The security and financial implications of blockchain technologies: Regulating emerging technologies in Canada

Evangeline Ducas
School of Public Policy and Administration, Carleton University, Ottawa, Ontario, Canada

Alex Wilner
Norman Paterson School of International Affairs, Carleton University, Ottawa, Ontario, Canada

Abstract
Driven by advances in data analytics, machine learning, and smart devices, financial technology is changing the way Canadians interact with the financial sector. The evolving landscape is further influenced by cryptocurrencies: non-fiat, decentralized digital payment systems, like Bitcoin, that operate outside the formal financial sector. While Bitcoin has garnered attention for facilitating criminal activity, including money laundering, terrorism financing, digital ransomware, weapons trafficking, and tax evasion, it is Bitcoin's underlying protocol, the blockchain, that represents an innovation capable of transforming financial services and challenging existing security, financial, and public safety regulations and policies. Canada's challenge is to find the right balance between oversight and innovation. Our paper examines these competing interests: we provide an overview of blockchain technologies, illustrate their potential in Canada and abroad, and examine the government's role in fostering innovation while concurrently bolstering regulations, maintaining public safety, and securing the integrity of financial systems.

Keywords
Blockchain, disruptive technology, money laundering, terrorism financing, financial regulation, cryptocurrency, Bitcoin
Introduction

Recent technological advancements in financial service delivery in Canada and abroad have elicited strong reactions and excitement from industry, government, and consumers alike. Canadians can now transact directly and cheaply through mobile phone applications, seek investment advice from near-autonomous online robo-advisors, and access seed funding for new business ventures from a variety of equity crowdfunding platforms. Advances in other industries, including data analytics, machine learning, and smart devices, have spurred further developments in these areas. While the link between finance and technology is nothing new, a surging interest in the use of technology to deliver financial solutions has resulted in a collective reimagining of the phenomenon, perhaps best captured by the increasingly popular portmanteau “fintech.” Many of the recent advancements in fintech appear to constitute a class of their own. As Douglas Arner and colleagues aptly illustrate, we have entered a new period of technological change across the global financial sector, driven as much by the unprecedented speed of innovation as by who is driving it.1 The emerging fintech era is characterized by the entrance of both agile start-ups and established tech giants, such as Apple and Facebook, which are competing with traditional financial institutions. In addition to providing new and at times innovative products and services, these changes in the financial sector landscape have pushed financial actors to revisit antiquated infrastructure, business practices, and priorities, spurring further innovation.2

Academic attention from various disciplines has been placed on better charting the novelty of these developments.3 Other work has gone towards understanding how emerging technology can best be approached from a regulatory perspective. Central to this discourse is Philip Cerny’s examination of how technological advancements have historically influenced financial regulation: technology drives financial globalization, impeding state control over these developments by increasing inter-jurisdictional decentralization.4 Other scholars, like Giselle Datz, have suggested instead that technological innovation (coupled with global economic integration) have forced some aspects of the traditional state, including centralized debt and asset management agencies, to evolve into private sector-like actors.5 Either way, rapid advancements in fintech evoke fresh concerns that contemporary technological developments are ushering in a new cycle of disruptive innovation, of economic boom and bust.6

6. Carlotta Perez, Technological Revolutions and Financial Capital (London: Elgar, 2002); D. Foray and C. Freeman, eds., Technology and the Wealth of Nations: The Dynamics of Constructed
Compounding these dynamics is the development of cryptocurrencies, non-fiat decentralized digital currencies and payment systems that operate at a global level, outside of the formal financial sector. While Bitcoin, the world’s first cryptocurrency, has garnered attention for facilitating criminal activity, including money laundering, terrorism financing, digital ransomware, weapons trafficking, and tax evasion, it is Bitcoin’s underlying protocol—the blockchain—that has the potential to alter and transform traditional financial services, and the security and financial regulations and policies that attend to them.\(^7\)

Canadian financial institutions and government actors are well-represented among blockchain proponents. In June 2016, for instance, the Bank of Canada partnered with Payments Canada, the owner and operator of Canada’s national payment-clearing and settlement infrastructure, along with several banks and the R3 consortium of financial institutions, to test the feasibility of using blockchain to undergird Canada’s interbank payment system, which clears more than $175 billion a day.\(^8\) Soon after, three Canadian financial institutions—the National Bank of Canada, Canadian Imperial Bank of Commerce, and ATB Financial—enlisted the services of San Francisco-based Ripple Labs to integrate blockchain technology into their respective business practices.\(^9\)

Despite interest among financial actors to develop and apply blockchain technologies to their products and services, Canada has yet to fully develop a coordinated regulatory strategy for the successful and safe implementation of these systems. And while the development of such a strategy is imperative, the policy and regulatory challenge is significant, requiring the right balance between oversight and innovation. Potentially disruptive technologies—blockchain included—necessitate a careful regulatory approach in order to safeguard existing financial systems and meet security prerequisites. But over-burdening emerging technologies in cumbersome regulatory frameworks risks undermining the benefits of innovation altogether. Our paper teases apart these competing interests—between security, stability, policy, and technological innovation. Until recently, International Relations (IR) scholarship has largely overlooked and under-theorized the relationship between technology, global affairs, and political behaviour. Stefan Fritsch has shown, for instance, that the core paradigms of IR scholarship treat technology as a passive or exogenous factor to systemic change,


\(^8\) While the Bank of Canada found that integrating blockchain into Canada’s interbank payment system could not yet meet all the “core international principles for financial market infrastructure,” the study suggested that as the technology evolves, so too would its applications. C. Wilkins and G. Gaetz, “Could DLT underpin an entire wholesale payment system?” The Globe and Mail, 25 May 2017.

state power, identity, and political behaviour. Our goal is to provide an empirically driven and practically oriented guide for Canadian policymakers that will serve to inform these larger, ongoing theoretical debates within IR. What opportunities, challenges, and threats do blockchain technologies present to Canadians? How might these technologies be properly regulated in keeping with evolving security environments and demands? What regulatory strategy provides Canadians with enough oversight, but leaves room for continued innovation, development, and application?

Canadian regulators and government decision-makers have only begun to explore these questions in earnest, despite the fact that a robust financial sector is crucial to Canada’s economic security. While Canada is seen as a world leader in financial regulation, partly as a result of having suffered relatively little harm during the 2008 global financial and 2011 European debt crises, it is now at risk of lagging behind other international jurisdictions who appear more willing and better able to simultaneously regulate and foster technological innovation in blockchain. Furthermore, the Canadian academic literature on the subject, from within IR at least, is nearly non-existent. Canadians of all stripes have much thinking to do. Relying on private and public-sector documents, media reports, academic literature, and a set of interviews, we explore the nexus between blockchain, security, and policy in Canada.

Our argument has five sections. First, we begin by tracing the emergence of contemporary fintech, situating blockchain technologies within the broader phenomenon. Next, we provide a technical overview of blockchain, relating these technologies to the financial sector and illustrating their potential in Canada and abroad. Third, we examine the Canadian government’s role in both fostering financial sector innovation and maintaining the safety and integrity of the financial system. Fourth, we explore the various regulatory considerations for blockchain technologies, including those relating to anti-money laundering and anti-terrorist financing (AML/ATF). Finally, we explore competing regulatory approaches common to a number of international jurisdictions, concluding that the regulatory “sandbox” model—a facilitative approach to fintech that eases regulations in the testing, development, and partial delivery to the public of new technologies—provides the most suitable approach to regulating blockchain technologies within the Canadian context.


Fintech in the current era

From the laying of the first transatlantic cable in 1866 to the introduction of the automatic teller machine in 1967, financial infrastructure has long been shaped by technological advancements. Indeed, the financial services industry has been the largest global purchaser of information technology products and services since the mid-1990s. Global interest and investment in fintech has skyrocketed in recent years, growing by 75 percent between 2010 and 2015, to $22.3 billion USD.

Contemporary fintech has emerged from a confluence of factors, including rising consumer expectations, rapid technological advancements, and both growing consumer mistrust of financial institutions and increased regulatory scrutiny in the post-2008 financial crisis era. Within this shifting landscape, traditional financial institutions are spurred to innovate as they face increasing pressure to remain relevant and profitable. In addition to directly competing with banks, and increasingly partnering with or being acquired by banks, fintech start-ups and established technology firms are altering financial services through their capacity to attract capital and talent, and to pre-select the areas of financial service provision that best leverage their business models and loyal customers. This has resulted in a financial sector landscape fractured by fintech product and service offerings.

These changes within the financial operating environment pose unique challenges to both financial regulators and market participants alike. While traditional financial institutions and regulators have a history of working together within well-established regulatory parameters, fintech firms have had much less interaction with the financial regulatory system. This has resulted in a proliferation of financial products and services across the industry that do not fit squarely within existing regulatory frameworks, or that have failed to fulfill basic compliance requirements or consumer protection obligations. Not only do fintech upstarts appear at times ignorant of the laws and regulations that uphold the financial system, but some firms have expressed a belief that as innovators they should not be held to the same regulatory scrutiny as their traditional financial sector counterparts. Kevin Sandhu, chief executive of Vancouver-based fintech consumer lender Grow, has aptly summarized this sentiment: “[f]intechs, by definition, are different than the incumbents, and as a result, they present different points of exposure and risk. . . . Saying that the same regulations that apply to large, multi-national banks should apply to smaller, nimbler, and niche fintech companies is effectively forcing a square peg into a round hole.”

While emerging fintech has undoubtedly complicated the contemporary regulatory environment in Canada and abroad, many of these innovations, such as peer-to-peer lending, have been recognized by Canadian regulators, including the Bank of Canada, as the next step in the progression of technological development across the financial sector. In these cases, the main regulatory concerns regarding consumer protection, market integrity, money laundering, and terrorism financing are seen as having remained largely consistent and well-managed under existing regulatory paradigms. Blockchain technologies, however, have demonstrated the potential to upend entire industries, disintermediate traditional financial institutions, and pose regulatory and policy concerns related to governance, legal environments, financial stability—and, in some cases, criminal investigation, financial intelligence, and counterterrorism financing measures. And unlike other fintech innovations, blockchain technologies have led to the development of new products and services well beyond the financial sector; they have demonstrated their potential to improve medical record keeping and land title registration, the administration of humanitarian aid and supply chain management, asset tracking and registration, and decentralized voting and governance. Blockchain technologies further facilitate the creation of “decentralized autonomous organizations”—entities able to cooperate with one another, and trade and provide services, based on the collective trust encoded in a blockchain. Nonetheless, it is within the financial services sector that blockchain technologies have shown some of the most disruptive potential to date. Non-financial start-ups and tech firms have established a foothold among incumbent financial firms by developing and launching their own proprietary blockchain systems, which allow them to establish next-generation payment provisions, loyalty and rewards platforms, smart contracts, asset management processes, and exchange platforms. Yet, beyond challenging existing products, services, and industry frameworks, the true potential of blockchain technologies is their capacity to enable open-source distributed consensus. And while these systems may present innumerable opportunities to industry and government, they also threaten those unable to respond to their development, fundamentally challenging conventional approaches to financial sector regulation. What follows is a technical exploration of blockchain.

What is blockchain?

The conceptual origins of blockchain technology can be traced back to the release of a 2008 white paper to a cryptography mailing list by an individual, or group of individuals, operating under the pseudonym Satoshi Nakamoto. The paper proposed the design of a purely peer-to-peer (P2P) electronic version of cash, capable of eliminating the need for central authorities and intermediaries in the payments system. Nakamoto’s treatise is regarded as the genesis of the open-source Bitcoin software released in 2009. Following significant adoption in recent years, Bitcoin is currently regarded as both a digital currency and a payments infrastructure.21 Its strength, according to Nakamoto, is its ability to circumvent “the weaknesses of the trust based model” inherent to all traditional financial systems. Moreover, the cryptocurrency’s underlying protocol—the set of rules and processes that govern interactions within the system—provides a solution to the financial sector’s inability to conduct irreversible transactions, while eliminating the high mediation and transaction costs that come with requiring the services of financial intermediaries, as well as the possibility of financial fraud.22

Blockchain is best understood as a digital distributed ledger used to record and share information throughout a peer-to-peer network (see Figure 1). Identical copies of the ledger are maintained and collectively validated by network members, with accepted information aggregated into “blocks,” which are added to a

---


chronological “chain” of existing, previously validated blocks, using a crypto-
graphic signature. Each new block is timestamped—a process of digitally encoding
time that corresponds to the creation of new and immutable data—and contains
information referencing the block that preceded it, ensuring that any attempt to
tamper with the blockchain would require the alteration of every block previously
created, a near-impossibility given the decentralized nature of the technology.
Importantly, blockchain has surpassed its Bitcoin origin. Among its many attri-
butes, the technology is perhaps most remarkable for its ability to ensure digital
authenticity without third-party intervention, ultimately ensuring “trust” through
cryptographic proof in inherently trust-less environments. The technology is also
both highly secure and resilient, employing public key cryptography—a form of
algorithmic encryption which makes it impossible to corrupt the blockchain—to
protect value transfer and ownership, and decentralized networks, to ensure that
each system is devoid of central points of trust or failure. Furthermore, block-
chain can be highly efficient, enabling peers to transfer value directly to one another
without intermediaries, permitting quick and low-cost transmission of information
and value across vast networks. Finally, the technology is transparent, providing
an immutable record of all transactions that have ever occurred on the protocol’s
distributed ledger.

Types of blockchains

Blockchain technology has evolved over time through the creation of new and
diverse systems, each serving specific functions through the incorporation of per-
missions, rules, smart contracts, digital signatures, and various other features. These
disparate blockchains can be categorized by the openness of their networks
and the nature of their validation process, with each blockchain type exhibiting
unique features and vulnerabilities which elicit very different regulatory and secur-
ity considerations. Blockchains can thus either be public, where the abilities to both
read and submit transactions for inclusion in the blockchain are unrestricted, or
private, where these abilities are limited to predetermined individuals or entities.
While all information recorded on the blockchain is universally accessible in a
public system, pseudonyms are assigned to network participants, which enhances
privacy but obscures identity. Conversely, in private systems, user identification is
central to system use and can be required to conform to certain specifications, such
as traditional know-your-customer (KYC) regulatory obligations. These design
features have rendered private blockchains more congruent with the existing

financial system, leading to significant interest and investment in these systems across the financial sector.\textsuperscript{27}

Blockchains can be \textit{permissionless}, where participation in the network consensus process is open to any individual or entity with the technical capacity to validate and add transactions to the network, or \textit{permissioned}, where this process is limited to known entities (see Figure 2). In the absence of a centralized authority, blockchains are secured through cryptographic verification. This verification process can be costly; it hinges on expending computational processing power to solve complex cryptographic problems, often in the form of “proof-of-work” processes.\textsuperscript{28} In the case of permissionless systems, members are incentivized to engage in this computational process through the promise of an economic reward: a cryptocurrency is issued to network members who successfully create a new validated block. Examples of these systems include Bitcoin and the hundreds of alternative cryptocurrencies—or “altcoins”—like Ethereum, Litecoin, and more recent iterations that provide enhanced user anonymity, such as Monero, Dash, and Zcash. Alternatively, no incentive structure (i.e. cryptocurrency issuance) is required to maintain a permissioned blockchain: pre-selected actors in the network, such as a consortium of financial institutions or a group of government departments, are simply tasked to verify and validate the data. These systems are considered partially decentralized, as network participation is limited to known actors.


In addition to recording information and data, the algorithmic technology underlying blockchain can be used to verify or enforce contractual agreements using “smart contracts,” which encode traditional contractual terms into a computer program and execute them automatically. Coupled with blockchain technology, smart contracts bypass the need for traditional intermediaries with the ability to self-execute, self-enforce, self-verify, and self-constrain the performance of a contract (see Figure 3). This technology is lauded for its ability to facilitate automation and eliminate manual processes; increase speed, efficiency, and trust in contractual enforcement; reduce the risk of moral hazard (e.g., strategic default); and reduce verification and enforcement costs. By automating the movement of pre-determined assets under certain conditions, blockchain-enabled smart contracts can be employed across the financial sector, including in securities, syndicated lending, trade finance, swaps, derivatives and other complex financial products. For example, smart contracts could execute payments with complex terms and conditions, such as those found in many financial derivatives contingent on external events and price fluctuations.

**Blockchain applications in the financial sector**

Financial sector interest in blockchain technologies has been largely limited to private permissioned systems. Owing to the security concerns associated with public permissionless networks—which are open to honest and malicious actors

---

alike—permissioned systems are more easily scalable, and allow financial actors to reap benefits from blockchain technology while maintaining control over internal operations and complying with existing regulations, including KYC, anti-money laundering, and anti-terrorist financing requirements. To date, financial industry actors have identified two dozen uses for blockchain, the most promising of which include:

- **Payment processing**: Contemporary payment processing systems are cumbersome, often involving multiple intermediaries, customer fees, and lengthy reconciliation tasks. Blockchain technology could enable financial institutions to connect directly to each other, ultimately shortening settlement periods, decreasing the cost of cross-border transactions, speeding up transactions, and reducing the risk of fraud.\(^{32}\)

- **Post-trade settlement (e.g. corporate loans, credit default swaps, derivatives)**: Blockchain technology could solve cluttered post-trade settlement processes by providing enhanced audit and regulatory functions, as information is more easily tracked and visible by all parties, enhancing resolution management capabilities. The technology further provides opportunities to greatly shorten post-trade settlement periods from the current standard of *trade date plus three days* (*T+3*), to near instantaneous settlement.\(^{33}\) Blockchain may be particularly useful for assets that have the least efficient netting, clearing, and collateral management, and the longest clearing periods.\(^{34}\)

- **Securities issuance and servicing**: Blockchain technologies provide an alternative to inefficient and, at times, inaccurate manual processes of issuing and exchanging shares in private companies, by providing a permanent digital record of securities transfer among private users. This will improve accounting, auditing, and regulatory supervision functions while increasing transparency of ownership.\(^{35}\)

- **Trade finance**: The contemporary trade finance system must ensure that goods have transferred before payment is made. The real-time visibility of data enabled

---

32. Several Canadian banks are implementing this technology. Oscar Williams-Grut, “Santander is experimenting with Bitcoin and close to investing in a blockchain startup,” *Business Insider UK*, 17 June 2015.


by blockchain technologies ensures that all parties, including financiers, trading houses, and other intermediaries, are able to witness when goods have shipped and can release funds accordingly.\textsuperscript{36}

- **Regulatory compliance**: Blockchain technology could automate regulatory compliance requirements, such as KYC processes, reducing compliance errors. While the technology is commonly associated with pseudo-anonymity, the technology can be used to connect real-world identities to cryptographic identities in a database. Implementation of these systems—such as blockchain-based identification registries—would not only remove duplication efforts in carrying out identification processes across institutions, but could also enable encrypted updates of client details to be distributed to trusted blockchain network members in near real-time.\textsuperscript{37}

As these various applications highlight, the financial services sector has recognized the potential of blockchain technologies to provide enhanced speed, security, transparency, efficiency, cost-savings, and accuracy across multiple business lines. These prospective gains have led to aggressive investment in the technology, with financial institutions expected to spend over $1 billion USD on blockchain-related projects in 2017 alone.\textsuperscript{38} As noted, Canadian banks are experimenting with these technologies: in June 2016, for example, Alberta-based ATB Financial conducted the first international money transfer using blockchain technology in partnership with Germany’s ReiseBank and Ripple Labs.\textsuperscript{39} Canadian membership has also been significant in many of the blockchain consortiums pervasive across the industry, including R3 CEV, a group of over 80 of the world’s largest financial institutions leading the financial market’s foray into blockchain.\textsuperscript{40}

Despite clear private-sector interest in the technology, there are several factors preventing widespread adoption of blockchain technologies across the formal financial system in their current form. Most notably, the scalability of the original Bitcoin blockchain—its capacity to grow and accommodate more interactions—is not promising. For instance, only a limited number of simultaneous transactions can be written into the blockchain at any given time. There is a gap, too, between the period in which new additions to the ledger are made and later confirmed into blocks. Further, there is a significant cost associated with running public permissionless blockchains, like that supporting Bitcoin, in terms of network bandwidth,

\textsuperscript{36} The first international trade transaction between two independent banks using blockchain technology was conducted in October 2016, involving a shipment of cotton from Texas, USA, to Qingdao, China. World Economic Forum, “The future of financial infrastructure,” August 2016, 21; Morgan Stanley, “Global insight,” 6; Byron Kaye, “Major banks mark first-ever international trade using blockchain tech,” Reuters, 24 October 2016.

\textsuperscript{37} Several companies, including I/O Digital, ShoCard, and others, have created systems enabling businesses to add encrypted client documents and identity information to a blockchain. Goldman Sachs, “Profiles in innovation,” 24 May 2016, 74; Deloitte UK, “Blockchain applications in banking,” 1.


\textsuperscript{39} Jane Wild, “Ones to watch: The rise of online-only money,” Financial Times, 2 November 2016.

storage, and processing power. Moreover, as new and untested technologies, both permissioned and permissionless blockchains elicit concerns regarding business continuity and data preservation in the medium- to long-run by businesses employing these technologies.\(^{41}\) As a result, new blockchain iterations are emerging to address these issues, which tend to incorporate permissioned networks, increasingly centralized systems, and varying block sizes.\(^{42}\) While the widespread adoption of blockchain across the financial sector is far from certain, the technology clearly has the potential to alter financial sector infrastructure and reform the manner in which financial institutions interact with clients and regulators alike. This nascent stage of blockchain development represents a pivotal opportunity for governments and regulators to engage proactively with industry stakeholders to help shape the future development of this technology, while minimizing identifiable risks to public safety and financial stability and maximizing national economic benefit.

### Canadian fintech: Promises and pitfalls

Governments across the globe have identified the fostering of innovation as a critical economic priority. Promoting fintech, in particular, is viewed as a mechanism able to tackle a variety of public policy issues, including increasing household financial health, providing small and medium enterprises with improved access to financing, improving cybersecurity in the formal financial sector, and enhancing financial inclusion in developing economies.\(^{43}\) Given its potential application across and beyond the financial sector, blockchain is being actively developed and promoted in the United Kingdom, the United States, China, Switzerland, Singapore, and a growing list of other countries. However, blockchain technologies butt against a range of other economic and security imperatives. Governments are tasked with identifying the appropriate balance between fostering innovation and safeguarding security. In Canada, these dual priorities are evident. What follows is an exploration of both.

Encouraging innovation is a priority for Canada, where the financial sector holds particularly significant economic importance, directly accounting for nearly 800,000 jobs and 7.0 percent of gross domestic product.\(^{44}\) Given the pace of financial sector transformation, continued Canadian innovation across the industry will be critical to remaining internationally competitive and to achieving levels of productivity required for economic growth.\(^{45}\) For illustration, according to the Digital Finance Institute,

---


\(^{43}\) Adrienne Harris, “The future of finance is now,” The White House Blog, 10 June 2016.


a Vancouver-based fintech think tank, fostering a Canadian fintech ecosystem could contribute to continued Canadian leadership in the global financial sector, attract international investment in Canadian technology, build local talent pools, create employment opportunities to offset losses in disrupted sectors, and open trade opportunities to export fintech talent, products, and services.46

Current Canadian initiatives to achieve these ends include the federal government’s Innovation Agenda and the Competition Bureau’s Fintech Market Study, examining innovation in the domestic financial services sector, both launched in 2016. Led by the minister of innovation, science and economic development, the Innovation Agenda’s commitment to “compete in a digital world” provides Canadian fintech companies a competitive boost in the digital economy, while supporting innovation across the sector.47 Other federal activities related to fintech development are being pursued elsewhere. For example, the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), the Canadian financial intelligence unit and AML/ATF regulator, conducts research on and monitors fintech activities. Other members of Canada’s security and intelligence community, notably the Royal Canadian Mounted Police and Communications Security Establishment, are similarly exploring how fintech and blockchain technologies relate to their investigative and intelligence mandates and capabilities.48 The Department of Finance is exploring P2P payments regulation and public policy, and the Bank of Canada is conducting fintech research and experimenting with blockchain technology.

Despite these early efforts, however, Canadian fintech stakeholders have been vocal about hurdles to domestic market development, with certain high-profile firms dismantling local activities in favour of operating in more permissive regulatory jurisdictions overseas. Most notably, Ethereum, a blockchain-based platform largely conceived by Canadians living in Canada, moved its operations to Switzerland, partly because of the difficulty it had working within Canada.49 In this vein, Canadian fintech firms have signalled frustration with a complex and poorly defined regulatory environment. Prominent financial regulators, including the Department of Finance, FINTRAC and the federal prudential regulator, the Office of the Superintendent of Financial Institutions, have been reticent to clearly define the regulatory treatment of all fintech entrants, particularly with regards to their classification as money services businesses (MSBs).50 This regulatory uncertainty may limit the

49. Alex Wilner, open-ended interview on Canadian and international regulations and blockchain innovation, with Dr. Ethan Wilding, resident philosopher, Ethereum, 12 May 2016.
50. Willms, “Canadian banks experiment.”
ability of fintech firms to solicit venture capital and investment needed to fuel their
growth, and, given potential money-laundering concerns, slow their establishment of
traditional banking relationships with financial institutions.51

Notwithstanding current market impediments, Canada is uniquely placed to
become a global fintech leader. First and foremost, Canada is globally renowned
for its strong and stable financial system, which has achieved successive rankings as
the soundest in the world. It is composed of both major banks that have long
championed consumer-focused financial service delivery, and a rapidly expanding
fintech sector offering Canadians options that are convenient, cost-effective, and
tailored to their needs. These factors are reinforced by business-friendly policy and
regulatory environments, leading Canada to be recognized by the World Bank
Group as the third best economy worldwide in which to start a business, and
fourteenth for overall ease of doing business.52 Canada is additionally well-
placed geographically, with access to investors and business opportunities in the
United States, Europe, and Asia.

Canadian strengths in the blockchain field are equally numerous. Home to
strong tech and cybersecurity sectors, Canada has the infrastructure and talent
needed to support homegrown blockchain development and applications. Leading university programs in computer engineering and quantum computing
have produced a generation of young Canadians driven towards innovation.
Furthermore, several of the world’s leading blockchain firms, including
Ethereum and ConsenSys, were developed or founded in Canada, providing experience and expertise to individuals who have since gone on to found new Canadian
blockchain initiatives.53 These factors have contributed to a growing number of
innovative Canadian start-ups offering blockchain products and services, fostering
a growing and vibrant Canadian blockchain ecosystem.

The Canadian regulatory landscape

The success of blockchain technology in Canada will ultimately rely on the wider
legislative and regulatory environment in which it develops. Similar to approaches
undertaken in other international jurisdictions, the Canadian legislative and regul-
atory approach to blockchain and related emerging technologies has predomin-
antly focused on cryptocurrencies, such as Bitcoin, and has largely attempted to
treat these technologies with pre-existing statutes and regulatory frameworks.54

51. Arner et al., “Evolution of fintech”; Christine Duhaime, “FinTechs are being derisked out of bank
accounts over terrorist financing and money laundering risks say UK study,” Duhaime’s Anti–
Money Laundering Law in Canada, 29 May 2016; Willms, “Canadian banks experiment.”
52. World Economic Forum, “Global Competitiveness report 2014–2015,” 147; World Bank Group,
53. Alex Tapscott, “Blockchain is a disruption we simply have to embrace,” The Globe and Mail,
9 May 2016.
2015), 17; Kiviat, “Beyond Bitcoin,” 589; Lawrence Trautman, “Is disruptive blockchain technol-
This approach has resulted in a multifaceted regime with overlapping levels of regulation between federal, provincial, and territorial governments, with different regulatory bodies responsible for different components of the financial system.

Given the inherent interlinkage of cryptocurrencies and blockchain, the regulatory treatment of these virtual currencies can be extrapolated to inform our understanding of the policy landscape relevant to this nascent technology. Cryptocurrencies are neither regarded as currency nor money in a legal sense in Canada, and are thus exempt from regulatory oversight by any government or central authority, such as the Bank of Canada. Nor are cryptocurrencies covered by deposit insurance, or subject to consumer protection measures. However, they are treated as commodities by the Canada Revenue Agency, and as such are subject to the barter rules of the *Income Tax Act*. The treatment of cryptocurrencies as securities, particularly in conjunction with smart contract technologies, is not entirely evident, and will require future clarity from provincial and territorial securities regulators.

The introduction of concrete measures to regulate business facilitating cryptocurrency transactions occurred in 2014 with amendments to Canadian federal AML legislation, the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*. In recognition of the strong possibility that emerging technologies could be abused for money laundering and terrorist financing purposes, these amendments were introduced to enhance FINTRAC’s ability to disclose to federal partners threats to Canada’s security relevant to the use of virtual and cryptocurrencies in criminal activity. These specific changes included an expanded definition of MSB to include persons engaged in the business of “dealing in virtual currencies.” The precise meaning of “dealing in virtual currencies,” however, has not yet been determined and is currently being developed by the federal Department of Finance.

Depending on the activities undertaken, businesses or other entities employing blockchain technologies may be subject to other federal, provincial, or territorial legislation related to trade and commerce in Canada more generally. This includes the federal *Competition Act*, which incorporates consumer protection provisions, such as requirements that companies refrain from deceptive marketing practices. Additional consumer protection legislation has been enacted at the provincial and territorial levels, such as the British Columbia *Business Practices and Consumer Protection Act*, and the Ontario *Consumer Protection Act*, which are applicable to

fintech companies operating in those jurisdictions. Companies employing blockchain may also be subject to provincial, territorial, and federal privacy legislation, such as the Personal Information Protection and Electronic Documents Act, which regulates how private sector companies collect, organize, and use private and personal information in their commercial activities. A Canadian business employing blockchain technology is therefore required to answer to a complex network of regulatory bodies located across various levels of government, demanding that it employ a comprehensive approach to regulatory compliance and seek costly regulatory counsel to help navigate this complicated environment.

Regardless of the complexity of the current regulatory landscape, the Canadian approach is perceived to be largely permissive of cryptocurrency and blockchain technology use and development when compared with other jurisdictions worldwide. There is reason to believe that the overall sentiment across Canadian governments regarding these technologies is fairly positive and reflective of the potential opportunities they present. This is evidenced by the research and experimentation in blockchain and fintech undertaken by the Bank of Canada, as well as calls for a "light regulatory touch" for blockchain by the Senate Standing Committee on Banking, Trade and Commerce.

Regulatory considerations for blockchain technologies

The development of a coordinated regulatory framework for blockchain technologies in Canada has significantly lagged behind market innovation. This delay is neither unprecedented within the greater context of regulating emerging technologies, nor necessarily detrimental to efficient market regulation. The wait-and-see approach has allowed Canadian policymakers and regulators to remain neutral as markets dictate whether and where these technologies will achieve significant adoption, and to draw on observable data to inform a deeper understanding of the risks created over time. This reactive regulatory approach can even facilitate technological innovation, allowing regulators to better understand the technical fundamentals of these new technologies, as well as the benefits and applicability of their uptake, prior to regulatory intervention.

However, in addition to subjecting market participants to regulatory uncertainty, allowing blockchain technologies to develop unchecked by coordinated regulatory measures introduces a host of risks that potentially threaten the safety and stability of the Canadian financial system. The threat is multifaceted, given the diversity of the contemporary blockchain ecosystem and the risks posed by each

variant of blockchain technology. For example, the transaction pseudonymity provided by public permissionless blockchains, such as Bitcoin, presents several operational and legal risks, and may be particularly vulnerable to money laundering, terrorism financing, fraud, and other financial crimes. Private permissioned blockchains may pose fewer risks to the integrity of the financial system, given their relative alignment with existing regulations and financial sector business models. What follows is an exploration of the specific risks posed by blockchain technologies.

**Money laundering, terrorist financing, and other criminal activity**

Blockchain technologies, particularly public permissionless systems, can be abused for illicit purposes. This is primarily a result of their ability to facilitate pseudonymous—and in some cases fully anonymous—cryptocurrency transactions across international borders quickly and without third-party oversight or intervention. Lacking the strict governance structures of traditional fiat payment systems, permissionless blockchains are unable to impose any obligation on users to verify user identity or cross-check watch-lists or embargoed countries. These characteristics may facilitate crimes like terrorism financing, weapons trafficking, ransomware, and tax evasion, and have elicited strong regulatory concern from AML/ATF regulators in Canada and abroad. The association between cryptocurrencies and illegal activities is further augmented by the exclusive use of these currencies across illegal online services and marketplaces accessed through an encrypted layer of the Internet, the so-called “dark net.” This dark net cryptocurrency standard is largely credited to the infamous Silk Road marketplace, known as much for retailing illegal drugs as for the dramatic takedown of its founder, Ross Ulbricht, aka “Dread Pirate Roberts,” by the Federal Bureau of Investigation (FBI) in 2013 after nearly three years of operation. Following Silk Road’s demise, countless dark net markets have subsequently emerged to facilitate the purchase of illegal goods, including controlled substances and narcotics, child exploitation materials, fake passports, weapons, and other nefarious goods and services. This dark net ecosystem additionally supports a host of privacy enhancing tools known as “tumblers” or “mixers,” which can obscure value ownership and transaction histories on blockchain ledgers, rendering them highly vulnerable to abuse for money

---

laundering and other forms of financial crime. Despite these risks, however, there is growing interest in private permissioned blockchain systems which raise fewer regulatory concerns because they are employed in closed systems administered by regulated entities, such as financial institutions, with long histories of KYC process implementation and compliance with existing regulatory obligations.

**Consumer protection**

To date, public permissionless blockchains have offered little by way of consumer protection. In various instances, cryptocurrency users have been subject to scams, theft, or other fraudulent operations when interacting with non-regulated system intermediaries, such as cryptocurrency exchanges or hosted wallet providers. Consumer vulnerability to exploitation is further enhanced due to the irreversibility of transactions under blockchain protocols. Due to both the limited regulation of cryptocurrency intermediaries, as well as the decentralized governance structure of these systems, victims have been left with little avenue for legal recourse. These risks, however, are again minimized under private permissioned systems employed by regulated entities familiar with prevailing consumer protection obligations.

**Macroeconomic and monetary policy considerations**

As both currencies and payments infrastructures, public permissionless blockchains have received significant attention from central banking authorities worldwide. While assessments have demonstrated that cryptocurrencies fail to satisfy full requirements of “money” from an economic perspective due to their high price volatility and low acceptance rate—and thus pose little threat to national monetary stability in their current form—concerns have been raised that future iterations of cryptocurrencies might yet influence national monetary policy objectives. Should new generations of cryptocurrencies achieve systemically significant uptake, subsequent effects on the demand for cash across jurisdictions could substantially impact the ability of central banks to conduct effective monetary and macroeconomic policy. Developments of public permissionless blockchain systems thus require long-term monitoring by governments and central banks. These risks are, however, largely absent under private permissioned blockchain systems which fail to exhibit a native cryptocurrency.

Financial stability considerations

The use of blockchain technologies poses several regulatory and policy considerations regarding systemic financial stability. Due to the interoperability of legacy financial systems, widespread acceptance of these technologies in any one area of the financial sector could drastically affect a wide range of interconnected financial markets and infrastructures, including payment systems, stock exchanges, central securities depositories, securities settlement systems, trade repositories, and others.\textsuperscript{70} The interdependence of existing financial systems suggests that issues arising in any one area of the larger ecosystem could result in the transmission of risk to other financial market infrastructures, leading to systemic damage at national and even international scales. These risks are further enhanced given the technological complexity of blockchain systems, including the use of strong encryption, decentralized governance structures, and status as software. Should widespread implementation of these systems occur, the International Monetary Fund (IMF) warns, scenarios where blockchain technologies become simultaneously ‘‘too big to fail,’’ yet too complex to resolve, could potentially occur.\textsuperscript{71}

Importance of standardization and international regulatory coordination

As distributed, decentralized networks, blockchain technologies—particularly public permissionless systems—are inherently borderless. Capable of being both hosted in multiple jurisdictions simultaneously, and of facilitating rapid cross-border transactions, blockchain technologies are highly vulnerable to regulatory arbitrage, whereby participatory nodes become concentrated in jurisdictions with loose regulatory controls.\textsuperscript{72} Given the inefficiency of jurisdiction-specific regulation, the effective mitigation of blockchain-related risks will ultimately require international cooperation amongst relevant authorities, as well as the establishment of universally acknowledged regulatory principles.

Regulatory sandbox model: A balanced approach to blockchain regulation?

Developing a regulatory framework for entities and businesses employing blockchain technologies in Canada’s financial sector will require a delicate approach. Policies must be sensitive to the evolving needs of the community of innovators, and strike an appropriate balance between addressing risks and abuses while avoiding regulatory measures that stifle innovation altogether. Policies must likewise be coordinated across a vast and complex network of regulatory authorities at the

\textsuperscript{70} IMF, “Virtual currencies,” 32.
\textsuperscript{72} Peters et al., “Trends in crypto-currencies,” 23.
federal, provincial, territorial, and even international levels. As the pace of blockchain and fintech innovation and application quickens, governments may no longer be able to depend on top-down approaches to regulation, but will need instead to be flexible and open to collaborative regulatory approaches involving the private sector and civil society. States and jurisdictions agile enough to meet these challenges will be rewarded with economic growth in blockchain industries and protection from potential risks and threats.

To date, no single regulatory approach to blockchain technologies and cryptocurrencies has garnered widespread endorsement. While Russia, Thailand, and China have attempted to institute a “restrictive” approach to these technologies by banning or limiting cryptocurrency use, these efforts have been largely unsuccessful or have been subsequently reversed.73 A majority of other jurisdictions, including Canada, have assumed a “watchful” approach, whereby potential risks and opportunities are carefully weighed against observable market activity. Still other states have assumed a “facilitative” approach, choosing to actively regulate blockchain technologies in order to both capitalize on potential opportunities that emerge, while minimizing identified risks. States within this cluster are largely regarded as fintech leaders.74

Facilitative approaches to fintech have largely emerged in the form of “regulatory sandboxes” in places like Australia, Singapore, Switzerland, Malaysia, Hong Kong, Indonesia, Thailand, and the United Kingdom. As a regulatory approach, laws and regulations are temporarily relaxed or suspended with respect to certain business activities in order to facilitate innovative approaches to products, services, and business models.75 Within the sandbox framework, businesses employing innovative technologies provide services and products to a limited consumer base within a pre-established threshold of limitations, insofar as they operate in a responsible manner with regards to established AML/ATF, sanctions, privacy, and consumer protection obligations. While the sandbox environment cannot remove all risk, appropriate safeguards are implemented to contain the consequences of any failure, maintaining the overall integrity of the larger financial system.76

73. European Securities Market Authority, “Regulation and DLT,” 2; Guadamuz and Marsden, “Blockchains and bitcoin.”
The regulatory sandbox model provides a high degree of regulatory guidance and clarity. Proponents suggest that it creates the requisite parameters in which emerging fintech firms can reduce time-to-market at potentially lower costs, gain better access to investor financing, and develop more innovative products.77 Firms are also vigorously pre-vetted by regulatory entities before they are accepted into the sandbox program. This makes participating firms strong candidates for partnership and investment, attractive to venture capitalists, investors, and established financial institutions looking to acquire innovative competitors, which leads to greater overall levels of investment in the wider economy.78 The sandbox model also provides consumers with access to a range of products and services at lower cost. Regulators, too, benefit. They are provided with an opportunity to interact with market participants, acquiring a better understanding of the risks and opportunities associated with new business models. This early contact between innovators and regulators creates further channels through which other developments and initiatives can be shaped by regulators and other relevant authorities. For instance, regulatory sandboxes provide venues in which regulators can ensure that appropriate safeguards and compliance mechanisms are pre-emptively built into new products, services, and business models prior to reaching the wider market.79 Further, it is only at the end of the pre-defined sandbox period that fintech participants are able to fully deploy their products or services at a broader scale, provided they meet the objectives established by the process and have demonstrated their ability to comply with relevant legal and regulatory requirements.80

While regulatory sandboxes have only just begun to be implemented, several initiatives have received global attention. Early signs of success are emerging from the UK, a vibrant global leader in both fintech innovation and progressive approaches to fintech regulation. In November 2016, two years after the launch of the UK’s Financial Conduct Authority’s “Project Innovate”—which aimed to provide regulatory guidance to market participants and promote competition in the interest of consumers through various initiatives, including the creation of a regulatory sandbox program—twenty-four fintech firms were accepted into the sandbox’s first cohort, including nine blockchain start-ups. This group is notable for its international makeup.81 By employing a flexible approach to fintech, the UK may secure early access to the most commercially viable blockchain initiatives.

The concept of a regulatory sandbox is not entirely new to Canada. In October 2016, the Ontario securities regulator, the Ontario Securities Commission (OSC), announced that it was “prepared to be flexible with market regulations to help
financial technology firms get to market.” The OSC later entered into an agreement with the Australian Securities and Investments Commission to provide mutual support to fintech firms looking to enter both markets, signalling its intention to internationalize its approach to fintech and blockchain regulation. Moreover, the Canadian Securities Administrators followed suit in February 2017 with the announcement of their own regulatory sandbox initiative. There is no indication, however, that this initiative will engage the host of other provincial, territorial, and federal regulators in Canada overseeing the activities of firms employing blockchain technologies or other fintech innovations. This may well limit the effectiveness of this initiative: only a partnership of all relevant regulators, as well as fintech and blockchain market stakeholders, will sustain a robust sandbox program.

Conclusion

The current wave of financial sector modernization driven by fintech innovation—and blockchain technologies more specifically—has resulted in a period of opportunity for consumers, the financial sector, and the Canadian economy. Canadians now have access to a vast array of innovative financial products and services that are convenient to use, cost-effective, and tailored to their needs. These emerging technologies have offered incumbent financial institutions an opportunity to replace existing financial infrastructure and seek larger profit margins through technological modernization at the precise moment where they concurrently face mounting international competition and regulatory scrutiny. New fintech firms developing these technologies have caught the attention of innovators and investors alike, boosting the Canadian economy. And yet, emerging technologies also threaten existing approaches to regulation, and empower groups and individuals—including criminals and terrorists—seeking to skirt regulations for nefarious purposes. More broadly, the effects of fintech and blockchain technologies on deeply integrated and internationally interconnected financial and economic systems is not known or appreciated; uncertainty can lead to instability.

For policymakers, this dilemma is a pointed one. As the article illustrates, on the one hand, the risks of failing to foster innovation through the development of a coordinated national fintech regulatory framework are consequential: Canada risks losing its competitive advantage in developing and profiting from blockchain technologies. Moreover, without defining the parameters within which both emerging fintech firms and financial incumbents can innovate, risk-averse business practices may become entrenched, increasing pressure on the strained profit margins of Canada’s financial institutions. Some Canadian fintech start-ups and venture capitalists will relocate to more favourable regulatory jurisdictions in Asia and Europe.

82. Barbara Schecter, “OSC keeps closer eye on fintechs while giving them more freedom to get to market,” Financial Post, 24 October 2016.
On the other hand, establishing an under-regulated environment may encourage criminality and undermine anti-money laundering and anti-terrorism efforts with dire consequences in Canada and abroad. Public blockchains and the cryptocurrencies, digital black markets, encrypted verification processes, and the underground communities they foster, may complicate and undercut law enforcement and intelligence gathering processes with very serious consequences.

The solution may lie in pursuing a flexible, adaptive, and coordinated regulatory approach. The nascent sandbox model, while still in its formative development, is meant to provide vetted technology start-ups with a tractable regulatory environment in which they can innovate safely. This will help limit threats to public safety and security, bolster existing financial systems, and provide regulators with a degree of necessary oversight. Even then, however, best practices for the regulatory sandbox have yet to be determined: fintech and regulatory leaders, like the UK, have only just implemented this approach. Adaptive and responsive regulatory leadership will be needed, providing states, governments, and regulators with the ability to react appropriately to unforeseen events and consequences within and beyond the sandbox itself. And from a Canadian perspective, seizing these opportunities will require Canada’s competing jurisdictions to find ways to cooperate efficiently across all facets of the financial sector regulatory paradigm. A pan-Canadian approach to the regulatory sandbox is the best, and perhaps only, way to foster fintech and blockchain technologies in a way that meets the competing demands of Canadians. Establishing such an expansive, cross-jurisdictional approach will be a challenge all its own.

For scholars, the article suggests two areas for further research. In the first case, more speculative research is needed in Canada on the influence blockchain technologies may have on the domestic economy, national security interests, and political and governance structures. What comparative lessons from abroad concerning the potential of blockchain technologies might Canada absorb at home in formulating effective and well-balanced policies and regulations? Are Canada’s existing bodies, agencies, and institutions able to address, with sufficient speed, the opportunities and challenges blockchain presents? How will Canada’s various levels of government, from the federal to the municipal level, cooperate on and prioritize a collective response? How might a Canadian response to blockchain be tailored to address larger, global trends? And what Canadian laws and norms might need to be reviewed, tweaked, or re-written to accommodate blockchain technologies while safeguarding against their negative effects?

The second area of research goes far beyond blockchain to encompass all forms of emerging and disruptive technology. Research is needed to better understand the ways that recent innovations in biology and gene editing technology (e.g. CRISPR/Cas9), engineering (e.g. additive manufacturing; nano-technology; robotics), computer science (e.g. machine learning; quantum computing), and digital space more broadly, interact with public policy, national security, and defence planning. The study of IR has only just begun to integrate technology into its theoretical folds. Can existing paradigms, approaches, and theories of IR properly account for the
political and social change resulting from the development, implementation, and proliferation of new technologies? How do we define emerging technologies as disruptive, as they relate to society, national security, public safety, economics, and governance? How are notions of power and coercion, diplomacy and statecraft, and values and interests linked to emerging technologies? And finally, what lessons can be culled from history (i.e. nuclear proliferation; the Space Race) to provide us with contemporary guidance?

Declaration of Conflicting Interests
The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding
The author(s) received no financial support for the research, authorship, and/or publication of this article.

Author Biographies
Evangeline Ducas is a recent graduate of the Masters of Arts in Public Administration, School of Public Policy & Administration, Carleton University, Canada.

Alex Wilner is an assistant professor at the Norman Paterson School of International Affairs (NPSIA), Carleton University, Canada.