for developing countries. *Proceedings of the IAVoSS Workshop on Trustworthy Elections (WOTE)*, 2008.
C03	J. Clark, P.C. van Oorschot, C. Adams. Usability of anonymous web browsing: An examination of Tor interfaces and deployability. *Proceedings of the Third Symposium On Usable Privacy and Security (SOUPS)*. 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. *Proceedings of the IAVoSS Workshop on Trustworthy Elections (WOTE), 2007*.
C01	A. Essex, J. Clark, R. T. Carback III, S. Popoveniuc. Punchscan in practice: An E2E election case study. *Proceedings of the IAVoSS Workshop on Trustworthy Elections (WOTE)*, 2007.

Articles in journals & periodicals

**Supervised student*

JIF = 2021 Journal Impact Factor, Journal Citation Reports, Web of Science / Clarivate

J10	Raphael Auer, Rainer Böhme, Jeremy Clark, Didem Demirag*. Mapping the Privacy Landscape for Central Bank Digital Currencies. *ACM Queue*, June/July 2022.
J09	E. Pimentel, E. Boulianne, S. Eskandari,* J. Clark. Systemizing the Challenges of Auditing Blockchain-Based Assets. *Journal of Information Systems*, Summer 2021.
J08	J. Clark, D. Demirag*, S. Moosavi*. Demystifying Stablecoins. *Communications of the ACM*. 63(7):40-46. Jul 2020. [JIF: 14.065]
J07	S. Ruoti, B. Kaiser, A. Yerukhimovich, J. Clark, R. Cunningham. Blockchain Technology: What is it good for? *Communications of the ACM*. 63(1):46-53. Jan 2020. [JIF: 14.065]
J06	G. Dagher*, B. Fung, N. Mohammad, J. Clark. SecDM: Privacy-preserving Data Outsourcing Framework with Differential Privacy. *Knowledge and Information Systems.* 62:1923–1960, 2020.
J05	A. Narayanan, J. Clark. Bitcoin's Academic Pedigree. *Communications of the ACM*. 60(12):36-45. 2017. [JIF: 14.065]

J04	E. Moher, J. Clark, A. Essex. Diffusion of voter responsibility: potential failings in E2E receipt checking. *USENIX Journal of Election Technology and Systems*. 3(1):1-17. 2014.
J03	J. Clark. Enhancing Anonymity: Cryptographic and statistical approaches for shredding our digital dossiers. *ACM Computing Reviews*. 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. Scantegrity II: End-to-End Verifiability by Voters of Optical Scan Elections Through Confirmation Codes. *IEEE Transactions on Information Forensics and Security*, 4(4):611-627, 2009. [JIF: 7.231]
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. *IEEE Security & Privacy*, vol. 6, no. 3, pp. 40–46, May/June 2008. [JIF: 3.105]

Book chapters

B05	J. Clark. The Long Road to Bitcoin. Foreword to: "Bitcoin and Cryptocurrency Technologies." *Princeton University Press*, 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." *CRC Press*, 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, *Springer*, 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, *Springer*, 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." *Oxford University Press*. 399-415, 2009.

Editorial activities

E03	Bracciali, A., Clark, J., Pintore, F., Roenne, P., Sala, M. (Editors). "Financial Cryptography and Data Security: FC Workshops 2019." Lecture Notes in Computer Science (LNCS) 11599. *Springer*, 2020.
E02	A. Zohar, I. Eyal, V. Teague, J. Clark, A. Bracciali, F. Pintore, M. Sala (Editors). "Financial Cryptography and Data Security: FC Workshops 2018." Lecture Notes in Computer Science (LNCS) 10958. *Springer*, 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. *Springer*, 2016.

Funding

External Funding

Year	Title, Program, Agency	Amount	PI	Co-Applicants
2023	“Understanding Blockchains through Experimentation,” Extension to previous project, Autorité des marchés financiers (AMF)	$200,000 over 3 years Share: 50%	Y	Emilio Boulianne (JMSB)
2021	“Privacy Design Landscape for Central Bank Digital Currencies,” Contributions Program, Office of the Privacy Commissioner of Canada (OPC)	$26,450 once Share: 100%	Y	
2021	“Understanding Blockchains through Experimentation,” Extension to previous project, Autorité des marchés financiers (AMF)	$100,000 once Share: 50%	Y	Emilio Boulianne (JMSB)
2021	“Enhancing transparency, inclusion, and privacy for financial and democratic technologies,” Discovery Grant (DG), Natural Sciences and Engineering Research Council of Canada (NSERC)	$35,000/year for 5 years Share: 100%	Y	
2020	“The Human-Centric Cybersecurity Partnership (HC2P),” Partnership Grant, Social Sciences and Humanities Research Council (SSHRC)	$2,434,323 over 5 years Share: TBD	N	Benoit Dupont + 32 others
2020	“Toward Scalable Systems for Securities on Blockchains,” Fintech Chaire, Autorité des marchés financiers (AMF) and Finance Montreal	$50,000 once Share: 50%	N	Kaiwen Zhang (ETS)
2019	“NSERC / Raymond Chabot Grant Thornton / Catallaxy Industrial Research Chair on Blockchain Technologies,” Natural Sciences and Engineering Research Council of Canada (NSERC)	$1,380,000 over 5 years Share: 100%	Y	
2017	“Understanding Blockchains through Experimentation,” Education and Good Governance Fund (EGGF), Autorité des marchés financiers (AMF)	$100,000/year for 2 years Share: 50%	Y	Emilio Boulianne (JMSB)
2016	“One Person, One Vote? Blockchain Technologies and Experiments in Voting and Party Governance,” Seed Grant, Centre for the Study of Democratic Citizenship (CSDC)	$6831 once Share: 50%	N	Fenwick Mckelvey (Comm)
2015	“Certificate Authority Report Card: Examining the Root of Data Protection on the Web,” Contributions Program, Office of the Privacy Commissioner of Canada (OPC)	$50,000/year for 1 year Share: 50%	Y	Mohammad Mannan (CIISE)

Year	Title, Program, Agency	Amount	PI	Co-Applicants
2015	“Vote par Internet : des technologies favorisant la démocratie,” Programme Établissement de nouveaux chercheurs universitaires, Fonds de recherche du Québec - Nature et technologies (FRQNT)	$19,000/year for 2 years Share: 100%	Y	
2014	“Secure online services for private user data,” Discovery Grant (DG), Natural Sciences and Engineering Research Council of Canada (NSERC)	$24,000/year for 5 years Share: 100%	Y	

Internal Funding

Year	Program	Amount	PI	Co-Applicants
2023	Aid to Research Related Events, Exhibition, Publication and Dissemination Activities (ARRE) Program	$5K once	Y	
2020	Aid to Research Related Events, Exhibition, Publication and Dissemination Activities (ARRE) Program	$5K once	Y	
2015	Aid to Research Related Events, Exhibition, Publication and Dissemination Activities (ARRE) Program	$5K once	Y	
2015	Individual Seed Program	$7K once	Y	
2013	Start-Up Grant	$50K once	Y	

Research Centres/Networks

- Human-Centric Cybersecurity Partnership (HC2P). Co-Investigator, 2020—present.
- Centre for the Study of Democratic Citizenship (CSDC). Member, 2016—present. Advisory Board, 2022—present.
- Smart Cybersecurity Network (SERENE-RISC). Knowledge Mobilization Network, Networks of Centres of Excellence of Canada (NCE). Co-Investigator, 2016—2021.

Evidence of Impact

Invited Talks and Seminars

- a16z crypto, "Fast Withdrawals from Optimistic Rollups," June 27, 2023.
- Digital Economy Taxation Network / Revenu Québec, DET 2023, “Going Digital: Tax Systems and Emerging Technology,” June 18, 2023.
- C-Dem/CSDC Forum, “Roundtable: Electoral Integrity,” Panel, June 4, 2023.
- CIADI/GCS Aerospace Meets Cybersecurity Forum, “Cybersecurity challenges in aerospace,” Moderator, April 17, 2023.
- Financial Management Institute of Canada, PD Week. "Blockchain and DeFi: Landscape," Nov 24, 2022.
- FIC, International Cybersecurity Forum, Nov 1-2, 2022.
- MTL Connect, "MTL Inspire." Panel, October 19, 2022.
- ACT International Midterm Conference, "Policing Blockchain." Panel, October 6, 2022.
- Fintech Cadence | Fintech Drinks, “Fintech & DeFi: How is fintech DeFi-ing the traditional banking system?” Panel, July 12, 2022.
- Blockchain Technology Symposium. “Blockchain Culture, Leisure and Luxury.” Panel, June 10, 2022.
- Quartier de l’innovation de Montréal. “Entre Terre et techno, ça clique ?” Panel, May 26, 2022.
- Fintech Cadence Certificate Program. "Understanding blockchain and its uses in the financial sector.” February 22, 2022.
- Autorité des marchés financiers. “Finance décentralisée et crypto : état de la situation, nouveaux risques et points de vigilance.” Panel, October 26, 2021.
- Smith School of Business, Queen’s University. “New Frontiers in Auditing: Risk and Opportunities in the Blockchain Sector.” Panel, October 7, 2021.
- Vancouver International Privacy & Security Summit (VIPSS). “Banking on the Future: How the Digital Surge Will Reshape How We Do Business.” Panel, May 6, 2021.
- CyberEco Cyber Conference. “Technology & blockchain.” May 5, 2021.
- Quartier de l’innovation de Montréal. “Blockchain - multiples usages.” Panel, April 28, 2021.
- Holt Accelerator, “[I AM PROTECTED].” Panel, April 21, 2021.
- UMBC Cyber Defense Lab Seminar. “Transparent Dishonesty: front-running attacks on Blockchain.” March 26, 2021.
- 1st Annual Lecture on Computer Science and Society. “The Blockchain and Cryptocurrency Landscape.” Carleton University. March 10, 2021
- Workshop on The State of Canadian Cybersecurity Conference: Human-Centric Cybersecurity. “Decentralized Finance: Landscape and Future Directions.” SERENE-RISC, February 18, 2021.

- Fintech Cadence Certificate Program. "Understanding blockchain and its uses in the financial sector." January 30, 2021.
- Montreal Lakeshore University Women's Club. "Bitcoins: What, why and how…" February 10, 2020.

Note: Parental & sabbatical leave Fall 2019—Summer 2021.

- Elections Quebec. "Internet Voting." 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. "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 Realestate 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.
- FinteQC. "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." CSDC 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.
- Online Voting Roundtable: Electoral Futures in Canada. “Blockchain and Voting: Assessment & Critique.” Invited Speaker, University of Ottawa. September 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

- Elections Quebec. "Internet Voting,” Citizen Jury. Nov 2, 2019.
- 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 — April 2018.
- Karina Gould, Minister of Democratic Institutions (House of Commons, Canada). CDSC roundtable. August 30, 2017.
- 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.

Press & Media (Selected)

- "What is Worldcoin and what does it mean for our privacy?" *Context.news (Thomson Reuters Foundation)*, June 7, 2023.
- "Clarity, please." *CBA/ABC National*, Nov 14, 2022
- "Deception, exploited workers, and cash handouts: How Worldcoin recruited its first half a million test users." *MIT Technology Review*, April 6, 2022.
- "It's a first, Bitcoin is now legal tender in one country." *CBC Radio*, Sep 23, 2021.
- "New kid on the blockchain: the young people using crypto for good." *DAZED*, Jul 22, 2021.
- "Digital currencies bring new options for financial privacy." *Hill Times*, May 5, 2021.
- "Satoshi & Company: The 10 Most Important Scientific White Papers In Development Of Cryptocurrencies." *Forbes*, Feb 13, 2021.
- "Contact tracing segment." *The Aaron Rand Show, CJAD 800*, May 26, 2020.
- "Are we ready for an app that trades privacy for more freedom?" *Montreal Gazette*, May 25, 2020.
- "Chaînes de blocs: dompter la décentralisation de l'informatique." *Le Devoir*, Mar 2, 2020.
- "Academic: All Undergrads Should Learn About Bitcoin & Blockchain." *Cryptonews*, Dec 22, 2019.
- "Why Quebec is betting big on Bitcoin." *Pivot Magazine (CPA Canada)*, Jan 8, 2019.
- "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.

Highly Qualified Personnel

HQP Job Placement

Sector	Organization
Blockchain Industry	ConsenSys Diligence, Offchain Labs, Trail of Bits, Quantstamp, BitAccess, Ether Capital
Faculty	Carleton University, Boise State University
PDFs	UQAM
Industry	KPMG, Deloitte, Morgan Stanley
Government	National Defence

Post-Doctoral

Name	State	Dates	Research Topic	Papers	Co-Supervisor
Elizabeth Stobert	PDF 🎓	2018/W-2018/F	Usable security	C24	

PhD

Name	State	Dates	Research Topic	Papers	Co-Supervisor
Reza Rahimian	PhD	2018/F-Part Time	Financial technology	C37	
Mahsa Moosavi	PhD	2018/S-	Layer-2 blockchain technology	C30, C35, J08, C44	
Didem Demirag	PhD 🎓	2018/W-2022/F	“Moving Multiparty Computation Forward for the Real World”	C33, J08, C40, C43, C47, J10	
Shayan Eskandari	PhD	2017/F-	Blockchain technology	C24, C27, C29, C32, C35, C37, C42, J09	
Pratyusha Bhattacharya	PhD	2017/S-	Smart Grid Security		M. Debbabi (CIISE)
Nan Yang	PhD 🎓	2014/S-2020/F	“Non-Local Contamination in Cryptography”	C28, C39	C. Crépeau (McGill)

Name	State	Dates	Research Topic	Papers	Co-Supervisor
Gaby Dagher	PhD 🎓	2013/F - 2015/F	“Toward secure and privacy-preserving data sharing and integration”	C26, J06	B. Fung (McGill)

MASc

Name	State	Dates	Research Topic	Papers	Co-Supervisor
Youwei Deng	MASc	2023/W-	Zero Knowledge Proofs		
Sina Pilehchiha	MASc 🎓	2021/ S-2022/F	“Improving Reproducibility in Smart Contract Research”		A.G. Aghdam (ECE)
Mahdi Nejadgholi	MASc 🎓	2019/ F-2022/S	“Nullification, a coercion-resistance add-on for e-voting protocols”	C39, C46	
Mehdi Salehi	MASc 🎓	2020/ W-2022/ W	“An Analysis of Upgradeability, Oracles, and Stablecoins in the Ethereum Blockchain”	C41, C42, C45	M. Mannan (CIISE)
Corentin Thomasset	MASc 🎓	2019/ F-2020/S	“SERENIoT : Politiques de sécurité collaboratives pour maisons connectées”		D. Barrera (Carleton), J. Fernandez (Polytechnique)
Chidinma Okoye	MASc 🎓	2016/S - 2017/F	“New applications of blockchain technology to voting and lending”	C31	
Mahsa Moosavi	MASc 🎓	2015/F - 2018/W	“Rethinking Certificate Authorities: Understanding and decentralizing domain validation”	C30, C35, J08, C44	
Michael Colburn	MASc 🎓	2014/F - 2018/S	“Short-Lived Signatures”		
Abhimanyu Khanna	MASc 🎓	2014/F - 2017/S	“Towards Usable and Fine-grained Security for HTTPS with Middleboxes”		M. Mannan (CIISE)
Shayan Eskandari	MASc 🎓	2013/F - 2016/W	“Real world deployability and usability of Bitcoin”	C24, C27, C29, C32, C35, C37, C42, J09	W. Hamou-Lhadj (ECE)

Supervised Graduate Projects (ENGR 6991)

Year	Students
2023	Mohammad Zawad Tahmeed
2019	Abhinav Kumar
2018	Jinumol James, Laleh Alimadadi, Rupesh Gawde, Brindha Shree, Isreal Tei, Saad Ahmen (MIAE: ENGR 6971)
2017	Temitiope Adetula, Shahab Odagar
2016	Ejiro Mary, Ogor Umukoro, Omoye Obazele
2015	S. Sandisha
2014	Paemka-Ojugbana Judah Chukwuma, Manish Megnath

Teaching

Courses Taught

Year/Term	Course	Class Size	Evaluation*
2022/4	INSE 6615: Blockchain Technology		
2022/4	INSE 6150: Security Evaluation Methodologies		
2022/2	INSE 6150: Security Evaluation Methodologies	70	1.72
2021/4	INSE 6630: Recent Developments in Info. Systems Security	67	N/A
2021/4	INSE 6150: Security Evaluation Methodologies	68	N/A
2021/2	INSE 6150: Security Evaluation Methodologies	49	N/A
2020/1	INSE 6150: Security Evaluation Methodologies	78	N/A
2018/4	INSE 6150: Security Evaluation Methodologies	92	1.20
2018/4	COMP 249: Object Oriented Programming II	109	1.73
2018/2	INSE 6630: Recent Developments in Info. Systems Security	53	1.19
2018/2	COMP 352: Algorithms and Data Structures	68	1.57
2017/4	INSE 6150: Security Evaluation Methodologies	88	1.69
2017/2	INSE 6110: Foundations of Cryptography	79	1.22
2017/2	INSE 6630: Recent Developments in Info. 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
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).*
- *Evaluations were suspended by the university from 2020-2021 due to COVID19*

Teaching Awards

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

External Lectures (Selected)

- "Decentralized finance (DeFi)," Faculty of Law, University of Ottawa. 22 Mar 2021.
- "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 University

University Committees

Leaves: Parental 2019-2020; Sabbatical 2020-2021

Year	Committee
2022-	GCS Elections Committee (Chair)
2022-	Concordia University Faculty Tribunal Pool
2021-	GCS Faculty Council
2018-2019	Concordia University Faculty Tribunal Pool
2018-2019	ENCS Blended/Online Pedagogy Committee
2017-2019	ENCS Elections Committee
2015-2019	CIISE PR/Website [Co-Chair]
2013-2019	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	Occurrences				
	MASc Defence	PhD Comp.	PhD Proposal	PhD Seminar	PhD Defence
2022	1	2	1		1
2021	3	1	1	1	1
2020	1	1		1	1
2019			2	3	3
2018		3	1		2
2013-2017	6	6	3	4	2

External PhD Examiner

- Md Mamunur Rashid Akand, University of Calgary, 2023
- Farimah Ramezan Poursafaei, McGill, 2022
- Patrick McCorry, Newcastle University, UK, 2017
- Giulia Alberini, McGill, 2015
- Jérôme Dossogne, Université libre de Bruxelles, Belgium, 2015

Service to Academia

Program Chairs

Year	Conference
2024	Financial Cryptography and Data Security 2024 (FC)
2022	Blockchain Technology Symposium (BTS)
2019	Workshop on Advances in Secure Electronic Voting (VOTING)
2018	Workshop on Advances in Secure Electronic Voting (VOTING)
2017	The Smart Cybersecurity Network: Spring 2017 Workshop (SERENE-RISC)
2016	Workshop on Bitcoin and Blockchain Research (BITCOIN)

General Chairs

Year	Conference
2024	Blockchain Technology Symposium (BTS)
2020	Privacy Enhancing Technologies Symposium (PETS)

Advisory Boards

Year	Journal
2019—	Privacy Enhancing Technologies Symposium (PETS)

Editorial Boards

Year	Journal
2013—2015	USENIX Journal of Election Technologies (USENIX JETS)

Program Committees (Selected)

Year	Conference
2023	ACM Computer and Communications Security (CCS)
2023	Workshop on Decentralized Finance (DeFi)
2023	Financial Cryptography and Data Security (FC)

Year	Conference
2022	Workshop on Privacy in the Electronic Society (WPES)
2022	Sixth International Joint Conference on Electronic Voting (E-VOTE-ID)
2022	Workshop on Advances in Secure Electronic Voting (VOTING)
2022	Workshop on Decentralized Finance (DeFi)
2022	Financial Cryptography and Data Security (FC)
2021	IEEE Security & Privacy on the Blockchain (IEEE S&B)
2021	Financial Cryptography and Data Security (FC)
2021	Sixth International Joint Conference on Electronic Voting (E-VOTE-ID)
2021	Workshop on Advances in Secure Electronic Voting (VOTING)
2020	Financial Cryptography and Data Security (FC)
2020	IEEE Security & Privacy on the Blockchain (IEEE S&B)
2019	Financial Cryptography and Data Security (FC)
2019	IEEE Security & Privacy on the Blockchain (IEEE S&B)
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)

Year	Conference
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	International Conference on E-Voting and Identity (VoteID)
2012	USENIX Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE)
2011	USENIX Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE)

Journals (Most Recent Year / Selected)

Most Recent Year	Journal / Conference
2023	IEEE Security and Privacy Magazine
2022	IEEE Transactions on Information Forensics and Security (TIFS)
2021	Bank for International Settlements (BIS) Working Paper Series
2021	IEEE Transactions on Dependable Secure Computing (TDSC)
2021	Communications of the ACM

Reviews for Funding Agencies (Most Recent Year / Selected)

Most Recent Year	Agency
2023	Israel Science Foundation (ISF)
2023	Natural Sciences and Engineering Research Council of Canada (NSERC)
2022	Social Sciences and Humanities Research Council of Canada (SSHRC)
2020	MITACS
2019	Fonds de Recherche du Québec – Nature et technologies (FRQNT)
2019	Alberta Innovates

Most Recent Year	Agency
2017	Office of the Privacy Commissioner