EXHIBIT 8

Declaration of Jeremy Clark

in Support of Motion for Class Certification

Jeremy Clark, Ph.D., P.Eng.

February 10, 2025

Contents

1 Preliminaries

1.1 Assignment

I have been engaged by Plaintiffs Ryan Huegerich, Jonathan Semerjian, Nabil Nahlah, Till Freeman, Marko Ciklic, Tunisia Brignol, Milan Puda, Neil Shah, Michael Buckley, and Christopher DeLuca ("Plaintiffs"), through their counsel, to provide a declaration in the case captioned *In re EthereumMax Investor Litigation*, Case No. 2:22-cv-00163, pending in the United States District Court for the Central District of California. Plaintiffs have retained me to independently analyze and opine on the EMAX token, its technical implementation, and the mechanisms used to exchange the token and establish its price.

1.2 Qualifications

I am an associate professor at the Concordia Institute for Information Systems Engineering (CIISE) at Concordia University in Montreal, QC, Canada. I hold the NSERC/Raymond Chabot Grant Thornton/Catallaxy Industrial Research Chair in Blockchain Technologies. I hold a Ph.D. in Computer Science from the University of Waterloo, awarded in 2011 with the university's Alumni Gold Medal, and in the discipline of applied cryptography. I am a professional engineer (P.Eng.) with the Professional Engineers of Ontario (PEO).

I have over 10 years of research expertise in digital assets and blockchain, and even more experience with related areas of cryptography. My expertise includes material knowledge of Bitcoin and Ethereum.

Bitcoin was described in late 2008 and released as software in early 2009. I began pursuing academic research on Bitcoin in 2011 and have published over 20 peer-reviewed papers on Bitcoin, Ethereum, digital assets, blockchain technology, and similar topics. Research highlights include CommitCoin [2], one the earliest academic works on Bitcoin published in

Financial Cryptography and Data Security (Conference Rank:[1] A) in 2012; our 2015 systemization of knowledge on Bitcoin and blockchain research [1] published in *IEEE Symposium on Security and Privacy* (Conference Rank:[2] A+; citations 1000+[3]); and our 2017 article on Bitcoin's academic pedigree [4] published in the *Communications of the ACM* (Journal Impact Factor:[4] 14.065; downloads: 300K+[5]).

I have testified on digital assets to the Standing Senate Committee on Banking, Commerce and Economy of the Senate of Canada (April 3, 2014), and to the Standing Committee on Finance of the House of Commons of Canada (March 27, 2018). I have given over 50 presentations on digital assets to companies, government agencies, law enforcement, pension plans, and academic groups.

My attached CV contains further evidence of my expertise and research impact in these subjects.

1.3 Facts, data, and documents relied upon

To prepare this report, I read technical reports on EMAX, reviewed the technical information distributed online by EMAX, examined the source-code made available on GitHub, and reviewed the academic literature on tokens. I examined the smart contracts deployed on Ethereum using tools like *Etherscan* and *Dune Analytics*. I also reviewed all legal documents and discovery presented to me by council. Finally, as necessary, I also reviewed the technical details of Ethereum. When I draw directly on the documents I considered, I will provide a citation inline. In cases where I make an assertion with a citation, it is asserted to be true as of the publication date of the cited document.

[1] CORE Conference portal, Feb. 2024.
[2] CORE Conference portal, Feb. 2024
[3] Google Scholar, Feb. 2024.
[4] Clarviate / Web of Science, Feb. 2024.
[5] 293 530 Queue + 41 257 CACM, ACM Digital Library, Feb. 2024

1.4 Principles and methods

I reviewed the complaint and disclosure provided by Plaintiff's attorneys. I reviewed background information and relied on my past research to understand the technology involved. From the Ethereum addresses associated with the EMAX token, I used analysis tools Dune Analytics and Etherscan to make determinations about activities involving the token, including purchases and sales. I used Mathematica to perform calculations based on the data. I examined the Ethereum contract code using verified code on Etherscan and the EthereumMax GitHub account.

1.5 Disclaimers

For serving as an expert witness, I am remunerated by *Scott + Scott L.L.P.* at $400 USD per hour. My compensation is not dependent upon me reaching any specific conclusion or opinion. All opinions are mine and do not necessarily reflect those of Concordia University or any sponsors of my research grants and chair. I have never purchased or knowingly[6] owned EMAX tokens. Portions (concerning background information) of this report may be copied or adapted from reports I have solely authored in the past.

2 Overview of technology

In this section, I provide an overview of the relevant technology and a summary of Ethereum, EthereumMax, EMAX, tokens standards, upgradable smart contracts, automated market makers (AMMs), and price discovery.

2.1 Blockchain technology

Bitcoin. Described in 2008 and launched in early 2009, the Bitcoin cryptocurrency introduced a digital system for asset creation and transfer that is operated through the consensus,

[6]Given the way Ethereum operates, anyone at any time could opt to 'airdrop' EMAX tokens to one of my Ethereum addresses without my consent, causing me to own them.

at every step, of a set of independent servers all around the world, with no one server in charge. Bitcoin is designed to run on the internet and since the internet contains hostile entities, the system is designed to run correctly even when a fraction of the servers are malicious and try to attack the system. We also say that Bitcoin is an "open" and "permissionless" system. Open means that anyone on the internet with the appropriate technical capabilities is invited to join the system. Permissionless means that joining the system (and leaving the system) does not require the authorization of any entity in the system. The protocol itself may impose rules about how and when servers can join but ultimately, a permissionless system will let anyone join eventually if they meet the in-protocol prerequisites. Once operating in the system, the servers (called miners or validators) work on verifying and recording transactions in a data structure called a blockchain, which uses cryptographic techniques to provide data integrity.

Ethereum. After the initial success of Bitcoin, a group of enthusiasts believed that an open and permissionless blockchain could be useful beyond use-cases like the transfer of assets. Bitcoin itself is limited in terms of what it can do beyond this. After failing to convince the Bitcoin community to expand the scope of Bitcoin, they created a competitor called Ethereum. The Ethereum blockchain began producing blocks in July 2015. The key difference of Ethereum is that users can design and deploy custom software applications (called "smart contracts") and have the validators run these applications for them. Smart contracts might allow users to make custom tokens, trade Ethereum's digital asset ETH for these tokens, borrow tokens, invest in tokens, purchase financial derivatives based on tokens, and many other use-cases that are now called "decentralized finance (DeFi)." The most popular smart contracts in addition to DeFi, according to the website DappRadar,[7] allow gambling, gaming, social platforms, and transacting digital art. "Smart contracts" are essentially computer programs or applications. They are sometimes called "decentralized applications" or Dapps instead.

[7] "Top Blockchain Dapps," Dapp Radar, Retrieved Jan–Feb 2025.

Ethereum[8] begins with the same capabilities as Bitcoin: users can create addresses to receive and send ETH, which is Ethereum's on-chain currency. Ethereum is designed with a new kind of transaction where a user can submit the code of a computer application (or a "contract") to Ethereum. The contract will be assigned an address and its code will be stored on the blockchain at this address. The user pays a fee to deploy a contract (proportional to the size of the contract). An address is a long, random sequence such as: `0x15874d65e649880c2614e7a480cb7c9a55787ff6` which we will abbreviate as `0x15...7FF6`. If the reader clicks on an abbreviated address, it will open a list of the address's activities on the website Etherscan.

At this point, the user who created the contract could disappear, and the application will still live on the blockchain and be accessible to current and future Ethereum users. Contracts are "autonomous" which means they cannot perform computations by themselves ("in the background") the way a computer or smartphone application might. Contracts only run code when users ask Ethereum to run the contract (and pay for it). Once the user-requested computation is completed, the contract code hibernates until the next user requests that it runs. What users are allowed to run computations and what computations a contract can perform are contained in the code of the contract itself (and can be anything the programmer of the contract decides when programming it).

While a sophisticated user might interact with a smart contract directly on Ethereum, most contracts are accompanied by a website with graphics, text input, buttons, and other user interface elements that will interact with Ethereum and the smart contract. A user will navigate to the website and if they wish to use the contract, they will "connect" the website to the Ethereum (or Ethereum-compatible) software they are using to manage their signing keys (called a "wallet"). The website will pass the cost and other details of what the user wants to do (called a "transaction") to the user's wallet software (*e.g.,* MetaMask). The wallet software will display the information to the user and ask the user for consent to

[8]Note that when relevant, this report describes how Ethereum operated during the relevant period (14 May–27 June 2021) and will differ from how it operates today, especially as it pertains to gas fees, consensus, and data storage.

execute the transaction (typically requiring a password) or provide an option to cancel the transaction.

Ethereum fees. To ensure validators are fairly compensated and to combat malicious actors from stalling the network ("denial of service" attacks) by asking for a long-running computation to be performed, all computations are broken into small steps ("instructions" or "opcodes") where each step is assigned a value in a unit called "gas." The value represents how complex the computation step is to execute or store (*e.g.,* a multiplication has a higher gas value than an addition). Users then specify a rate of ETH per unit of gas that they are willing to pay as a fee to the validator who includes their transaction in a block. In practice, the user's software examines the current conditions of Ethereum and suggests a rate to the user. The main takeaways are: (1) all computations cost the user ETH in fees, (2) more complex computations cost more than simpler ones, and (3) validators earn revenue by performing computations on Ethereum.

2.2 EthereumMax and the EMAX token

The EthereumMax project implemented a 'token' which is called EMAX. Over the relevant period (14 May–27 June 2021), the EMAX token was operated through smart contracts running on Ethereum. The code for a token contract can be thought of as a ledger of every address that has held EMAX at some point, and the current balance held by that address. Addresses have functions available to them to transfer EMAX tokens to another (new or existing) address, among other things we will describe below.

I am aware of two separate deployments of the EMAX token. The first deployment occurred on 12 May 2021 when the Ethereum address `0xb9...5C7e` deployed the token contract at address `0xA3...11df`. The token was made available for trading on Uniswap (see below) on 14 May 2021. Ownership of the token contract was transferred to `0x35...e226` on 23 May 2021.

On May 25, a second deployment of the EMAX token was made. This time, the ad-

dress 0xa1...d202 deployed the token at the address 0x15...7FF6 (as discussed below, this address is the 'front door' of a structured set of contracts).

2.2.1 The ERC-20 interface

Many tokens exist on Ethereum. Many applications, implemented as smart contracts, also exist on Ethereum to allow traders to exchange tokens for ETH (and vice-versa), lenders to lend tokens with interest, speculators to enter leveraged financial positions on token prices, and other services under the umbrella term of decentralized finance (DeFi). When EMAX or any other token launches, it is useful if the token behaves similar to other tokens. This allows the token to 'plug-and-play' with the DeFi services even if the DeFi services were coded up long before the token existed.

To enable the interoperability between tokens and services that use tokens, a standard called ERC-20 was proposed and widely adopted for tokens that are designed to be fungible [5]. ERC-20 specifies that token function in a specific way with known names and patterns for operations. This way, services (whether online as websites or on-chain as smart contracts) can be coded to interoperate with any ERC-20 token that follows the standard, allowing near instant integration of new tokens that are ERC-20 compliant.

EMAX tokens implement the ERC-20 interface (*i.e.,* are ERC-20 compliant).

2.2.2 The ERC-1967 interface

As mentioned, the EMAX token contract was deployed more than once. The first, I will call the EMAX-Pilot token, was deployed at 0xA3...11df on 12 May 2021. An important characteristic of Ethereum is that the code of a smart contract cannot be changed once deployed (contracts are 'immutable'). Items stored in the smart contract can be changed, provided the code enables resetting values, and thus the functionality of a smart contract can be indirectly changed, but it requires developers to anticipate the way the contract might be changed in the future and ensure the code exists for allowing it. Immutability is problematic if developers do not anticipate changes or if a flaw (bug or security vulnerability) is found

in the code.

For these reasons, developers have proposed ways to 'cheat' the immutability of smart contracts to enable updates. The simplest is a 'social upgrade [6]' where a new contract is deployed at a new address and users are told where the new contract is and websites are updated to the new address. This could explain the second deployment of EMAX to a new address of `0x15...7FF6` on 25 May 2021. As alleged in the complaint, on May 26, 2021, EMAX's official Twitter account tweeted: 'Our new token to buy $eMax is LIVE! This is our updated and ONLY contract address – 0x15874d65e649880c2614e7a480cb7c9A55787FF6.' Social upgrades are tedious for a few reasons: the new address needs to popularized, the old contract may still be functional (depending if a locking mechanism was anticipated and coded in the contract), and all the data from the old contract (*e.g.,* account balances and allowances in the case of an `ERC-20` token) needs to be copied from the old contract to the new contract (if the intention is to preserve the state of the old contract in the new contract), which could be costly in both time and fees.

Developers have thus proposed additional ways of allowing upgradeable contracts, patterns that are typically complex to deploy but once in place, allow fluid upgrades. The most popular is the proxy pattern with techniques standardized in `ERC-1967`.

In this pattern, several contracts with different roles work together to give the appearance of a single contract. Users are given the address of a 'proxy contract' which does not have any of the actual code of the contract. Instead, it works as a 'front door' and simply forwards every request (*e.g.,* transfer tokens from address A to address B) to a second contract called the 'logic contract' which implements the actual code. The address of the logic contract is held by the proxy contract in a modifiable variable. If an upgrade to the code is required, the new logic contract is deployed at a new address and then the proxy contract is changed to point at the new logic contract. All the memory of the contract (*e.g.,* account balances) is stored within the proxy contract (technically achieved by forwarding function calls from the proxy to logic contract using `delegatecall` instead of `call`). As it is not stored within the logic contract, when the logic contract is changed, no migration of state is needed.

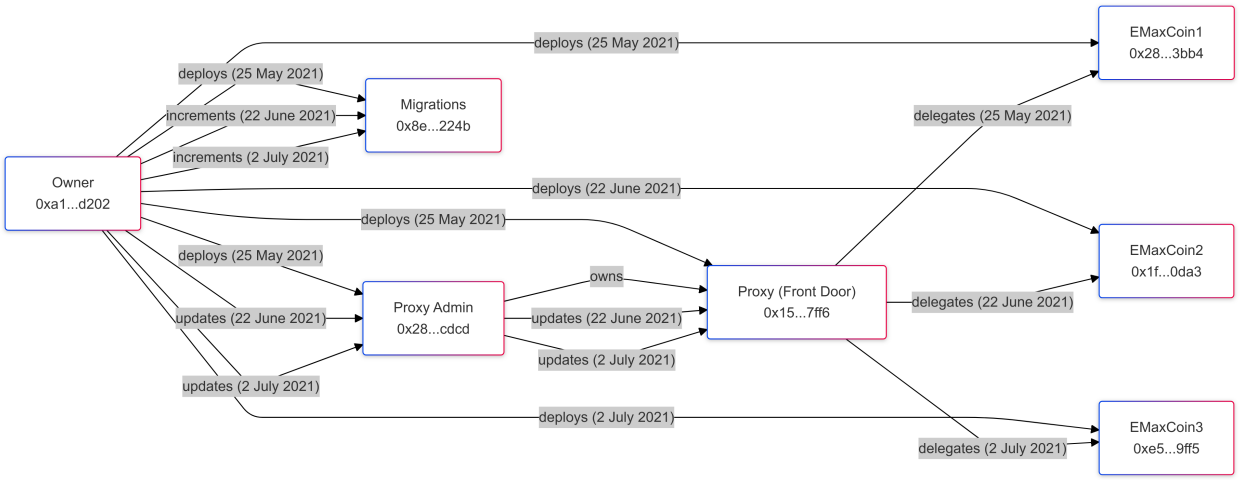

Figure 1: The second deployment of the EMAX token, using a transparent proxy upgrade pattern.

A small technical point remains. If the proxy forwards *every* functional call to the logic contract, then the proxy contract's pointer to the logic contract's address can never be updated as this is the one function that should not be forwarded and should be executed within the proxy contract. The typical way to handle this is to create an additional contract, called the proxy administrator. The proxy contract will forward every function from every address except the proxy administrator to the logic contract, and any function calls from the proxy administrator will not be forwarded and will be executed within the proxy.

The second deployment of EMAX on 25 May 2021 followed the `ERC-1967` upgradability pattern. It is illustrated in Figure 1. Each contract in the pattern was deployed from address `0xa1...d202`. The commonly understood address of EMAX is in actuality the address of the proxy: `0x15...7FF6`. The code of the `ERC-20` token is in `0x28...3bb4`. The administrator address is `0x28...cdcd`. Another contract, called migrations, is also deployed but not important—likely an artefact of the development tool Truffle Suite.

Again, the purpose of this complex deployment is to allow the logic contract to be changed. EthereumMax has utilized this functionality many times over the years, including once during the relevant period (14 May–27 June 2021) and once shortly after. On 22

June, the logic contact was updated to `0xff...0da3` (EMAX2) and on 2 July 2021, it was updated again to `0xe5...9ff5` (EMAX3)

For the purposes of this report, I did not fully investigate the changes made to code of the EMAX contract (EMAX-Pilot, EMAX1, EMAX2, and EMAX3) however all are ERC-20-compliant contracts where the vast majority of the code is the same. EMAX1 appears to add a cap to the maximum amount of a single transfer, not present in EMAX-Pilot. EMAX2 changes fee amounts. EMAX3 adds functionality for tokens to be burned and also appears to remove the 'deny list' for addresses excluded from transacting EMAX tokens (I did not check if any addresses were ever on this list). EMAX3 was deployed after the relevant period and many more updates have followed to the present time.

2.3 Automated market makers (AMMs)

To buy and sell blockchain tokens, a user might arrange a trade with another user, use an exchange service running on an internet server, or perform the trade through smart contracts running on Ethereum—called a decentralized exchange (DEX). The advantage of a DEX is that registering a new token (compliant with ERC-20) for trading can be completed autonomously by anyone without permission or approval, as can trading. The disadvantage of a DEX is that Ethereum is very expensive (compared to an internet server or cloud service) and it was financially infeasible in 2021 to trade through a traditional market structure like an orderbook or an call market on Ethereum [3].

For this reason, the most popular DEXes in relevant period used a market structure tailored for Ethereum (or other constrained computational platforms) called an automated market maker (AMM)—the most popular of which was Uniswap v2. Note that Uniswap v3 was launched in May 2021 but was not immediately adopted by users (who could continue to use v2).

An AMM is akin to an on-chain vending machine that anyone can use at any time. It is loaded with two kinds of ERC-20 tokens (called a trading pair)—in this case, (1) Ethereum's native currency ETH, which is put into ERC-20 compliant form and called Wrapped ETH

(WETH), and (2) EMAX tokens. If a trader wants to purchase x EMAX tokens, they must deposit y WETH tokens (and vice-versa). Each trade changes the ratio of tokens in the AMM (called the liquidity pool). The values of x and y vary depending on the ratio of tokens in liquidity pool (the 'starting price'), the size of the trade (the smaller the pile of one token gets, removing more requires a greater and greater number of the other token), and the total size of liquidity pool (the larger the pool, the less the price slips for trades of equal size). Everything about the pricing rule is public and deterministic. Uniswap v2's pricing rule is called a constant product rule.

Consider an AMM that presently holds A WETH and B EMAX. This indicates that the market considers B EMAX equal to A WETH, and thus the price of EMAX is A/B EMAX/ETH. If the true value of EMAX is not A/B (whether worth more or worth less), an arbitrageur can make a trade with the AMM that is profitable and will result in the AMM's pool being adjusted to its actual value.

The remaining question is where does the AMM get its tokens from? Anyone can become a liquidity provider (LP) by supplying tokens for the AMM to trade and earn fees on every trade. If an AMM for a given token does not yet exist, the first LP to fund it can set the opening price of the token by depositing equal values (in price) of both tokens. As trades are executed against the AMM, the ratio of token volumes changes, and the AMM's price is determined by its current token ratio. Additional LPs must add tokens in the current ratio. When LPs withdraw liquidity, they receive their proportional share of the AMM's total liquidity, based on the current ratio, which is likely different from the ratio at which they initially added liquidity.

2.4 EMAX Activities in Uniswap v2

The EMAX-Pilot token was added to Uniswap v2 on 14 May 2024 and the upgraded EMAX token deployed on 25 May 2024 was added to Uniswap v2 on the same day. Over the relevant period, different DEXes were used to trade EMAX but Uniswap v2 accounted for the majority, around 300K transfers of the upgraded token were initiated on Uniswap, which

is 2 orders of magnitude more than any other DEX.

The price and trading volume of EMAX on Uniswap v2 correlates to the period during which the complaint describes EthereumMax as launching a massive celebrity-driven social media marketing campaign to promote the token. As users purchase EMAX, they deposit WETH into the AMM, growing the amount of WETH in the AMM. This results in the nominal price of EMAX, as determined by the ratio of tokens in the AMM, to increase. At any point, participants who believe that EMAX is over-valued by the AMM can deposit EMAX into the AMM to extract the WETH that was added to the pool by EMAX purchasers. This however requires access to EMAX to perform. Liquidity providers (LP) who believe the same can also withdraw from the liquidity pool and receive a higher ratio of WETH than they put into the liquidity pool originally (and this requires the LP to have access to EMAX before adding liquidity). In both cases, large EMAX holders (such as project founders) are able to extract WETH quickly, causing the price of EMAX to crash, especially when acting in a coordinated manner. Other investors in EMAX are left with a near worthless token. Based on my review of the transaction data from the EMAX liquidity pools, this is a coherent explanation of what transpired in the data.

3 Opinions

I have been asked by counsel for the Plaintiffs to discuss how data can be collected about transfers, purchases, and sales of the EMAX token.

Opinion 1: On-chain actions involving the EMAX token can be determined

As EMAX is an Ethereum-based token, every action taken on Ethereum is recorded in Ethereum's blockchain data structure. The data is widely available. The blockchain data may be obtained by asking a full (potentially archival) node on Ethereum. It is also made available through third party sources including the website Etherscan and the blockchain analytics tool Dune Analytics. Commercial companies also offer analytical tools, with popular options including Chainalysis and TRM.

As the EMAX token implements the ERC-20 interface, the token contract will emit an 'event' every time the token is transferred. Events are logged with the blockchain data and timestamped. Examining event data for transfers on Etherscan can determine EMAX token transfers, regardless of whether the transfer was originated by an EMAX holder or if it was initiated through a third party decentralized application (DApp) such as Uniswap.

For purchases and sales of EMAX tokens, Uniswap v2 and other on-chain exchange services also use standardized transaction types that are recognized and labeled by analysis tools like Etherscan and Dune Analytics. Over the relevant period, on-chain EMAX purchases and sales (as a trading pair with WETH) were primarily conducted on Uniswap v2. For every trade on Uniswap v2, the trade price in EMAX/WETH can be determined. As necessary, the price of EMAX/USD can also be determined by noting that WETH trades with ETH at parity and historical prices of ETH/USD are widely available from many sources (*e.g.,* CoinMarketCap).

Opinion 2: A common methodology can be used to determine EMAX purchases on Uniswap

Over the relevant period, over 300,000 purchases of EMAX-Pilot or EMAX was made through Uniswap v2. Of these, 100,000 were made by unique Ethereum addresses. While Ethereum makes no restriction on how many addresses a single individual may operate, it is indicative of a large set purchasers who may have loss money on EMAX investments. A complete list of such addresses can be precisely determined using blockchain data.

Given an Ethereum address, the blockchain has recorded a complete set of EMAX activities: every purchase, sale, and transfer. Each activity is timestamped (at the time it is finalized by Ethereum) and the current price on Uniswap can be determined from the ratio of EMAX and WETH tokens in the AMM. This data is sufficient to compute the profit and loss of any address, by summing the value of each of the purchase transactions and subtracting out the value from any sales. The final step would be to subtract the value of any unsold tokens currently held, which would likely have zero or a *de minimus* value.

I built a proof-of-concept tool on Dune Analytics to assist in this computation. I tested it on each address of each plaintiff, who have collected and produced their addresses and transaction records in discovery. Additionally I tested it on other randomly selected addresses (of unknown individuals) who purchased EMAX over the relevant period. As expected, the methodology works for any EMAX purchases made on Uniswap from any address without distinction. As necessary, it could be expanded to cover airdrops, other DEXes, liquidity provision, or any on-chain event.

4 Declaration

The opinions expressed in this report are based on my review and analysis of the documents I cite. I reserve the right to supplement my report and analysis based on any new evidence brought to my attention.

February 10, 2025

Montreal, QC, Canada

References

[1] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. Kroll, and E. Felten. Bitcoin and second-generation cryptocurrencies. In *IEEE Symposium on Security and Privacy*, 2015.

[2] J. Clark and A. Essex. Commitcoin: Carbon dating commitments with bitcoin. In *Financial Cryptography*, 2012.

[3] M. Moosavi and J. Clark. Lissy: Experimenting with on-chain order books. In *FC Workshops (WTSC)*, 2023.

[4] A. Narayanan and J. Clark. Bitcoin's academic pedigree. *Communications of the ACM*, 60(12), 2017.

[5] R. Rahimian and J. Clark. Tokenhook: Secure erc-20 smart contract. *arXiv preprint arXiv:2107.02997*, 2021.

[6] M. Salehi, J. Clark, and M. Mannan. Not so immutable: Upgradeability of smart contracts on ethereum. In *FC Workshops (WTSC)*, 2022.

5 Curriculum Vitae

Attached.

February 6, 2025
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 June 2018 – present.
- Assistant Professor, Concordia Institute for Information Systems Engineering (CIISE), Concordia University. 1 August 2013 – 31 May 2018.

Professional Designations

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

Consulting

- Subject matter expert on digital assets, *Susman Godfrey LLP,* In re Ripple Labs Inc. Litigation (4:18-cv-06753). 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

- Program Advisory Committee (Information Technology – Cybersecurity/Cybersecurity & Threat Management), Seneca Polytechnic, Oct 2024—present.
- 3iQ Digital Asset Management, Advisory Board, 2017—2021.

Leaves

- Sabbatical: 1 July 2020—30 June 2021
- Parental: 27 October 2019—26 April 2020

Academic Background

Degrees

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

Post-Doctorate

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

Awards

- 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
- Grand Prize: Best Election System. "The Punchscan Voting System." University Voting Systems Competition (VoComp). 2007

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 and A*). 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 250+ times, while the journal version has been cited only 130+ times.

Statistics

Type	Lifetime	Concordia
Journals & Periodicals	11	9
Refereed Conferences & Workshops	50	30
Book Chapters	5	2

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.

Updated Fall 2024	Lifetime
Citations	10027
h-index	30

Abbreviations

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

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

Refereed conference publications

C50	R. Rahimian, J. Clark. A Shortfall in Investor Expectations of Leveraged Tokens. *Advances in Financial Technology*, 2024.
C49	M. Moosavi*, M. Salehi*, D. Goldman, J. Clark. Fast and Furious Withdrawals from Optimistic Rollups. *Advances in Financial Technology*, 2023.
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

J11	E.V. Mangipudi, K. Rao, J. Clark, A. Kate. Pepal: Penalizing multimedia breaches and partial leakages. *International Journal of Information Security*, September 2023.
J10	Raphael Auer, Rainer Böhme, Jeremy Clark, Didem Demirag*. Mapping the Privacy Landscape for Central Bank Digital Currencies. *Communications of the ACM*. 66(3):46-53. March 2023. [JIF: 14.065]
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. July 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. January 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	“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)
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	

Year	Title, Program, Agency	Amount	PI	Co-Applicants
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	

Research Centres (as co-PI)

Year	Title, Program, Agency	Amount	PI	Co-Applicants
2024	“Centre pour l'étude de la citoyenneté démocratique (CECD),” Regroupements stratégiques / Centre en fonctionnement, Fonds de recherche du Québec - Société et culture (FRQSC)	$2,219,922 over 5 years Share: TBD	N	Frédérick Bastien + 46 others
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

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 Membership

- Human-Centric Cybersecurity Partnership (HC2P). Co-Investigator, 2020—present.
- Centre for the Study of Democratic Citizenship (CSDC). Co-investigator, 2016—present. Advisory board member, 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, “Towards Succinct Proofs of Solvency,” Invited Talk, June 18, 2024.
- CSNet 2023, "Privacy Options for Central Bank Digital Curriencies (CBDCs)." Keynote, October 17, 2023.
- Cyberjustice Labratory, University of Montreal, "Web3: Landscape and Future Directions." Keynote, October 16, 2023.
- Cybersecurity and Privacy Institute (CPI) Annual Conference, University of Waterloo. "Transparent Dishonesty: front-running attacks on Blockchain." Invited Talk, October 12, 2023.
- UMBC Cyber Defense Lab Seminar, "Fast Withdrawals from Optimistic Rollups.” Invited Talk, September 8, 2021.
- a16z crypto, “Fast Withdrawals from Optimistic Rollups,” Invited Talk, June 27, 2023.
- MIT Digital Currency Initiative (DCI), “Privacy Options for Central Bank Digital Curriencies (CBDCs),” May 23, 2023.
- Berkman-Klein Center for Internet & Society (Harvard), “Privacy Options for Central Bank Digital Curriencies (CBDCs),” Blockchain and Privacy Workshop, May 22, 2023.
- Digital Economy Taxation Network / Revenu Québec, DET 2023, “Going Digital: Tax Systems and Emerging Technology,” Panel, 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," November 24, 2022.
- FIC, International Cybersecurity Forum, November 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.
- Elections Quebec. "Internet Voting." November 2, 2019.
- Blockchain at McGill. “Introduction to Blockchain for Non-Profits,” Social Innovation: Int’l Development and Blockchain. 29 March 2019.
- Canada Mortgage and Housing Corporation (CMHC). "Blockchain Technologies: Landscape and Future Directions.” 26 February 2019.
- CFA Montreal FinTech Rendez-vous. "Blockchain Technologies: Landscape and Future Directions.” 7 February 2019.
- Loto-Quebec. “Lunch and learn.” 22 January 2019.
- RISQ Colloquium. "Blockchain Technologies: Landscape and Future Directions.” 29 November 2018.
- TriPAC Pension Advisory Committees. "Blockchain Technologies: Landscape and Future Directions." Treasury Board Secretariat. 21 November 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, August 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,” March 22, 2016.
- MIT Bitcoin Expo. ”Blockchain-based voting: potential and limitations,” MIT, March 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. November 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). CSDC 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)

- “Where Did Bitcoin Come From?” *Mornings With Sue And Andy. QR Calgary 770*, 8 November 2024.
- “Who Invented Bitcoin?” *Mornings with Simi, CKNW 980*, 4 November 2024.
- “Did a Canadian developer really invent bitcoin? A new HBO show explores an intriguing theory,” *The Conversation*, 31 October 2024.
- “Parsing Satoshi: What the Malmi emails reveal about Bitcoin’s creator,” *CoinTelegraph*, March 6, 2024.
- “Bridging traditional investment with cryptocurrencies? One Canadian miner tried it,” *CBC News,* January 24, 2024.
- “Two years after peak crypto, Bitcoin has faded from the political conversation,” *CBC News*, November 3, 2023.
- “Are Quebec’s Crypto Mines Here to Stay?” *The Rover*, June 16, 2023.
- “What is Worldcoin and what does it mean for our privacy?” *Context.news (Thomson Reuters Foundation)*, June 7, 2023.
- “Clarity, please.” *CBA/ABC National*, November 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*, September 23, 2021.
- “New kid on the blockchain: the young people using crypto for good.” *DAZED*, July 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*, February 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*, March 2, 2020.
- “Academic: All Undergrads Should Learn About Bitcoin & Blockchain.” *Cryptonews*, December 22, 2019.
- “Why Quebec is betting big on Bitcoin.” *Pivot Magazine (CPA Canada)*, January 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*, February 28, 2017.
- "Block the vote: Could Blockchain Technology Cybersecure Elections?" *Forbes*, August 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*, February 19, 2016.
- "Princeton University releases first draft of bitcoin textbook," *CoinDesk*, February 10, 2016.
- "The top 10 cryptocurrency research papers of 2015," *CoinDesk*, December 27, 2015.
- "Canada's Internet Voting Problem," *SC Magazine*, February 2015 issue.
- "Latest Internet voting reports show failures across the board," *Al Jazeera America*, February 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*, March 28, 2014.
- "2014 Federal Budget Calls Bitcoin A Terrorist, Crime 'Risk', " *Huffington Post*, February 12, 2014.
- "Bitcoin: How its core technology will change the world," *New Scientist*, February 5, 2014.
- "More than money, bitcoin's real value lies in its algorithms," *InfoWorld*, January 12, 2014.
- "U. researchers develop Bitcoin prediction market," *Daily Princetonian*, January 5, 2014.
- "This Princeton professor is building a Bitcoin-inspired prediction market," *The Verge*, November 29, 2013
- "Montreal's Bitcoin Embassy bridges gap between digital currency and real world," *Montreal Gazette*, November 29, 2013.

- "Bitcoin online currency gets new job in web security," *New Scientist*, January 11, 2012.
- "Secure, verifiable voting: Cryptography, invisible ink, and other voting magic," *Imprint*, November 6, 2009.
- "Scantegrity: Voters Test New Transparent Voting System," *Huffington Post*, November 5, 2009.
- "Maryland Voters Test New Cryptographic Voting System," *Wired News*, November 4, 2009.
- "Voters try out new security system," *UW Daily Bulletin*, November 3, 2009.
- "E-voting system lets voters verify their ballots are counted," *Computerworld*, November 3, 2009.
- "First Test for Election Cryptography," *Technology Review*, November 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*, November 4, 2008.
- "Canadian voting machine technology enters American political scene," *CBC.ca*, October 28, 2008.
- "New Voter Counter System Uses Encrypted Codes, Invisible Ink," *Voice of America*, October 24, 2008.
- "A Really Secret Ballot," *The Economist*, October 22, 2008.
- "Class voting hacks prompt call for better audits," *MSNBC*, October 20, 2008.
- "Clean Elections," *Communications of the ACM*, October 2008.
- "Protecting Your Vote With Invisible Ink," *Discover Magazine*, October 2008.
- "Flawless Vote Counts," *Technology Review*, September/October 2008.
- "Shift Back to Paper Ballots Sparks Disagreement," *Morning Edition*, March 7, 2008.
- "Down for the Count," *ACM netWorker*, March 2008.
- "The future of voting IT," *Government Computer News*, March 10, 2008.
- "A Damaging Paper Chase In Voting," *Washington Post*, September 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)*, January 29, 2007.
- "Making Every E-vote Count," *IEEE Spectrum*, January 2007.

Concordia Promotional Activities

- Thinking Out Loud. "Bitcoin & Cryptocurrency," Podcast, Episode 14. 27 February 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
PhD, Post-Doctoral	UQAM
General Industry	KPMG, Deloitte, Morgan Stanley
Government	National Defence

Includes jobs while in program and first job after graduation

Post-Doctoral (Completed)

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

/F (Fall term), /W (Winter term), /S (Summer term)

PhD (Completed)

Name	Dates	Research Topic	Papers	Co-Supervisor
Shayan Eskandari	2017/F-2024/F	“The Hidden Layers of Blockchains: Technical Nuances and their Unforeseen Consequences”	C24, C27, C29, C32, C35, C37, C42, J09	
Didem Demirag	2018/W-2022/F	“Moving Multiparty Computation Forward for the Real World”	C33, J08, C40, C43, C47, J10	
Nan Yang	2014/S-2020/F	“Non-Local Contamination in Cryptography”	C28, C39	C. Crépeau (McGill)
Gaby Dagher	2013/F - 2015/F	“Toward secure and privacy-preserving data sharing and integration”	C26, J06	B. Fung (McGill)

Masters (Completed)

Name	Dates	Research Topic	Papers	Co-Supervisor
Sina Pilehchiha	2021/S-2022/F	“Improving Reproducibility in Smart Contract Research”		A.G. Aghdam (ECE)
Mahdi Nejadgholi	2019/F-2022/S	“Nullification, a coercion-resistance add-on for e-voting protocols”	C39, C46	
Mehdi Salehi	2020/W-2022/W	“An Analysis of Upgradeability, Oracles, and Stablecoins in the Ethereum Blockchain”	C41, C42, C45, C49	M. Mannan (CIISE)
Corentin Thomasset	2019/F-2020/S	“SERENIoT : Politiques de sécurité collaboratives pour maisons connectées”		D. Barrera (Carleton), J. Fernandez (Polytechnique)
Chidinma Okoye	2016/S - 2017/F	“New applications of blockchain technology to voting and lending”	C31	
Mahsa Moosavi	2015/F - 2018/W	“Rethinking Certificate Authorities: Understanding and decentralizing domain validation”	C30, C35, J08, C44, C49	
Michael Colburn	2014/F - 2018/S	“Short-Lived Signatures”		
Abhimanyu Khanna	2014/F - 2017/S	“Towards Usable and Fine-grained Security for HTTPS with Middleboxes”		M. Mannan (CIISE)
Shayan Eskandari	2013/F - 2016/W	“Real world deployability and usability of Bitcoin”	C24, C27, C29, C32, C35, C37, C42, J09	W. Hamou-Lhadj (ECE)

Post-Doctoral (In Progress)

Name	Dates	Research Topic	Papers	Co-Supervisor
Vathsan Morkonda	2024/W -	Usable security		

PhD (In Progress)

Name	Dates	Research Topic	Papers	Co-Supervisor
Nahid Rahman	2024/F-	Blockchain analytics		
Reza Rahimian	2018/F-	“Enhancing DeFi by improving ERC-20 Token Security and Addressing Leveraged Token Shortcomings”	C37, C50	

Name	Dates	Research Topic	Papers	Co-Supervisor
Mahsa Moosavi	2018/S-	“Navigating decentralized finance (DeFi) risks and challenges through user-centric solutions”	C30, C35, J08, C44, C49	
Pratyusha Bhattacharya	2017/S-	Smart Grid Security		M. Debbabi (CIISE)

Masters (In Progress)

Name	Dates	Research Topic	Papers	Co-Supervisor
Youwei Deng	2023/W-	Zero Knowledge Proofs		

Supervised Graduate Projects (ENGR 6991)

Year	Students
2025	Adrijeet Deb
2024	Arun Sankar
2023	Mohammad Zawad Tahmeed
2019	Abhinav Kumar
2018	Jinumol James, Laleh Alimadadi, Rupesh Gawde, Brindha Shree, Isreal Tei
2018	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
2024 W	INSE 6615: Blockchain Technology	89	1.41
2024 W	INSE 6150: Security Evaluation Methodologies	87	1.46
2023 F	INSE 6150: Security Evaluation Methodologies	118	1.16
2022/4	INSE 6615: Blockchain Technology	69	1.30
2022/4	INSE 6150: Security Evaluation Methodologies	100	1.48
2022/2	INSE 6150: Security Evaluation Methodologies	70	1.72
2021/4	INSE 6630: Recent Developments in Info. Systems Security	67	*Evaluations suspended (COVID)*
2021/4	INSE 6150: Security Evaluation Methodologies	68	
2021/2	INSE 6150: Security Evaluation Methodologies	49	
2020/1	INSE 6150: Security Evaluation Methodologies	78	
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

Year/Term	Course	Class Size	Evaluation
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).*
- */1 means summer term, /2 means fall term, /4 means winter term (of the following calendar year)*

Teaching Awards

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

External Lectures

- "Decentralized finance (DeFi)," Faculty of Law, University of Ottawa. 22 March 2021.
- "Improving usability and trust for moving Bitcoin adoption forward," MAS.S65 - Blockchain Technologies, Massachusetts Institute of Technology (MIT). Guest lecture, 4 November 2015.
- "History of cryptocurrencies," Bitcoin and Cryptocurrency Technologies, Princeton University. Guest lecture, Online: Coursera, recorded in September 2015.
- COMP 4109: Applied Cryptography, Carleton University. Course, Winter 2013.

Service to University

University Committees

Leaves: Parental 2019-2020; Sabbatical 2020-2021

Year	Committee
2024-	GCS EDI Award and Research Grant Committee
2024-	GCS Faculty Research Committee (FRC)
2023-	GCS Faculty Personnel and Tenure Committee (FPTC)
2023-	CIISE Curriculum Committee
2022-	GCS Elections Committee (Chair)
2021-2023	Concordia University Faculty Tribunal Pool
2021-2023	GCS Faculty Council
	Parental Leave and Sabbatical
2018-2019	Concordia University Faculty Tribunal Pool
2018-2019	ENCS Blended/Online Pedagogy Committee
2017-2019	ENCS Elections Committee
2013-2019	CIISE Seminar Committee
2014–2016	Concordia University Faculty Tribunal Pool

Graduate Student Committees (Concordia)

Year	Occurrences					
	MASc Defence	PhD Comp.	PhD Proposal	PhD Seminar	PhD Defence	Total
2025		1	1		2	4
2024	5	2	1	2	2	12
2023	5	1	2	1		9
2022	1	2	1	3	1	8
2021	3	1	1	1	1	7
2020	4	1		1	1	7
2013-2019	6	9	6	7	7	35

External Examiner

- Bofeng Pan, PhD, University of Saskatchewan, 2024
- Ghassan Al-Sumaidaee, PhD, McGill, 2024
- Alireza Arjmand Shakouri, Masters, University of Alberta, 2023
- Md Mamunur Rashid Akand, PhD, University of Calgary, 2023
- Farimah Ramezan Poursafaei, PhD, McGill, 2022
- Patrick McCorry, PhD, Newcastle University, UK, 2017
- Giulia Alberini, PhD, McGill, 2015
- Jérôme Dossogne, PhD, Université libre de Bruxelles, Belgium, 2015

Service to Academia

Program (Co-)Chair (Conferences)

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

General (Co-)Chair (Conferences)

Year	Conference
2024	Blockchain Technology Symposium (BTS)
2023	Blockchain Technology Symposium (BTS)
2020	Privacy Enhancing Technologies Symposium (PETS)

Advisory/Editorial Boards (Conferences/Journals)

Year	Journal
2019—2024	Privacy Enhancing Technologies Symposium (PETS)
2013—2015	USENIX Journal of Election Technologies (USENIX JETS)

Program Committees (Conferences)

Year(s)	Conference
2016—	Financial Cryptography and Data Security (FC)
2023—	ACM Computer and Communications Security (CCS): Blockchain Track
2025—	USENIX Security Symposium
2023—	Advances in Financial Technology (AFT)
2021—	International Joint Conference on Electronic Voting (E-VOTE-ID)

Year(s)	Conference
2021—	ACM CCS Workshop on Decentralized Finance and Security (DeFiSec)
2017—	ESORICS Workshop on Cryptocurrencies and Blockchain Technology (CBT)
2023—	Science of Blockchain Conference (SBC)
2025—	The Latest in DeFi Research (tldr)
2022—2024	FC Workshop on Decentralized Finance (DeFi)
2022	Workshop on Privacy in the Electronic Society (WPES)
2018—2021	IEEE Security & Privacy on the Blockchain (IEEE S&B)
2013—2018	FC Workshop on Bitcoin Research (BITCOIN)
2017—2018	APWG Symposium on Electronic Crime Research (eCrime)
2018	Symposium on Usable Privacy & Security (SOUPS)
2016	RSA Conference: Cryptographer's Track (CT-RSA)
2016	ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM)
2014	Annual Computer Security Applications Conference (ACSAC)

Reviewer: Journals (Most Recent Year)

Most Recent Year	Journal / Conference
2024	IEEE Transactions on Network and Service Management (TNSM)
2024	IEEE Transactions on Parallel and Distributed Systems (TPDS)
2024	IEEE Transactions on Network Science and Engineering (TNSE)
2023	IEEE Security and Privacy Magazine (S&P)
2022	IEEE Transactions on Information Forensics and Security (TIFS)
2021	Bank for International Settlements Working Paper Series (BIS WPS)
2021	IEEE Transactions on Dependable Secure Computing (TDSC)
2021	Communications of the ACM (CACM)

Reviewer: Funding Agencies (Most Recent Year)

Most Recent Year	Agency
2025	Natural Sciences and Engineering Research Council of Canada (NSERC)
2024	Social Sciences and Humanities Research Council of Canada (SSHRC)
2024	MITACS
2024	National Cybersecurity Consortium (NCC)
2024	Austrian Science Fund (FWF)
2023	Israel Science Foundation (ISF)
2023	Luxembourg National Research Fund (FNR)
2019	Fonds de Recherche du Québec – Nature et technologies (FRQNT)
2019	Alberta Innovates
2017	Office of the Privacy Commissioner of Canada (OPC)

Reviewer: Prizes (Most Recent Year)

Most Recent Year	Agency
2024	Bitcoin Research Prize, Chaincode Labs