Central Bank Digital Loonie: Canadian Cash for a New Global Economy

Final Report for the Bank of Canada's Model X Challenge

Andreas Veneris, Andreas Park, Fan Long, and Poonam Puri*

February 11, 2021

*A. Veneris is with the University of Toronto's Department of Electrical and Computer Engineering, and Department of Computer Science (veneris@eecg.toronto.edu); A. Park is with the University of Toronto Mississauga's Department of Management and the Rotman School of Management (andreas.park@rotman.utoronto.ca); F. Long is with the University of Toronto's Department of Computer Science, and Department of Electrical and Computer Engineering (fanl@cs.toronto.edu); P. Puri is with York University's Osgoode Hall Law School (ppuri@osgoode.yorku.ca).

Executive Summary

Today's global economic digitization of society, driven by technology trends, continues to advance at exponential speeds. Billions of Internet of Things devices have already made their way into our daily lives, our homes and cars, but also into health care, manufacturing, supply-chains and other infrastructure. This development is in sharp contrast to the financial sector which still operates on legacy infrastructure(s). The net-effect is that current systems of payment lack the flexibility to adapt to the digitization of the economy. They remain slow, clunky, and expensive; often one receives a digital service, or even physical goods, faster than the merchant receives the payment. Further, the emergence of Decentralized Finance, through blockchain technology, has already demonstrated a capacity to disrupt the financial sector, impact national sovereignty, and affect established monetary transmission channels. Hence, it is no surprise that nations and tech-firms are now building new digital infrastructures for finance, banking, and payments that circumvent those legacy practices.

Governments around the globe equivalently find themselves in an awkward position. On the one hand, monetary policies rely on the established functions of the financial sector. For many decades, banks have conveniently served as deputies in enacting those policies, along with efforts to squash money laundering, tax evasion, and the financing of terrorism. On the other hand, over the past decade, governments have publicly recognized the need to enable digital innovation to keep their economies competitive. Further, they acknowledge the responsibility to enable their citizens to protect their privacy from unabridged data harvesting, and the need for financial inclusion in core economic national activities, irrespective of means and location. Finally, economies such as Canada's risk that their home currency is displaced, or their national security gets severely compromised, if consumers and businesses alike flee to a more convenient, let alone foreign, digital payments alternative.

Against this backdrop, in recent years many central banks have raced to explore, research and test the issuance of digitally native money, or Central Bank-issued Digital Currencies (CBDCs), in an effort to rediscover the very essence and use of "fiat cash". The Bank of Canada (BoC) has emerged as a thought leader on CBDCs at an international level having spent almost a decade and significant resources on this endeavour. The Bank is now preparing to put itself in a position where it can issue a digital loonie should certain conditions mandate it. As the BoC has been contemplating the design of a CBDC for some time, given the scale of the particular enterprise, it wanted to sample ideas at arm's length. To do this, in early 2020, the Bank ran a competition among universities to research and propose a CBDC design. Being a finalist in this competition, this manuscript presents a design proposal for a Central Bank Digital Loonie (CBDL) based on careful academic research of the possible technological, legal, and economic components of such an unprecedented and historic expedition.

Here, a two-phased KYC-backed approach is proposed for a CBDL that mitigates risks at a global scale, promotes financial inclusion and welfare, and safeguards Canada's socioeconomic sovereignty in the IoT/5G-and-beyond/AI era. The design also creates new monetary transmission channels for the BoC if needed, it protects user's data and anonymity, but it also leverages Canada's past social investments. In the first phase, the BoC introduces a centralized platform that establishes digital cash with an authentication protocol that leverages existing infrastructure, yet safeguards users' privacy/data. In the second phase, the BoC expands the platform to become the backbone (and supervisor) for an enterprise-level blockchain as a common resource. This transforms CBDLs into "programmable e-money" that enables Canadians to operate, innovate, compete and thrive in the new global digital economy. Although the BoC has not committed to issue a CBDC, it already has a concrete contingency plan. The findings here urge it to issue digital-cash sooner rather than later. After all, as Arthur Clarke squarely put it: "the truth, as always, will be far stranger."

Contents

1 Introduction

In the past decade, the promise of electronic cash through Decentralized Ledger Technologies (DLT), also known as the blockchain, has electrified the world, creating an excitement for technology that was last seen in the 1990s when the internet first entered mainstream. The core premise of the technology is that blockchains are secured by cryptography and economic incentives, but also governed by decentralized consensus to enable value transfers without the involvement of a "central" authority. The widespread adoption of the technology has been coined to form a new "Internet of Value(s)" [1] or "Internet of Money" [2] with the potential to replace legacy financial infrastructure(s) by eliminating multiple layers of intermediation. If true, this will cause ripple effects on personal privacy, national security, law/regulation, property rights, and healthcare, among others. Today, the prospect of a widespread adoption, and the underlying technological philosophy, of decentralized "smart" (or "programmable") money has rattled leaders in governments and the private sector alike. Notably, the development of these technologies has almost entirely occurred outside of the mainstream tech sector and has instead been advanced by individuals, or self-declared "cypherpunks." It therefore comes as no surprise that this exogenous disruptive financial innovation has motivated many central banks in recent years to rethink payments, traditional monetary transmission channels, and even the very essence of "cash" [3–8].[1]

At the same time, billions of Internet of Things (IoT) devices have been deployed in our daily lives. These devices continuously collect enormous amounts of valuable data that impacts large sectors of the Canadian economy such as health care, automotives, manufacturing, supply-chains and other infrastructure [9–11]. As much of this data is collected in foreign tightly-closed silos, it is often unavailable to Canadian entities, including their rightful owners (*i.e.*, producers) to profit from it.[2] The data hoarding to potential foreign jurisdictions stifles competition and innovation for Canadians, notwithstanding that it adds layers of new challenges in safeguarding Canada's sovereignty at multiple levels [12]. Finally, contemporary domestic and international commercial micro-payment systems lack appropriate platforms and economic incentives in creating efficient IoT marketplaces where Canadians can trade their data in a cost-effective, secure and "fair" way.

Evidently, this rapidly changing environment has prompted the Bank of Canada (BoC) to investigate its own disruptive innovation in the field of "currency technology" for quite some time. For one thing, its work has been keenly motivated by the candidate scenario where cash disappears, leaving people without risk-free money issued by the government. Further, as extensively noted in the existing literature [3–8], digital currency can create novel payment channels, new transactional communities, and safe networks-of-relations — all of which with a potential to further secure Canada's monetary identity, nourish its past investment in social values, but also safeguard its geopolitical digital boundaries in a

[1] See also the joint report of the Bank of Canada, European Central Bank, Bank of Japan, Sveriges Riksbank, Swiss National Bank, Bank of England, Board of Governors of the Federal Reserve, and Bank for International Settlements, "Central bank digital currencies : foundational principles and core features," as well as the Bank of Canada's Contingency Planning for a Central Bank Digital Currency.

[2] See Toronto Star: Sidewalk Labs' brief presence in Toronto taught us much about privacy and digital governance — two of the thorniest dilemmas facing smart cities (January 6, 2021).

rapidly emerging and evolving global techno-economy [13].

What is Central Bank Digital Currency? The growing interest of central banks in digital money, or *Central Bank Digital Currency (CBDC)*, has had many drivers in the past few years and opinions on their origin vary [4, 5].[3] However, two primary factors seem to have sparked this interest. First, the use of traditional cash by the general public has been decreasing, in favour of digital alternatives such as debit and credit card transactions and wire/electronic fund transfers. In some jurisdictions, like Sweden or Canada, the decline in the use of cash has been particularly stark. The second factor is private altcoins and other tokenization initiatives that followed the advent of Bitcoin [14], and later Toronto's Ethereum [15] which provides a Turing-complete smart contract language to build decentralized applications. Today there are more than 5,000 cryptocurrencies and blockchain-based tokens in circulation. Cryptocurrencies trade at free-floating prices relative to fiat currencies and most have volatile price histories, limiting their usability as "money." Subsequent attempts to limit price volatility of those original alt-coins led to the development of stablecoins and most recently to "mega-stablecoins" such as Facebook's Libra/Diem [16]. This tech-driven development of digitally native finance applications outside of the legacy networks challenges the traditional bank-based payment and monetary policy transmission mechanisms [17],[4] prompting central banks to heed their raison d'être and protect financial stability by exploring their own tokenizations of fiat currencies with CBDCs.

By means of a brief technical introduction, the literature differentiates between *wholesale* and *retail* CBDCs: a wholesale CBDC is a settlement mechanism between Financial Institutions (FI) for inter-bank transfers (usually large-value funds transfer systems such as Real-Time Gross Settlement Systems), whereas *retail* (or *general purpose*) CBDCs are available to the public at large. From those two forms, retail CBDCs (also the topic of this work) are the most transformative as an evolution to public transmission channels of central bank monetary holdings/policies. Architecturally, a CBDC scheme can be either a *one-layered* system, where the central bank directly manages all aspects of its lifecycle (distribution, KYC, settlement, etc.), or *multi-layered*, where (non-government) entities (commercial banks, payment service providers (PSPs), non-government organizations (NGOs), etc.) act as intermediaries for market placement, compliance, distribution or settlement. Further, many authors differentiate between *account-based* CBDCs, where users open an account or "e-wallet" at a central bank or at a PSP, and *token-based* CBDCs, where users hold digital units, such as a token, in a physical device [18]. Notably, as government-issued money, a CBDC needs to be universally accessible, including for people of low means, those without access to (or an ability to) handle technology, those in remote communities with only intermittent access to the digital world, the unbanked, and international visitors [19].

Most of the literature converges that in terms of their legal status, a CBDC is a digital representation of a fiat currency, hence a digital liability of the central bank (just like physical cash), denominated in an existing unit of account, which serves both as a medium

[3] See also the Group of 30 report on "Digital Currencies and Stablecoins: Risks, Opportunities, and Challenges Ahead."

[4] For a recent report in the popular media see commentary on the legal case SEC V. Ripple.

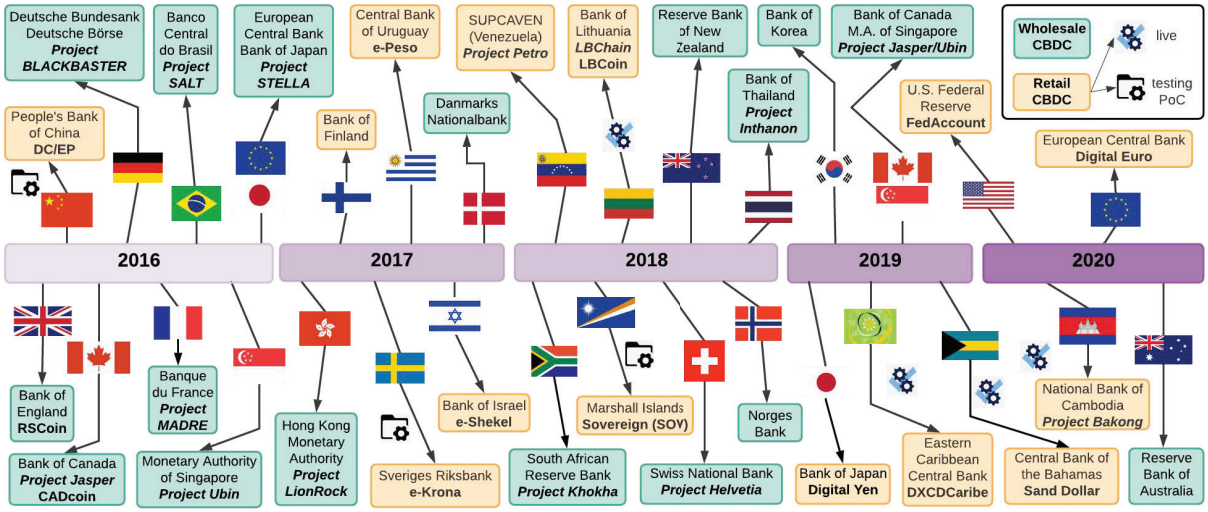

Figure 1
A Timeline of the International Interest in CBDCs

of exchange and a store of value [20]. Occasionally, CBDCs are devised as an "enhanced" version of cash in terms of universal accessibility and transaction capabilities, thus placed in between physical M0 cash and commercial bank money. Pursued goals vary according to the specific needs of the jurisdiction, as advanced economies generally rank their goals differently than emerging economies. Most existing CBDC plans envision improved payment efficiency (including new monetary policy transmission channels), financial inclusion, safety, privacy and compliance [3, 17, 21].

A Brief History of CBDCs. CBDC Proof-of-Concepts gained prominence in recent years and extensive commentaries have already been published by diverse stakeholders [4–8, 22]. The work of [21] classified central bank projects as early adopters, followers, and new entrants; Figure 1 provides an overview of their historical development.[5] In the first 2015-16 phase, research pioneers explored mostly wholesale CBDCs. The Bank of Canada (BoC) piloted the four-phased Project Jasper, one of the most comprehensive DLT-sandbox efforts to date. In Europe, Deutsche Bundesbank and the Banque de France put forward projects BLOCKBASTER and MADRE, respectively. The Bank of England (BoE) initiated a CBDC research program, and the People's Bank of China (PBoC) started developing a retail-CBDC titled *Digital Yuan* or *Digital Currency Electronic Payment (DCEP)*. In 2016, the Banco Central do Brasil set up Project SALT, the Monetary Authority of Singapore (MAS) launched Project UBIN and the European Central Bank (ECB) with the Bank of Japan started Project Stella. In the second phase (2017-19), retail CBDC projects started to emerge. Project Inthanon-LionRock of the Monetary Authority of Hong Kong addressed inter bank settlements. Other central banks explored general purpose CBDCs and their

[5] Figure 1 is from [23] and replicated here.

relation to cash such as the Sveriges Riksbank's e-Krona Project in Sweden.

By mid 2019, Ecuador, Ukraine and Uruguay completed a retail CBDC pilot and another six retail CBDC pilots were ongoing: Bahamas, Cambodia, China, the Eastern Caribbean Currency Union, Korea and Sweden. By now, as many as 18 central banks have published research on retail CBDCs, and a number of central bank officials have made public speeches on CBDCs, where the tone is becoming increasingly positive [24]. Although the U.S. Federal Reserve was notably on the sidelines without publishing any comprehensive technical note on the topic, the year 2019 was a breakthrough one for CBDCs, the watershed moment arguably being Facebook's announcement of Libra in late June 2019.

Today we are in the third phase of CBDCs: In February 2020, the BoC announced is contingency plan for a CBDC; in May 2020 the Digital Dollar Project released a whitepaper, in October the European Central Bank issued a report on principles and configurations for a candidate retail *Digital Euro* – also announcing a pilot program starting in the summer of 2021. Finally, October 2020 saw the launch of the first CBDC by the Central Bank of the Bahamas through the Sand Dollar platform. The Sand Dollar is pegged to the Bahamian dollar, which in turn is pegged to the U.S. dollar on a 1:1 basis under currency board-like rules. This move also seems to validate claims that smaller economies may want expedite the implementation of their CBDCs because of the risk that their local currency gets displaced by larger foreign economies.

Proposal Outline. This paper outlines our proposal for a retail Central Bank-issued Digital Loonie (CBDL). In more detail, Section 2 summarizes the objectives, mandates, and requirements that the BoC has made public; Section 3 provides a succinct summary of its main features; Section 4 describes the underlying technological architecture; Section 5 outlines how the proposed system complies with anti-money-laundering requirements; Section 6 demonstrates how our setup achieves the Bank of Canada's policy goals; Section 7 elaborates on the business plan that the BoC requires; Section 8 describes the legal framework that enables the proposed CBDL design; Section 9 expands on additional risks and alternative approaches; and Section 10 concludes this work.

2 BoC Policy Objectives and Model-X Challenge

Soon after completing the four phases of *Project Jasper*, on February 25, 2020 the BoC published its Contingency Planning for a Central Bank Digital Currency. In that plan, the BoC recognizes the following set of objectives:

- Supporting Payments Canada's Payment Modernization program to improve the speed, reliability, accessibility and end-user experience of Canada's payment systems;
- Ensuring bank notes remain available to Canadians who want to use them, including maintaining a distribution model that remains resilient and cost effective; and,
- Building, as a contingency, the capability to issue a cash-like CBDC to the public, should the need ever arise.

In the same plan, the Bank disclaims that it has no plans to launch a CBDC, but only wants to build the capacity to issue a general purpose, cash-like, CBDC should the need to implement one arise. This is because it takes several years for any authority to build the necessary expertise or launch any such preparatory work. Hence, preparing in advance remains a critical step for the BoC. The Bank also notes that it will consider launching a CBDC if certain scenarios materialize or appear to be likely triggered.

The two notable scenarios are:

- A continuous decline in the the use of bank notes to the point where Canadians no longer can use them for a wide range of transactions; and/or,
- A situation where one or more alternative private sector digital currencies start to become widely used as an alternative to the Canadian dollar as a method of payment, store of value and unit of account.

Later, in April 2020, the BoC issued an academic competition-for-proposals under the "Model X" title with the following five policy objectives for a potential Canadian CBDC:[6]

- **Privacy:** maximized but complying with regulations such as anti-money laundering;
- **Universal Access:** regardless of user's means, ability or geographical location;
- **Security:** resistant to the most sophisticated cyber-attacks;
- **Resilience:** operating continuously both online and offline; and,
- **Performance:** scaling for daily use in Canada.

In more detail, by formulating the above policy objectives, the BoC highlights the value of a layered platform approach so that third parties can build on top of the core CBDC platform. Furthermore, it expresses an interest in a flexible, long-run sustainable architecture that separates the core system from the front-end user experience, but also one that is adaptable to new consumer devices so it can accommodate the ever-changing commercial use cases. In contrast to commercial systems that focus on a specific market(s), the Bank notes that a CBDC needs to guarantee universal access to all Canadians irrespective of financial means or sight, dexterity or cognitive impairments so as to ensure accessibility and financial inclusion, and to also be usable in remote communities, even those without internet access. Although user/transaction privacy should be protected, a digital Canadian dollar must adhere to regulatory standards, in particular with regards to Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) legislation. The system must also be resilient and robust, able to operate continuously and without fault while it is scalable so it can serve the entire population of Canada. The BoC further requires that CBDCs should be able work with with existing retail payment systems and banking ecosystems including *Interac* and the forthcoming *Real-Time Rail* platform by Payments

[6] See also [25].

Canada. This compatibility is necessary to allow users to access their funds from accounts at commercial banks and to allow merchants to accept CBDCs as a means of payment.

Notably, the Model X competition asked for engineering proposals that are also accompanied by a clear business model that defines a CBDC's value proposition, ecosystem, interrelationships, and incentives that deliver on the aforementioned public policy goals/values to all stakeholders. In the Model-X competition, the BoC specifically requests a solution that does not put it in direct contact with the end-users (*e.g.*, with services such as identity verification or account opening/servicing) although it remains open to providing a baseline service to them. Finally, it asked for products and service-quality metrics of the highest standards, for a system with high operational yet low-cost efficiency that provides seigniorage income from CBDCs to the BoC, and for a design that fosters healthy competition in the payments market.

3 Central Bank Digital Loonie: A Project Synopsis

The remainder of this paper outlines our technical, business, and regulatory design proposal. This section presents the synopsis and an introductory reasoning behind our forward-looking model for a *Central Bank-issued Digital Loonie*, or *CBDL*, issued by the BoC.

In brief, we argue for a *two-phased* account-based KYC-backed approach for a CBDL that mitigates risks at a global scale, promotes financial inclusion and welfare, safeguards Canada's socioeconomic sovereignty in the IoT/5G-and-beyond/AI era, [7] may create new monetary transmission channels for the BoC, if those alternatives are deemed as attractive alternatives in the future, and leverages Canada's past social investments. The first phase involves the BoC introducing a mechanism to establish digital cash based on a *centralized platform* with an authentication protocol that is based on existing resources, and that safeguards users' privacy and data. Later, in the second phase, the BoC expands this platform to become a backbone that allows private enterprise to build *a decentralized messaging platform* (or *channels*) that transform CBDLs into "programmable e-money." These channels create a decentralized financial architecture that enables Canadian enterprises and the public to operate, innovate and thrive in the new global digital economy. Finally, offline transactions are served through a token-like portable card system.

Value proposition to Canadians. The global economy is becoming increasingly digitized and an efficient digital payment system is a prerequisite for the ever-changing digital commerce, as noted earlier in this proposal. Canadian businesses that want to compete in this environment need access to digital money. China's RMB-based DCEP or Facebook's Diem/Libra have the potential to establish new "default global digital trade currencies" that may undermine the Loonie's role even for domestic payments. In fact, it can be

[7] Modern IoT/AI markets involve the handling (or trading) of massive amount data, with low latency system responses that are facilitated by micro-payments (*i.e.,* fractions of a cent per datum) that cannot be facilitated by legacy commercial payment mechanisms.

safely argued that Facebook's Diem corporate expedition is not only a challenge to existing financial firms or central bank money — it is also a bellwether that the current financial system is *inadequate* for this new digital economy. A prerequisite for any design, therefore, must be that the CBDL can accommodate new fast-emerging technology trends. Today's payment processing fees are also too expensive: for instance, in 2016, they accounted for over $17B in costs to the Canadian public. Offline businesses do accept cash or cheques to avoid such costs, but as noted earlier, those payments tools are archaic for digital commerce and already in decline. Hence, CBDL transaction fees should reflect marginal processing costs. They should also allow transactions in sub-denomination of a cent to serve cost-effectively the needs of emerging IoT (micro-payment) markets. Finally, a major concern with privately operated electronic payment systems (some of which can be owned by foreign jurisdictions) is the protection of the public's data/privacy, business secrets, and national security. This becomes particularly important today in the context of IoT/5G-and-beyond/AI technologies that generate enormous amount of data for commercial and/or political harvesting.[8] It is no coincidence that this was also a major concern at Facebook's U.S. Congressional/Senate Hearings just days after the introduction of Libra/Diem in June 2019. Evidently, our proposed CBDL architecture ensures Canadians' privacy by default, but also allows them to monetize their own data.

CBDL Principles. CBDLs have the following physical-cash characteristics: *(i)* they are a liability on the BoC's balance sheet where each CBDL is equivalent to one Canadian dollar; *(ii)* they are available to every registered Canadian resident and corporation; *(iii)* they transfer quasi-anonymously among verified e-wallets that require one-time e-KYC; *(iv)* they transfer in real-time with minimum fees; *(v)* they allow offline transactions; *(vi)* they generate seignorage income for the BoC at creation; and *(vii)* they comply with AML/CFT regulations. Whether CBDLs bear interest or not, a viable option in the proposed architecture, is a policy decision beyond the scope of the work here.

Project Roadmap. We propose an implementation in two phases. In the first phase, the BoC establishes an entity that provides CBDL-accounts and processes all CDBL transactions within a tightly-closed centralized system. It also establishes a new status-quo by introducing CBDLs. The platform will follow domestic/international standardization, it will be open-source and it will provide publicly a limited number of entry-level communication APIs to third-parties. Later, the second phase will introduce a tightly-regulated permissioned DLT to enhance the functionality of the centralized system. In this phase, the aforementioned entity will transition to a supervisor and validator of the enhanced architecture. Simply put, this blockchain ecosystem will become a "common resource" infrastructure that benefits from BoC's ongoing R&D investment, it improves scalability/applicability for CBDLs while it contains the associated costs for the Bank. Further, it will be open-source and the information it produces will not be siloed. This will enable private service providers to innovate, compete fairly and provide utility and value to Cana-

[8] A prominent example is the Cambridge Analytica Scandal.

dian businesses and consumers. In this phase, network participants (*i.e.,* the few private validators and the non-validating service providers) will undergo an auditing and licensing process — similar to what Facebook's Diem seems to plan for its network today.

Although the BoC has not yet made a commitment to issue a CBDC, it did release a contingency plan to do so if Canadians are threatened losing the ability to use risk-free money issued by the government. Market research suggests that Canadians clearly value cash [26]. Therefore, a CDBC should operate alongside the existing e-payments rails by the major FIs. However, as outlined in Section 7, if the conditions of the contingency plan are met, it is difficult to imagine that legacy FIs may have "sincere" incentives to expend resources in establishing an alternative digital currency that may compete with established revenue stream(s). Therefore, one may safely conclude, that it is prudent that the BoC *alone* spearheads the development of CBDLs on a centralized system first, while committing to later offer the private sector the ability to profitably innovate.

Operation in Phase 1. Our proposal requires an expansion of BoC activities by incorporating and overseeing an entity that provides CBDL-accounts to millions of residents and businesses and is responsible for the processing of large numbers of transactions of BoC-issued CBDLs per day. Based on a thorough legal analysis (see Section 8), we propose to establish a separate legal entity that is connected to the existing payments network to ensure interoperability and that manages all CBDL transfers. This entity resembles what we refer to as a *"Narrow Bank" (NB)*.[9]

CBDL transaction messages in the first phase trigger push transactions providing immediate settlement. This is possible because those transactions are direct transfers between fully-funded CBDL-wallets that involve no credit. As we describe in detail later, offline transaction are enabled through a dedicated device, namely a "CBDL-cash-card," that links to an e-KYC wallet when it is online. Roughly speaking, offline transactions will be accommodated by NFC/QR functionality widely available in smartphones or merchant terminals today, and they only serve capped small-scale transactions sufficient for typical daily use cases (restaurants, movies, gas, etc.).

Operation in Phase 2: *Business Innovation-by-Design.* The second phase will introduce a permissioned decentralized payment messaging programmable layer on top of the Phase 1 infrastructure to improve scalability and innovation in the ecosystem. A select number of entities (such as major FIs) with experience in handling technology, AML/CFT and data will be invited to join as validators in this DLT network to process CBDL-related transactions but also the execution of archetypal smart contracts. As detailed later in this report, the lucrative opportunities at a global scale behind this novel platform will offer incentives to private FIs to participate — just as in the case of other commercial permissioned networks. In this setup, the NB will transition to be one of the validator nodes but it will also be the single entity that performs overnight "CBDL housekeeping".

[9]The term "Narrow Bank" formally refers to a financial institution that provides only monetary (aka payments) services and invests its depositors funds in safe assets only (such as treasuries). For early descriptions see [27] and [28]; for a theoretical analysis see [29].

Finally, the system could collapse back to a centralized platform in the rare case of a systemic crisis exclusively operated by the NB under the basic operations of Phase 1.

Evidently, the redundancy allowed by decentralization increases both scalability and fault-tolerance of the underlying distributed platform. The messaging layer will be open-source, it will follow tight domestic/international standardization for inter-operability, and it will continue releasing entry-level public APIs for third-parties. This setup extension will enable the platform's core functionality to allow FIs, FinTechs/PayTechs, and other service providers to build digital commerce services that leverage the BoC's efforts. Examples of such services include further data-protection/data-mining mechanisms, digital-authorizations and e-signatures, asset-tokenization ecosystems, low-latency system processing/markets for IoT/AI operators, account and spending management tools, and cross-border payments to existing overlay networks such as SWIFT or other permissionless/permissioned blockchains. In this phase, it is also desirable for Canada's government to spearhead initiatives such as those by e-Estonia or Dubai Smart City that leverage its social values and past investments in health/immigration/environmental protection so as to support Canada compete/lead in the realm of open-commerce at a global scale.

Onboarding, Privacy, and AML. The CBDL platform should secure Canadians' privacy by default. It should *also* allow them to monetize their data. We propose using outputs of recent digital ID initiatives in Canada, *e.g.*, by the Ontario government or the Treasury Board Secretariat, as well as leveraging the existing public infrastructure (*e.g.,* provincial service agencies, or Canada Post) and private sector solutions such as those by Canadian-owned FINTRAC compliant financial services firms for our proposed onboarding process. In a sense, this onboarding process bears a level of similarity to India's Aadhaar system [30] that provides each citizen of India with a digital biometric identity allowing them to transact without releasing identities or transaction-data between the parties.

Eligible Canadian residents and businesses will obtain their wallets addresses after under-going a third-party e-KYC process. These wallet addresses will be represented by a quasi-anonymous identifier, in the sense that it is built to not identify the user identity or the respective transaction-data to other system parties. This process is further extensively described in latter parts of this document. However, owners of CBDL wallets will undergo regular overnight checks for AML/CFT compliance by the NB. [10]

To transfer funds from their wallets at the BoC-supervised NB payments processor, transacting parties will use their authenticator (*i.e.*, through a smartphone or their online computer app) to prove their identity, which then forwards the authorized transaction message to the NB that settles the wallet transfers. The NB itself does not know the person or business behind a wallet identifier, unless mandatory and routine AML/CFT checks warrant an in-depth investigation. The NB thus processes transactions quasi-anonymously,

[10] In this document, we use the term "quasi", rather than "pseudo", to represent the very nature of CBDL wallets, those of the offline CBDL "tokens" but also the corresponding user/transaction-identities/data. All those entities are not anonymous when AML/CFT triggers compliance flags, or to court orders that direct to reveal certain information – all within a NB "behind-the-doors" protected environment. However, our proposal mandates their anonymity to non-NB parties, hence the terminology distinction.

but it will also keep and analyze records periodically to comply with AML/CFT provisions. We propose that wallets have upper limits (*e.g.,* 10,000 CBDLs) sufficient for typical cash-like transactions. To encourage Canadians to invest time in setting up their e-KYC (the significance of which we describe later) and, to ensure that there is no sudden drop in commercial bank deposits that threatens financial stability, the BoC may want to seed-fund each new wallet with a small amount [31] through a one-time expansion of its balance sheet (*e.g.,* 100 CBDLs, but this, or the exact amount, are policy questions beyond the scope of our work). Wallets with special provisions, such as ones with reduced functionality or with preset-expiration dates, could exist for non-Canadian residents such as tourists or business visitors. Finally, the e-KYC process should altogether avoid contracting international parties to safeguard Canada's sovereignty by ensuring that data does not leave Canada.

In closing, as transactions are quasi-anonymous to intermediaries, involve no credit, and wallets are tied to e-KYC owners, we expect the proposed architecture to simplify regulatory compliance for CBDLs, provided that the direct wallet claims on the BoC are segregated from the balance sheets of the intermediaries. Section 8 discusses policy assumptions and recommended regulatory amendments to support this streamlined technology advancement.

4 CBDL System Architecture

4.1 Overview

We call for a CBDL introduction via a two-phased process. In the first phase, the BoC will establish a centralized platform by supervising a newly-formed NB entity that performs real-time clearing/settlement of CDBL transactions and keeps account balances of CBDL-wallets. This new platform will be integrated into the existing payments network infrastructure. We expect this phase to foster rapid adoption while keeping costs low. The second phase will open the system to private service providers/intermediaries via a permissioned blockchain that is controlled by the NB and, in effect, ultimately supervised by the BoC. In this new ecosystem, licensed third-parties (called service providers) will be enticed to build decentralized services. A few private validators, also approved by the NB/BoC, will significantly contribute to the cost-recovery of the overall platform. Under certain critical circumstances, the Phase 2 blockchain will degenerate into a centralized fully NB-controlled system. We also introduce an electronic Know-Your-Customer (e-KYC) prerequisite for users to attain CBDL wallets. In effect, this e-KYC exists to protect privacy and data sovereignty for Canadians.

4.2 Phase 1: Wallets, e-KYC and Transaction Lifecycle

4.2.1 CBDL Wallets

Users will obtain a CBDL e-wallet from an app store for use on their smartphones, tablets, computers, etc. Subsequently, after they undergo a one-time e-KYC (described next), they will register this wallet online, or through a provincial government service with the NB, so

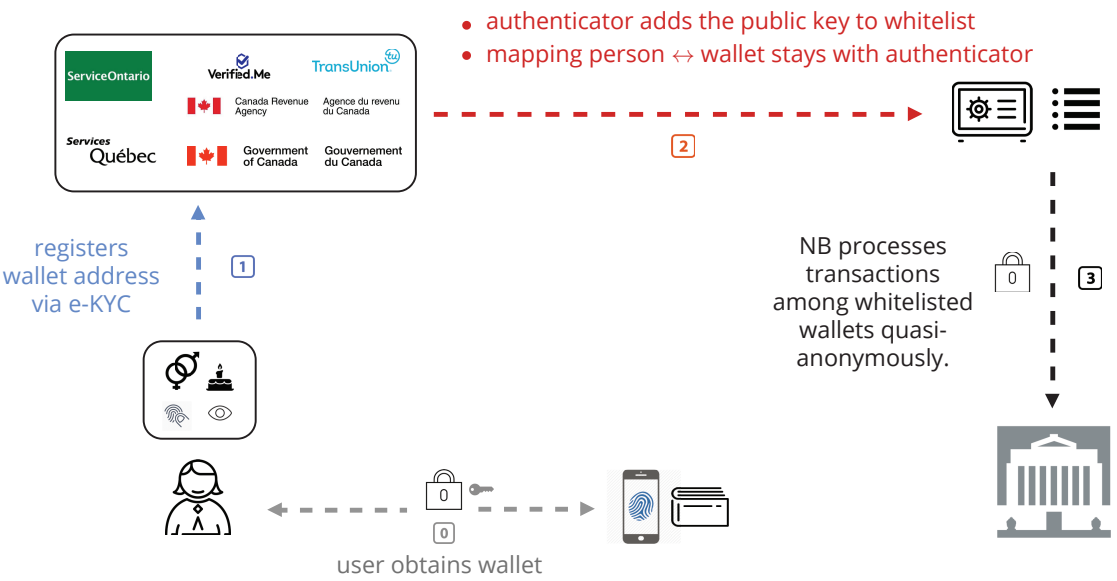

Figure 2
The e-KYC Process

its identifier is added to the "whitelisted" set of e-KYC-ed CBDL-wallets.[11] Wallets are a bare-bone piece of software typical to crypto-currency wallets today embedded in secure smartphone apps or browser plug-ins. This software can be downloadable from standard app stores like Google, Samsung or Apple, or from government websites. CBDL transfers will be enabled with PIN or biometric permissions, just as at credit card merchant terminals today, and by using QR, NFC, or even Interac-style emailing/text-messaging.

4.2.2 Electronic Know-Your-Customer Onboarding

For a Canadian citizen or corporation to get a whitelisted CBDL-wallet, the account holder first needs to undergo an e-KYC process to obtain a unique ID that can activate their respective wallet. Figure 2 illustrates this process where users obtain this ID (*i.e.,* similar to a public-private key pair) by using existing infrastructure. In particular, we expect the majority of Canadians to be onboarded using existing tools such as the financial sector's VERIFIED-ME process. Other entry points can be the Canada Revenue Agency and provincial service agencies such as Service Ontario, Services Québec, etc. The goal here is to reduce the cost of onboarding without compromising on security. After e-KYC clearance by an approved authenticator, each wallet is added to a whitelist that the NB subsequently uses to verify that a transaction is between legitimate/authorized CBDL users.

[11] There are rare cases where a Canadian does not have access to the internet or a digital device, for which we propose government service-administered solutions that's based on the CDBL-cash debit-like cards that we discuss in great detail below.

Each whitelisted CBDL-account will be associated with an encrypted unique ID connected with a KYC-compliant account with the approved authenticator. This will permit CBDL transaction records to be quasi-anonymous, both to the NB but also to all other system intermediaries. In the case that the NB is required to provide certain transaction records to FINTRAC so to comply with its AML/CFT obligations, only the necessary unencrypted data will be compiled across the NB and the authenticator. Prior to this, the NB should only maintain the minimal amount of data associated with each CBDL-wallet as is required for it to perform homomorphic encryption for AML/CFT obligations, as discussed below.[12] This architecture maintains privacy for users (similar to cash) and reduces cybersecurity risk for the NB without jeopardizing AML/CFT compliance standards. A process will also be required to update the whitelisted account in the case that the users' KYC information becomes outdated with the approved authenticator.

Notably, even visitors (tourists, business travellers, etc) to Canada who want to use CBDLs and obtain a wallet would need to undergo e-KYC by using their passport and possibly a credit-card. The process can also apply to new immigrants to Canada until their status settles with a work permit, permanent residency, etc. This process is no different to the registration of pay-as-you-go SIM cards for phones for one who travels abroad. In addition to the information about the registered wallet, the white-listing process should include additional information such as the authenticator's name and whether the wallet belongs to a person, a business, or an international traveller. Wallets for visitors to Canada may need to have limited life spans to reflect any respective visa restrictions.

The process will feature strong encryption and we suggest it be similar to that of the Indian Aadhaar system [30] — a system that has proven to be quite successful in the past decade.[13] In other words, the authenticator will have no knowledge of the individual registrar and this information will be cryptographically transmitted/stored in a central database managed by the NB. In this manner, existing homomorphic encryption techniques can be regularly applied by the NB overnight for the purpose of AML/CFT without revealing the identity of the underlying parties.[14] The exception is the case of an AML/CFT infraction: then the identity of the party would need to be revealed by the NB, but only if required by law. The BoC may decide to provide incentives to the public to undergo this e-KYC process. For example, it can endow each new wallet with a small amount (*e.g.*, 100 CBDLs) or provide tax credits or repayments in CBDLs [31] – a policy question outside the scope of this proposal. All in all, the proposed e-KYC process reduces costs and increases efficacy by registering every Canadian with a unique cryptographically-protected ID. Finally, considering recent initiatives, the private banking sector would also likely welcome the advent of a government-issued digital ID, and therefore, they should be invited to partially fund

[12] For example, the CBDL-wallet could be tagged if the owner is a "politically exposed domestic person" (as per AML/CFT) without revealing the identity of that person. If the NB needs to report a transaction by the CBDL-wallet, the necessary identity information would be retrieved by the approved authenticator.

[13] We recognize that over the past years there have been occasional challenges with Aadhaar, however, it continues to operate with a remarkable level of success serving more than 700,000,000 citizens daily; for instance, see articles from The H. Jackson School of International Studies or in the Washington Post.

[14] This type of homomorphic encryption parsing of data by the NB is expected to be a relative low-cost one considering it is performed centrally overnight.

the effort [32].

4.2.3 Transaction Processing

As it stands, the Canadian Payments Association, known as Payments Canada (PC), established by the Canadian Payments Act, has the legislative mandate to establish and operate national systems for the clearing and settlement of payments, and to facilitate the development of new payment methods/technologies (s.5, Canadian Payments Act). Our proposed Phase 1 solution includes a centralized system that allows KYC-approved quasi-anonymous identifiers to directly submit payment messages to a message processor. We propose to establish a new separate system or entity with the following characteristics:

- It is a separate legal entity from the BoC; [15]
- It is entirely digital (*i.e.*, it has no physical banking locations);
- It operates fully under the auspices of the BoC to handle BoC-issued CBDLs;
- Users establish accounts with the entity through the e-KYC procedures outlined earlier in this proposal;
- Users can send CBDL payment requests to that entity;
- The entity performs the necessary checks on the validity and eligibility of payments;
- The entity enables/settles "internal" transactions between CBDL-wallets in real time;
- Wallet messages follow ISO20022 specifications to ensure system compatibility; and
- The entity is eligible to access the RTR and Lynx and has a reserve account with the BoC.

Furthermore, the last feature of having a reserve account with the BoC also introduces the following benefits:

- It allows for straightforward convertability between reserves, commercial money, and CBDLs;
- It enables the BoC to include CBDLs in their monetary policy mix and to gain seigniorage income via CBDL issuance; and
- It allows users to transfer funds between their commercial bank accounts and their CBDL accounts using the RTR.

[15] For a detailed legal analysis of this entity and its enactment, please see Section 8.

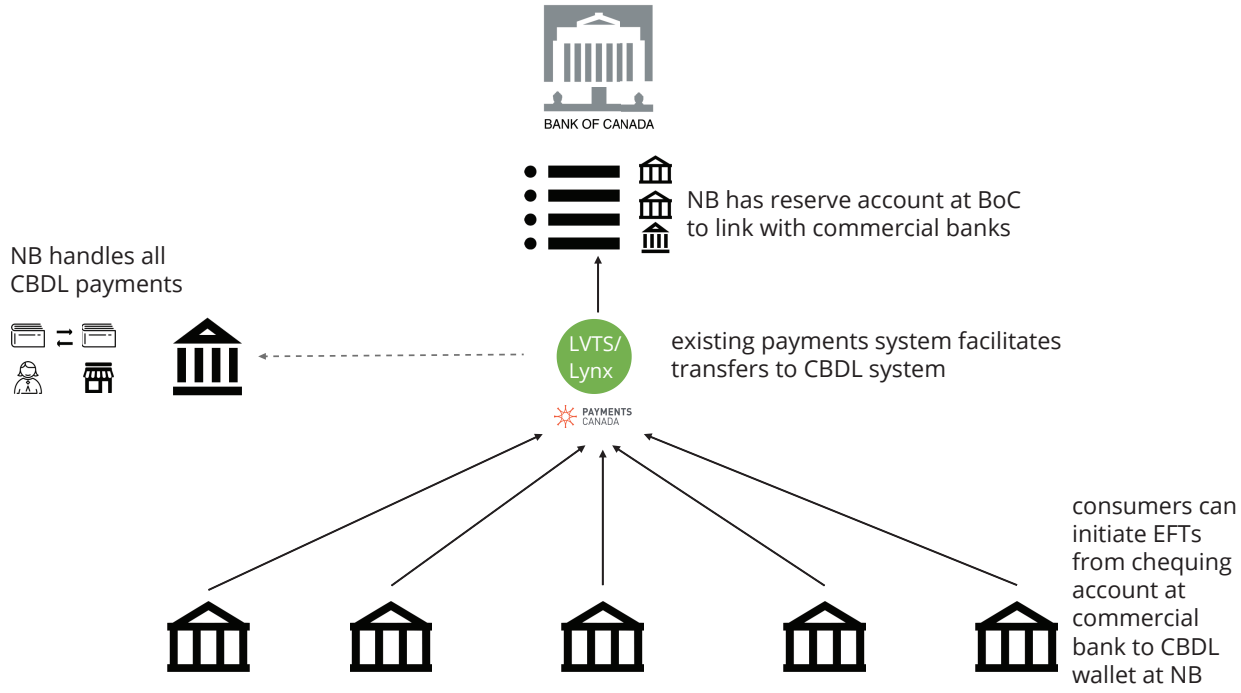

Figure 3
The Link of the NB to the Banking System

We thus propose to establish a separate public utility that the BoC oversees — roughly speaking, no different to what the BoC already does with Payments Canada through the Payment Clearing and Settlement Act and the Canadian Payments Act. This arrangement establishes the aforementioned *"Narrow Bank – NB"* entity that exclusively processes all CBDL payments, keeps account balances, and remains closely connected to the existing payment system/infrastructure. By definition, the NB would be fully funded and run-proof. Since CBDLs are backed by treasuries (which creates seigniorage for the BoC), there is also no need (or, at least, a much reduced one) for government-backed deposit insurance. Figure 3 illustrates how the NB links with the existing banking system.

In Phase 1, all CBDL-accounts/wallets would be maintained/managed by the NB. User-to-user CBDL payments will be internal transfers at the NB and outside of the existing payments network. These payments involve the transmission of cryptographically secure payment instructions between user apps and the newly established NB system. To transfer funds from commercial bank accounts to their CBDL wallet, users would initiate an Electronic Fund Transfer (EFT) using the existing banking network. Those EFTs would route via the new Lynx RTGS System and involve the user's bank requesting an exchange of CAD to CBDL via its reserve account at the Bank of Canada to the NB. Thus, within the new ISO20022/ISO4217 standard, a CBDL EFT could simply be a transfer using a newly designated three-letter currency.

All in all, the functional/architectural role that we envision is that of a public utility

that provides an infrastructure *at cost*. Admittedly, the setup of the NB entity raises a number of legal questions that we address in Section 8. In what follows, we continue to focus on the technical vision and its architectural components.

4.2.4 A Brief Note on Alternative Arrangements

Roughly speaking, in the current world, commercial banks hold two types of state-issued money: cash and reserves. Under our proposed system this would not change as the NB is a participant of the payments network and therefore, banks will interact with this new entity in the same manner as they do with any other commercial banks today. As such, the exchange of commercial money for CBDLs via the reserve accounts closely resembles a conversion of commercial deposit money into cash. In other words, commercial banks will never have to handle CBDLs directly. In the remaining of this subsection, we briefly discuss two alternative arrangements. First, the BoC could establish an entirely separate system where commercial banks hold an account at the NB. In that case, when a bank customer wants to obtain CDBLs, the commercial bank would then internally transfer funds from its CBDL account at the NB into the client's CBDL account at the NB in exchange for deposit funds. These CBDC holdings would thus be similar to the bank's cash holdings but add a third type of state-issued money that the banks would need to manage on their books. Admittedly, establishing such a system adds additional practical and regulatory burdens on commercial banks because they would need to run a new/separate internal system. This option would also likely require a multi-year high-cost development process without immediate incentives for the commercial banking sector. Another alternative would be to add CBDL wallets to the existing LVTS system/new Lynx. Again, this option would have far-reaching implications (and costs) for the required technology – notwithstanding, it exposes CBDLs to an untenable mix of "external" private/commercial participants. In our sincere view, both of these arrangements are inferior to the one proposed here.

4.2.5 The lifecycle of a CBDL transfer

Customers receive information about the destination of their funds and sign their wallet transfer to the target wallet using their private key, biometrics, or PIN. The NB verifies the validity of the signature, the legitimacy of the wallet against the public-key whitelist, and the sufficiency of wallet-balance before it approves, and immediately records, the transaction in its central database. Evidently, this process mimics public blockchain transactions (minus their latency) but it also resembles IBAN-style "push" executions. As CBDL payments messages satisfy ISO20022 standards, they should include information that simplifies AML/CFT audits, such as the usage of funds (*e.g.*, retail purchase, contractor payments, etc.) — all of which to be cryptographically protected and homomorphically processed.

Homomorphic encryption allows one to parse encrypted data without having to decrypt it first. In this context, as the privacy of citizen's data even from the government remains a premise of paramount importance in this proposal. Homomorphic encryption allows the NB to conduct overnight AML/CFT CBDL checks on transactions without revealing, even to itself, the content of those transactions or the identities of the underlying parties, unless

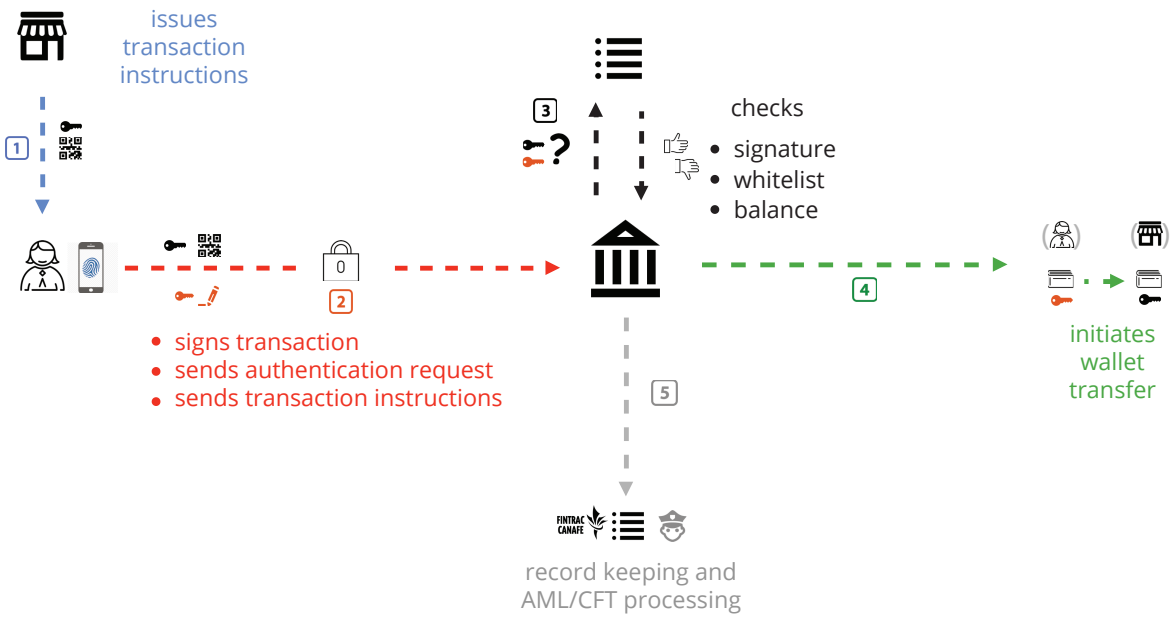

Figure 4
The Lifecycle of a CBDC Transfer

of course at the end of this process data triggers AML/CFT set-regulatory conditions (or there is a specific court order for same) that require decryption/reporting. Since the NB is a centralized service, parsing homomorphically encrypted data is expected to be a rather fast process — or, it can even be outsourced as it is common practice today with health- or financial-related data. Evidently, such a practice will not only reaffirm the existing trust of Canadian citizens into their government, but it is also provides an opportunity for the BoC to lead this concept by-example at a time where the world's governments and private corporations seem to be in a race for such data from the public.

The system stores transaction records for 30 days while AML/CFT compliance checks are pending. Following which, any transaction data that is not required to be stored under AML/CFT regulations will be deleted. These checks are performed based on the quasi-anonymous identifiers to preserve privacy, except when activities trigger FINTRAC reporting requirements. Additionally, we believe that it may be useful to review AML/CFT rules to highlight which ones may be unnecessary or overly stringent, *e.g.*, regarding the ongoing analysis of small-scale CBDL transactions (like those that are less than $50, for instance – similar to what China's DCEP seems to envision). It may also be necessary to enact/amend laws that insulate the NB from becoming a *de-facto* monitoring tool for the CRA or other law enforcement agencies, should those entities seek information on users and/or transactions from the NB. Policy considerations behind such amendments are contemplated further and balanced in Section 8. Finally, Figure 4 depicts the different

components in the life-cycle of an online transaction.

4.2.6 A Note on the Supervisory Authority

There are several ways to constitute the NB. One is to run it as a registered bank under the Bank Act. Another is to regulate it as a payments system under the Payment Clearing and Settlement Act and Canadian Payments Act. These options, among others, are examined in more detail under a legal and regulatory prism in Section 8. In the following, we just briefly discuss those two options.

In regard to the paragraph above, the former solution would create an independent "private" banking NB entity. According to current statutes, the BoC does not have custodial or supervisory status over such a bank-like entity under the Bank Act (the Office of the Superintendent of Financial Institutions has that power) except in cases of a systemic crisis. Another exception is the supervisory role of the BoC by virtue of the new entity's mandatory participation (as a registered bank) in the Canada Payments Association. This shelter will inevitably promote an undesirable impression that the government is creating a public entity that "competes" with the private banking sector and it may trigger other undesirable/adversarial legal, reputation or practical concerns. Since the new entity's envisioned role is merely to facilitate payments (and there is no role for other bank-like services, including the provision of credit), our preferred approach is to create (or simply amend) a statute similar to the Canadian Payments Act. In this case, a body is created for the purpose of distributing and transferring CBDLs, as well as having custody of the digital currency. The entity would be established by a federal statute that provides for the NB's mandate, sets out its governance structure, and provides the BoC with oversight authority over the entity. Aligned with the BoC's mandate in promoting a safe, sound, and efficient financial system (including payments systems, financial institutions, and financial markets) within Canada and internationally, the BoC would have authority under the Payment Clearing and Settlement Act to oversee the NB's operations.

4.2.7 Custody of the Assets

The BoC is generally not a custodian of financial assets, including money.[16] The NB would, as the maintainer of the central ledger, effectively have custody over the CBDLs. The NB's authority to do so would be outlined in its governing statute. To support the NB's role as a custodial entity, it may be necessary to amend the Bank of Canada Act to permit the BoC to issue CBDL to the NB and for the NB to hold a reserve account with the BoC. At all times, however, the CBDL in the custody of the NB would be considered assets of the CBDL account holder, not the NB. Special considerations apply for offline payments, because the NB processes only transfers between e-wallets and syncs e-wallets to cards. When CBDL is transferred to a card, as we will see in the next subsection, the account-based CBDL gets converted into a quasi-token-like CBDL. In that case, the NB does not process transfers between offline cards. Therefore, the user assumes sole control

[16] There are some exceptions, such as the Canada Deposit Insurance Corporation or foreign central banks.

(*i.e.*, custody including a risk of loss) over the tokens stored in their card, but also of all subsequent card CBDL transactions. Section 8 discusses those legal avenues in detail.

4.3 Offline Payments

Overview. A central requirement for CBDLs is that they are usable even when users have (temporarily) no access to the online world. In our view, facilitating offline transactions results in a *trade-off* between hardware/software security, costs, and convenience. The main security challenge is lost (or stolen) funds. Another equally important concern is an adversary that may attempt to double-spend offline as they may have not yet been settled through the online system. We address both of these issues in our scheme.

One way to implement offline transactions is via tamper-proof hardware [3]. Many processor chips, including those in our smartphones, have Trusted Execution Environment (TEE) enclaves/capability (*e.g.,* SGX in Intel and TrustZone in ARM). Alternatively, the federal government can mandate TEE compliance for all (imported or domestic) smart devices by proper configuration of the embedded FPGAs (eFPGAs) that are typical components of Systems-on-Chips or ASICs embedded in smart devices today. This would possibly call for new Design-for-Security (DfS) hardware architectures — a semiconductor research area that demands a more holistic hardware design approach than just a traditional cryptographic implementation(s) [33] — but also domestic/global CBDC/L hardware/software co-design standards. With TEE and DfS capabilities, we can verify that any CBDL software applications are running on the hardware in an unmodified and untampered way, eliminating the risk of adversaries modifying the software to double-spend the money.

Another approach, which is both complementary and additional, would be to issue *CBDL-based cash cards* that are associated with and pre-loaded by whitelisted wallets. These debit-like cards have an additional feat as they can replicate the aesthetics of physical bills, used in the past centuries to celebrate Canada's history or landmark events. Their chips can be programmed (through NFC) to match to wallets and receive small amounts of CBDLs from the user's smart device (that contains the whitelisted wallet) when that device is online. This amount could be spent later offline via the cash-card as we explain in this subsection. In fact, existing payment systems already allow such offline transactions where even the merchant terminal does not connect for an authorization. Just like today, this model obviously requires the merchant to bear a risk that the payer may not have the proper funds. At the merchant's end, offline transactions will settle when their terminal comes online. In other words, these pre-loaded CBDL-cash-cards act as cold storage for small amounts of money and they can be also used by international visitors to Canada.

In Phase 2, offline transactions can also be enabled by private agents by using trusted intermediaries similar to Bitcoin's Lightning Network. The intermediary provides collateral to cover the risk associated with the offline payment and recovers its costs via user fees. In all cases, we assume CBDL-wallets will have periodic access to the network. This way we can balance any inherent compromise in the underlying security mechanisms.

Technology. Our proposal recommends using the Trusted Execution Environments (TEE) in the processing units of contemporary smartphones, tablets, laptops, etc (such as Samsung's KNOX, ARM's TrustZone, Intel's SGX, etc), so as to create appropriate hardware/software cryptographically-secured enclaves that store a limited amount of CBDLs. These protected wallets can be good enough for day-to-day transactions when access to the internet is not available and capped to a maximum limit (*e.g.,* 200 CBDLs) containing enough for common expenditures (gas, food, movies, etc.). Although research has demonstrated that TEEs may occasionally exhibit vulnerability, they are widely used for secure transactions today and further, as also pointed elsewhere in this proposal, offline CBDC transactions pose an inherent trade-off between security vs. cost of the implemented solution(s). Our proposal goes further by suggesting the introduction of CBDL-cash-cards that communicate with merchant terminals via NFC transmission. Those cards have the potential to alleviate the need of carrying a smartphone altogether for offline transactions, thus *also* serving those individuals without smart devices. In what follows, we first describe hardware considerations for those devices. Next, we outline their use-cases for different types of offline payments, but also how this innovation can be used to promote financial inclusion.

Advances in technology in the past decade have allowed for credit/debit cards that do not have an embedded power source to drive them, but act as an RF receivers/transmitter when the RF signal itself from other devices acts as the power source to activate them. Further, those cards can be programmed to store securely in their ROM chips items like a PIN number, or even the biometric information of their owner. Further, when activated by a nearby RF signal, they can perform sufficient power-efficient operations such as two-way cryptographic authentication and/or transmission of the encrypted data stored into them. This is essentially how "tap" operations occur with credit/debit cards today on merchant terminals; the merchant RF signal acts as the power source for those cards so to conduct transactions for small purchases, typically around a $100 threshold.

Evidently, in the case of smartphones, tablets, laptops, etc, the process described above is even simpler. These smart devices already have their own power source and secured hardware to emulate the behavior of those RF-activated credit cards. Moreover, it is notable that those devices can also act as terminals that can "activate" through RF other CBDL-cash-cards, provided their battery is not emptied. Finally, in the rare cases when those devices are already out of battery, their dedicated hardware can emulate the functionality of CBDL-cash-cards, provided they are in proximity to some external strong enough RF signal to act as the power source to "activate" it.

With the above information at hand, in the following we will use the term "RF-storage-card" interchangeably to denote either the standalone physical CBDL-cash-cards, or the smartphone/tablet embedded functionality that emulates a CBDL-cash-card. In this environment, an RF-storage-card will receive a limited number of CBDLs (*e.g.,* upper limit of $200/day, see below) from a smartphone, tablet, laptop, etc. when the latter device is online. As the transmitting device is online during this exchange, the wallet of the recipient will be debited this amount with the NB instantaneously. The reverse process will also be possible, that is, the user will be able transfer funds from the remainder balance in their RF-storage-card back to their online wallet via a device that it is online, an operation

that will also settle immediately with his NB wallet. Finally, the process of transferring offline CBDLs can be complemented with a two-level security protocol (like a PIN or biometric information), as already occurs today with traditional credit/debit cards issued by commercial banks.

Once loaded, the RF-storage-card can be used later to spend these funds when the user is offline. In this environment, there are three scenarios for one to consider:

- **CBDL-cash-card vs. online merchant**: The merchant's terminal, or even its smartphone (if online), can be used to power-up the CBDL-cash-card so the user pays for the service. As the merchant is online, the funds will directly deposit into its wallet with the NB, while getting "erased" from the card;
- **CBDL-cash-card vs. offline merchant**: This case is identical to the above, with the exception that the merchant will need get online later so as to settle its account with the NB. This case poses some risk to the merchant, as it may forfeit the money if the RF-storage-card that holds the CBDL gets damaged, lost, or stolen. However, this is no different to the situation with physical cash where the merchant loses its physical wallet/cashier — in other words, digital cash is not a panacea. Nevertheless, one should not expect a merchant to be offline for extended periods of time and therefore, the case described here is expected to be rare. Finally, to accommodate daily merchant operation, BoC may want to consider issuing slightly increased RF-storage-card limits for registered merchants.
- **CBDL-cash-card vs. CBDL-cash-card**: The two cards can communicate with each other provided there's a source of RF to power them. Further, this source should be able to help users transfer a specific amount of funds required by the transaction as the cards themselves do not have such functionality. One may argue this will be a rare case, but as CBDLs come into circulation, we expect third-party merchants to offer such devices that are both portable and cheap (*e.g.*, RF "flash-lights"). Note that in this scheme CBDL-cash-cards may become "fully" anonymous, thus emulating the anonymity of today's physical cash. Only the transfer service provider (at the time the CBDL-cash-cards are synced with online wallets) may have the chance to learn the identity information of the two participants (origin/destination). This is not a limitation, as the BoC does not envision CBDLs to completely eliminate physical cash. Further, we mitigate some of those concerns later in this subsection.

Evidently, RF-storage-cards do not require a bank account and their usage (albeit limited due to the CBDL-cap) can serve the few unbanked who can obtain such cards for their transactions in a regulated manner (like food-stamps). They can be also used for bartering in the communities that do so for a living.

4.3.1 The lifecycle of an offline transaction

Figure 5 depicts the lifecycle of an offline transaction. Each offline CBDL-cash-card (or simply "card" in this subsection) links to a unique e-wallet by programming its embedded

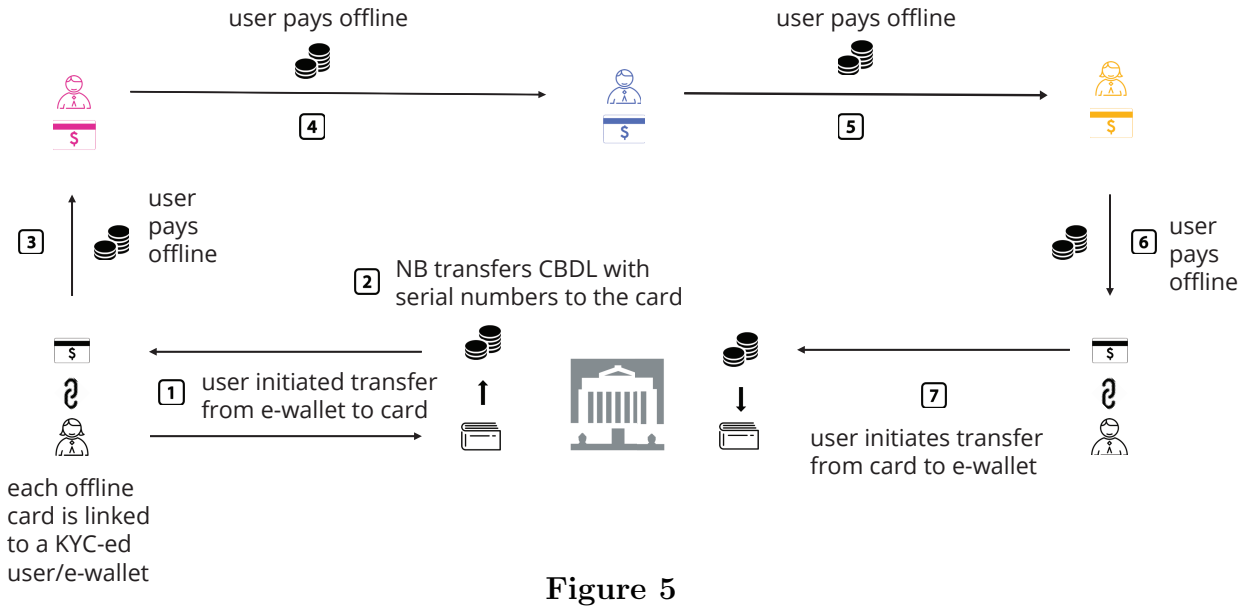

Figure 5
The Life-Cycle for Offline Transactions

RAM cryptographically. As we recall, e-wallets are already *uniquely* linked to a specific person following an e-KYC process. To use the card, a user first transfers funds from their e-wallet to the card (Step 1 in Figure 1) *while the e-wallet is online*. This entails a transfer of said unique CBDL serial numbers (or cryptographic tokens, if the BoC does not elect to use a serial number for the smaller denomination of CBDLs) from the user's e-wallet to the card (Step 2). In other words, those token serial numbers (or "account balance" if no tokens are used) get transferred to the card. As noted, this process needs to occur when the e-wallet is online, so the NB registers this transfer and updates the user's account balance. Further, also outlined earlier, a card does not necessarily need be a physical card, but it can reside in a hardware/software enclave of a modern smartphone.

In the above, we suggest the number of tokens to be based on the smallest unit of account, *e.g.*, 5 cent tokens (1 cent coins are already out of circulation in Canada). This is because we do not envision those cards to be used for IoT micro-payments that may require much smaller denominations as they trade data. In other words, if Alice transfers \$10 worth of money to her card, in essence, she transfers 200×5-cent CBDL-coins, each of which has a unique serial number (if BoC elects to use one) or cryptographic identification. This solves the issue of change as all amounts transferred will be exact. When the user uses their card to pay offline (Steps 3-6), the respective tokens are registered in the recipient's terminal while deleted from the sender's card at the same time. This terminal can be online or offline, but it needs be a "more functional" device than a simple card so to sign off on the transaction (power up the sender's card, input PIN, etc.). Users can transfer CBDL tokens from their card back to their CBDL-wallet balance if they wish (Step 7) when they

are online so that the NB registers this transaction (Step 8).[17]

Offline cards are invisible to the NB, and one may argue, they are also irrelevant — just as today, when the BoC has limited ability to track usage of the physical cash it issues. In other words, as an example, an original user Alice who synced her card with her e-wallet can pass her CBDL card (and the money deposited on it) to John, who can pass it to Mary, who can pass it to Bob. Neither John, Mary nor Bob can sync this card to their e-wallets as they are not the rightful owners of this card even if Alice tells them her PIN. However, Bob, for instance, can transfer the card CBDLs to his own CBDL card (if he knows Alice's card PIN) and later sync the balance to his online e-wallet. If this happens, the NB will know that some of Alice's funds reached Bob, but it will never learn about John or Mary.

To elaborate further through means of another example, if Alice loses her card, then she has also lost all the money on this card (similar to losing a wallet with physical cash), as there is no way to retrieve the CBDL "synced" in the card. As another example, if Alice loses her smartphone, she will also lose all the CBDLs in the smartphone's card-enclave (if any), but she will not lose her e-wallet money. This is because the e-wallet balance is held ("sits") at the NB, not in the smartphone that only acts as a way to identify the user, and validate/settle transactions, via a wireless network with the NB. When Alice declares the phone lost at the proper agency, they will disable it from her NB account and register her new phone. In our proposal earlier we also speculated for card-to-card transactions, but these are more complicated in terms of the hardware design, and we omit their description here. Finally, it is also suggested that cards have an upper limit of CBDLs that they can hold (*e.g.,* $200 worth of CBDLs) to serve as trade-off between security vs. invested hardware effort to build those cards. In conclusion, one may argue that, to a certain extent, the card-scheme proposed here bears a small degree of conceptual resemblance of the voucher idea proposed by the ECB in 2019 [34]. We respectfully note though, that this is in a more limited role and only within the context of our CBDL proposal.

Cap on offline amounts. All in all, RF-storage-cards emulate physical cash – today, when an owner loses their wallet, they care more for any personal items they have in the missing wallet (such as driver's license, credit cards, etc) rather than the dollar bills it may contain. Finally, the introduction of RF-storage-cards poses a favorable trade-off between security and risk due to the limited amount of CBDLs they are allowed to contain. This trade-off calls for slightly amending, or simply building upon the existing, Design-for-Security hardware/software TEE standards that semiconductor companies should welcome. In closing, RF-storage-cards should be anonymous, but this does not prohibit the bulk of the respective transactions being the same for AML/CFT purposes since loading a card or storing the CBDL in a regular wallet both involve online access/syncing to the respective owner's NB wallet. To avoid triggering certain AML/CFT record-keeping requirements, non-traceable offline transfers via CBDL-cash-cards need to be for less than $1,000. However, in the context presented here, we envision a much smaller limit per card in the

[17] Of course, as a further example of the system functionality, they can transfer to the secure enclave of their phone while this is offline, but these CBDLs will not be account-settled until their phone comes online.

proximity of $200 so these cards only mimic the use of cash for day-to-day transactions (gas, movies, food, etc) and mitigate the security risks that their low-cost hardware entails.

The final amount would need to be calibrated to the most likely users and/or use cases. According to the market research in [35], the average Canadian holds $136 cash in their wallet and has $460 in cash holdings elsewhere. The same survey shows that people with lower financial literacy, lower education, and lower income use cash more regularly. It is important that users first become comfortable with the usage of CBDL-cash-cards and understand that they are cash-like and not bank account/deposit-like. In striking a balance to have limits that are high enough to satisfy user needs with limited risk of loss, we recommend proceeding with caution and to initially restrict the total amount of money that an offline card may carry. Finally, the intended CBDL-cash-card users are those without regular access to the cell network, not the average Canadian, or those who have a temporary disruption to internet access (driving in remote places, etc). Since the survey does not reveal the geographic distribution of cash holding habits, more research is required to calibrate the amounts to the needs of the intended users.

Resilience, privacy and security with offline transactions/cards. China's DCEP experience with the digital Yuan provides guidance to address this question. Coincidentally, our proposal falls into this realm as: *i)* CBDL-cash-cards provide an e-KYC-based on/off-ramp process, and *ii)* their conservative CBDL cap-limits discourage AML/CFT activities (when compared to the anecdotal status quo of "physical cash stacked in suitcases," where the government has very little control for AML/CFT).

Are offline cards a new bearer instrument? A bearer instrument is usually an item that can be transferred without a record. Without enabling tracing, one can therefore argue that the tokens in offline wallets may indeed be quasi-bearer instruments, but one should also note that those cards are linked to the owner's e-wallet for CBDL deposit/withdrawal.

What happens if a card is lost or stolen? CBDLs are a cash alternative and should be seen and treated as such. If a CBDL-cash-card is lost or stolen, the user will lose these funds (just like today with physical cash when a wallet is lost or stolen). If a user loses his or her smartphone, the NB will not be able to restore the funds in the card, but it will be able disable the e-wallet in that phone. Following, the user merely has to obtain a new smartphone and activate their underlying wallet using their unique e-KYC ID data (akin to cryptocurrency wallets today). In Phase 2, service providers who may hold proxy-custody of user CBDL funds will be responsible for conducting this recovery process.

CBDL cash cards as an additional mechanism for inclusion. For the rare cases where people never have access to the internet (*e.g.*, as they never get access to a digital device), we envision a similar card-like device that holds a specific number of CBDLs. This low-cost device would be registered via e-KYC to a particular user and it can be loaded with a small number of CBDLs by a government agency, at a post office, or an ATM.

4.4 Phase 2: The Decentralized Messaging Platform

4.4.1 Motivation

In the current world of payments, electronic transfers are either easy but expensive (*e.g.,* credit/debit card transactions), or cheap but cumbersome (*e.g.,* wire transfers). Notably, despite advances in technology and reduced technology costs in the past two decades, banking services remain expensive and cost savings have not been passed onto the end consumer [36]. The purpose of Phase 1 is to spearhead and establish CBDLs as a novel payment tool for cost-effective, fast, and easy cash-like transactions that can also accommodate participants in the new IoT/5G-and-beyond/AI digital economy.

Phase 1 provides baseline, commoditized-type transaction processing with basic functionality and APIs. The purpose of Phase 2 is to enable the private sector to innovate "fairly" under rudimentary regulatory supervision by the NB/BoC. Private sector *licensed* service providers will leverage the CBDL payment platform from Phase 1 to build innovative fintech/data services (*e.g.,* fintech reward programs/applications, IoT services, data analytics, etc.) through the expansion of the original centralized ledger into a permissioned blockchain. This provides an exciting new set of incentives for the private sector to innovate and generate new profit channels both domestically and internationally, either as service providers, or as one of the few approved validators in the NB/BoC-supervised consortium.[18]

4.4.2 Phase 2 Architecture

Baseline Mechanism and Architecture. Figure 6 depicts Phase 2. Expanding the principles of technology and system architecture in Phase 1, the second phase transitions CBDLs into a distributed ledger/permissioned blockchain with a limited number of licensed *validator nodes*, operated by carefully selected entities (in our view, major FIs and telcos). In this DLT the NB will be one of the validating nodes with supervising authority as described later in this subsection. Apart from those few validators, other private sector *service provider nodes* will have access in Phase 2 to commit transactions.

A side effect of the expansion in Phase 2 is that the stream of transactions among the quasi-anonymous wallets now becomes visible to all validator nodes. Evidently, this introduces a risk as those validators will now have an ability to snoop the full extent of cash-like CBDL transactions across all Canadians. The obvious downside is they may leverage this information to trace, and possibly identify, the individual businesses/citizens behind the identifiers and their market behavior, with whatever commercial benefit this may entail to them, or security risks this poses to the government/public. Therefore, in this phase the BoC/NB would need to employ further Privacy Enhancing Techniques (PET) such as mixers/tumblers or one-time-addresses (similar to the pseudo-random identifiers utilized by the Aadhaar system) with seeds that periodically change during NB's overnight housekeeping. In this way, the NB will obfuscate data from the private validators. Zero-knowledge proofs can also be employed, albeit with a cost to transaction settlement latency,

[18] We believe that the selection of the validators/service providers and the context of the services that they provide raises a set of interesting policy questions which, however, go beyond the scope of this work.

as further discussed later in this proposal.[19]

Architecturally, private validator nodes can also serve as "entry points" for users and other service providers to commit transactions (no different to existing commercial banking services today). This allows them to provide branding services and further reduce operational demand on NB's resources. In the case of service providers, they will be committing their transactions to the ledger either by using the standard APIs or (eventually) with their own smart contracts once they are approved by the consortium of validators. In both cases, ledger transactions will be processed and settled by the consortium of validators. Examples for third-party service providers could be SMEs, franchises, IoT providers, or even private small businesses that want take advantage of this new distributed marketplace. Since CBDL user wallets have already passed e-KYC, service providers are expected to face significantly lower bars to entry and regulatory burden. Section 8 discusses potential amendments to existing AML/CFT regulation to secure the above distributed ecosystem.

As described earlier, CBDL e-wallets operate under a quasi-anonymous veil. However, entering Phase 2, the users may want choose to reveal their identity and/or their transactions (or, by using ISO20022 tags, a subset thereof) to a particular validator or a service provider in exchange for perks or services. This will allow the commercial entity to obtain a better view of an individual's transaction history and decisions (*e.g.,* clothing brands, food/restaurant/gasoline trends, etc), while it enables the users to "bargain" in exchange for additional services, credit, discounts, and other perks for revealing part or all of their data. This practice promotes an environment with fair market competition and provides incentives for economic innovation. Finally, it is our recommendation that wallet creation continues to follow the Phase 1 approach where CBDL wallets are created by the NB and not by FIs to ensure that the system remains open, does not become siloed, and consumer privacy continues to be shielded. Since wallet balances are kept on a blockchain and overnight housekeeping is conducted by the NB to sign-off balances before the next day, users are formally not depositors and thus validators cannot use their participation as a basis for banking-like operations.

Figure 6 illustrates the elements of Phase 2. The NB's Phase 1 central ledger architecturally expands into a permissioned DLT system (2) where the NB now is simply one of the validators (1). Businesses or consumers, both owners of CBDL wallets, will have the ability to enter into service arrangements with either the validators (such as major banks, telcos, etc – in green) or other third-party service providers (in blue), for instance, in exchange for data of their NB wallets (3). Subsequently, they will have the opportunity to reveal all or part of their identities and transaction data to receive various perks. In this system, service providers deliver the services agreed with the user (4) while validators (through permissioned consensus) process all the transactions/transfers among the various wallets. The BoC performs general housekeeping (such as system-wide AML/CFT checks, restoring lost wallets, registering court orders, etc.) overnight (5) and eventually certifies

[19]The fourth phase of *Project Stella* by the ECB and Bank of Japan [37] focused on the implementation and classification of PETs to balance confidentiality and auditability of transaction information in payment and settlement DLT-based systems [23, 37]. We refer the interested reader to that work for more technical details and trade-offs.

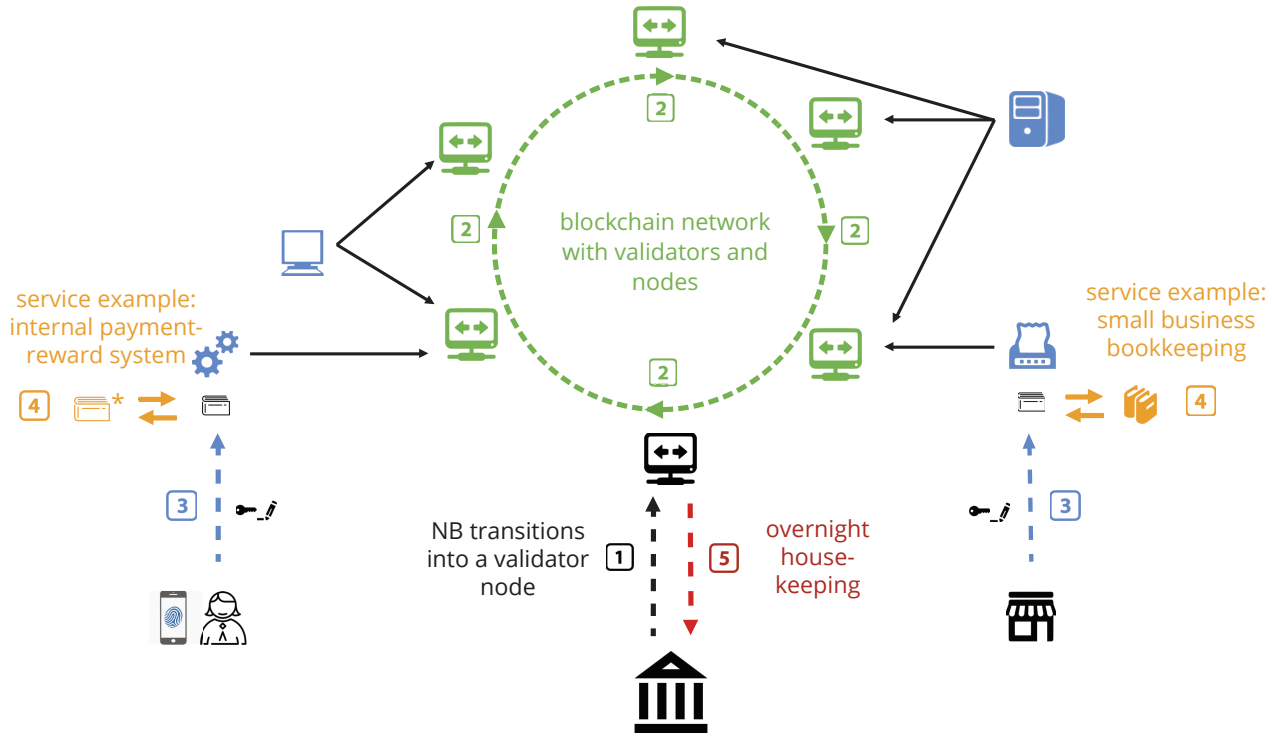

Figure 6
The Phase 2 Blockchain Architecture

the state-of-the-ledger to kickstart operations for the next day. Finally, it is important to note that in rare times of a *systemic crises/stress*,[20] the system will be reduced to the centralized Phase 1 ledger with reduced functionality (*i.e.*, without the processing smart contract perks but only basic CBDL functions) wholly operated by the NB as a single validator to consolidate/stabilize it.

Part of the rationale behind Phase 2 is to reduce the load and costs on the BoC's infrastructure as the CBDL system evolves. As the CBDL APIs will be open, and with the expected introduction of foreign-CBDCs and cross-border CBDC-transmission-mechanisms that may rival SWIFT, transaction processing and commerce is expected to dramatically increase possibly (and desirably) beyond Canadian borders.[21] This benefit should be further viewed under the angle of IoT/AI transactions in modern high-throughput networks. For example, advances in permissioned blockchain systems in recent years easily accommodate a throughput that exceeds that of existing commercial payment's systems by an

[20]This scenario strictly means "financial crises" and not cyber-attacks. Existing peer-to-peer permissionless systems, such as Bittorrent (in operation for 20 years now), Bitcoin and Ethereum, they all have exhibited high levels of system-wide resiliency against cyber-attacks. By architecture, closed-permissioned systems are even more secure than the aforementioned permissionless ones.

[21]See a recent article in Russia Today.

order of magnitude.[22] Further, modern IoT system require micro-transactions of highly time-sensitive data traffic (in terms of both high-volume and real-time/low-latency) in denominations of one cent or less. Such transactions can easily run on a private dedicated "side-chain" DLT system between the interested parties, and periodically settle them with the Phase 2 infrastructure. Admittedly, these types of operations are not accommodated by legacy payment systems today, and further, the vast data transmission/harvesting processes can put significant stress on a centralized system. The introduction of a DLT allows the private sector to innovate by creating side-channels/markets (akin to layer 2.0 efforts in permissionless blockchains today) that settle only periodically onto the distributed ledger. Moreover, the duplication of data and processing by trusted third-party validators will significantly improve the system resiliency, redundancy, data-availability, and fault-tolerance.

Finally, innovation, entrepreneurship (from both the public and the commercial sectors) and "healthy" competition will arrive with the introduction of additional APIs or dapps by the validators, but also by other third-parties. All new pieces of smart-software will need be approved by the system validators and pass strict formal verification programming benchmarks to ensure correctness — no different to what happens today with the Google and Apple app-stores. All in all, also discussed in more detail in Sections 4.4 and 7, Phase 2 provides all the proper economic incentives to build a balanced *socioeconomic operating system* at a global scale under the auspices of the BoC/NB with the assistance of approved private validators that generate revenue for the NB (through transaction fees) but also to themselves (through innovative services) while absorbing operational costs.

More on the Rationale/Role of the NB in a DLT Environment. The NB will remain a transaction processing validator in Phase 2 and it will retain central rights/privileges that are both necessary and sufficient for the security and resiliency of the system. A prerequisite for this expansion is that the Phase 1 technology allows some rudimentary programmability for CBDLs through the use of basic APIs. In the alternative where the NB maintains the platform for all those "upgraded" functionalities, it would need to continually upgrade its centralized technology to meet the ever-increasing needs of its constituents. This is a practice that we advise against because as computing continues to evolve exponentially, this becomes a costly proposition beyond the NB's core competencies. Instead, with our proposal the NB provides a fast but basic service in Phase 1 and lets the private sector manage the needs/costs of the ever-evolving market/technology trends in Phase 2.

During Phase 2, where private entities are expected to offer technical services to increase and/or capture new markets, the NB will need to mandate *programmable-CBDC standardization* to allow third-parties to build network overlay fintech/data services, but also to "communicate" with other emerging foreign CBDC projects. Evidently, the BoC has already demonstrated success in this department with their collaboration with MAS during the fourth phase of Project Jasper/Ubin. Further, to reduce AML/CFT risk, dapps that provide payment overlay services may also be required to register as money services businesses with FINTRAC. Finally, as a member of the Committee on Payments and

[22]For instance, Payments Canada's Automated Clearing and Settlement System processes about 30 million transactions per day [38].

Market Infrastructure (CPMI)'s *Cross-border Payments Task Force* for the Bank of International Settlement, Phase 2 also provides the BoC with an opening to lead the *global standardization* efforts for CBDC cross-border payments in the G20 task-force.

Validators vs. Service Nodes Although FinTech startups or even non-FIs such as Tim Hortons could become (non-validating) service nodes in this system, we believe that only BoC-approved entities, likely major banks and telcos, may qualify as network validators in the Phase 2 DLT. This is because validators need to have significant experience with the handling of sensitive private data. In contrast to the current siloed world of banking, however, the proposed DLT setup ensures that there are no intrinsically captive consumers but that the system is open and that validators abide to its "open competition" incentives to onboard third party service providers so as to enjoy new revenue streams. Validators in the DLT work cooperatively to verify/settle the transactions submitted and to maintain the consistency of the ledger. However, other private/public service providers may be able to deploy authorized DLT applications in Phase 2 for their users without a validator license. For instance, Tim Hortons may want develop a smart contract dapp for its rewards program. When a customer uses CBDLs to purchase coffee, they may choose to interact with this deployed smart contract to receive rewards. All such transactions from whitelisted wallets to the smart contracts are automatically and faithfully executed by validators of the DLT. In this picture, Tim Hortons does not need to be a DLT validator to submit such transactions. To take this concept further, as elsewhere noted in this paper, different entities may want to create their own permissioned/permissionless side-private DLT-channels that "communicate" with the CBDL network through the public Phase 2 APIs.

Clearly, as CBDLs evolve in Phase 2, one policy decision is how to regulate the third-party deployed smart contracts. Smart contracts can be used by FinTech startups to encode transaction rules for money services business or traditional companies like Tim Hortons to provide non-monetary services, as seen in the example above. The conservative approach would be to require them to obtain prior authorization from the NB and the handful of validators and pass some standard formal code-verification/auditing procedures [3], etc. Validators and service providers who offer money services would also need to register with FINTRAC. Finally, the NB's constituting statute should include a process for licensing third party payment services providers under the oversight of the BoC — this registration process is further discussed in Section 8.

Checkpoints and Overnight Housekeeping. Since CBDLs resemble cash, users cannot spend into a negative CBDL wallet balance. This has consequences for users but also for the NB: all wallets will always be fully funded and cannot incur accidental overdraft charges. Furthermore, the NB is not a lender — borrowing and lending is the role of the traditional banks. Therefore, the NB creates minimal intrinsic financial stability risk. It is important that this lack of risk extends to Phase 2, in that service providers do not engage in lending activity or internal clearing. Furthermore, in contrast to the traditional world of banking where overnight settlement acts as a buffer to stave off run-risk, the immediate settlement of transactions on the blockchain would create unprecedented run-risk if entities

were to engage in CBDL-based lending. In other words, Phase 2 will not enable any of the private validators to declare wallets as deposits and use them as a basis for banking activities. However, service providers or validators may engage in some form of bank-like activities if a wallet's owner gives permission to do so, *e.g.*, by creating service wallets that become de-facto deposits to later make loans in the form of margin accounts for securities trading. Run-risk should therefore be one of the criteria in the service licensing process.

As such, the NB will need to perform housekeeping checks on CBDL accounts overnight. These checks will ensure transaction accuracy and compliance, including tasks such as AML/CFT checks, restoration of lost wallets, clarity of where/how wallet funds have been flowing, or even "burning" of CBDLs.[23] Those overnight checks by the NB will prevent abuse of funds, and the regular auditing of CBDL holdings will create a level of certainty for Canadians reaffirming their trust in the government/system by making sure that everyone is "playing by the rules". Once this CBDL information is validated, the NB will certify the ledger from transactions of the previous day, and give the "green light" to process/settle transactions again for the next day in real time onto the blockchain.

New Business Opportunities. Many entities may want to provide payment services in CBDLs; others may provide add-on services over the network through the APIs/standards available. Firms such as Starbucks, Disney, or international providers such as WeChat or PayTM have found numerous applications such as rewards, discounts, as well as IoT product apps to attract customers to their internal payments systems. We imagine that further innovative offerings will ensue when firms can process payments without passing through the complex and expensive links of the legacy financial sector. Additionally, as other jurisdictions are actively engaging in pilot CBDC programs, this presents a plethora of new instruments/tools for cross-border payments. As such, we feel that elaborating at depth on the technical details behind all those new opportunities that Phase 2 enables is outside the context of our work.

5 AML/CFT Compliance

Anti-Money Laundering and Combating the Financing of Terrorism describes the set of laws, regulations and procedures aiming to protect the integrity of the financial system by preventing criminals from enjoying illicit profits or from conducting illicit activities [23]. Although most countries and supranational organizations provide their specific frameworks, the general structure of AML/CFT measures in the past few decades have been somewhat harmonized across jurisdictions. In most cases, a set of regulated entities is required to provide "active cooperation" to the particular authorities in light of their perceived oversight capacity. These entities range from commercial banks and financial institutions, to

[23]The option of whether the bearer of CBDLs (in the case of offline cards) has the capacity to destroy/bury/melt them, another intrinsic property of physical cash, is an interesting yet long one to debate. As such, we feel it is beyond the context of our current response here to sample its philosophical, technological and historical implications. Nevertheless, our design parameters allow for this option.

professionals (such as lawyers and notaries), to casinos and art galleries. There are numerous AML/CFT duties, and discussing them here goes beyond the scope of this paper. To highlight a few, they encompass licensing regimes, Customer-Due-Diligence obligations such as Know-Your-Customer and ongoing monitoring (*e.g.*, transaction scrutiny), as well as record retention and Suspicious Transaction Reporting.

Our design implies that the NB undertakes a costly compliance effort and keeps records quasi-anonymous since it is the sole processor of CBDL settlement in the Phase 1 platform. However, since CBDLs are intended to mirror cash flexibility/usability, it makes little sense for procedures to verbatim resemble those of traditional bank accounts. Moreover, in Phase 2, a significant portion of the compliance burden should be shifted to the private entities offering CBDL products/services to the end-users as it already happens today. A key question relates to the responsibility for compliance duties, account management, and identity/transaction checks. The delegated e-KYC process proposed here will leverage the compliance efforts that have already been undertaken, for instance, by government agencies and commercial banks. Hence, our proposal leverages existing customer-facing services and avoids the unnecessary duplication of KYC efforts. Section 8 discusses certain amendments to existing AML/CFT regulations to support this streamlined process.

As we examined earlier, CBDC designs entail different trade-offs at multiple levels. Likewise, there is a correlation between those trade-offs and AML/CFT provisions when it comes to anonymity/privacy. Notably, any interlink between technical and regulatory compliance builds on the assumption that the latter can be embedded into the technology itself. This concept is at the root of contemporary *regulation-by-design* schemes [23] as a means to foster socially and legally desirable outcomes, and in contrast to traditional "command and control" approaches such as prohibitions and sanctions. In other words, the notion that compliance aspects not only can, but they *ought to* be taken into account from the early stages of the system design or process is gaining momentum among law and technology experts today, and it should be applied to the design of CBDCs. This forward-looking approach requires preliminary engineering and standard setting as to said regulatory goals and available tools. Choices are seldom binary and need to be made early in the design cycle with interdisciplinary teams cooperating from the beginning.

Section 8 outlines existing AML/CFT Canadian regulations and canvasses avenues to tailor it for CBDLs. With the above considerations in mind, in the remainder of this subsection we strictly elaborate on the technical aspects of CBDLs for AML/CFT compliance.

5.1 AML with Online Payments

All e-wallets undergo an e-KYC-process, performed by licensed entities (previously referred to as "approved authenticators") such as FIs, Telcos, or provincial and federal service providers. In other words, qualified wallet holders are indeed "registered" users. Once a person passes e-KYC with an approved authenticator, their wallet address will be added to a whitelist of authenticated wallets with the NB, and it will contain information on the authenticator and the type of entity that has been authenticated (individual, business, visitor). Beyond this information, the whitelist will have no direct link to individuals

to preserve privacy. An identity can only be uncovered when a law enforcement agency obtains a court order for the authenticator to release information about the person behind an identifier, or if it is required to be reported to FINTRAC to comply with AML/CFT obligations. Until this point, the NB will only store the absolute minimum data required in order to perform homomorphic encryption techniques to remain AML/CFT compliant. All transactions will also be quasi-anonymous, that is, a merchant, for instance, will not be able to receive any information about the purchaser other than the proper amount of the CBDLs – unless the purchaser elects do so for perks/discounts. We refer the interested reader to the Indian Aadhaar system that has successfully implemented similar procedures [30].

The NB processes/settles payments between wallets and maintains the account balances. Since CBDLs are envisioned to be a cash replacement system, we expect most transactions to be small and below the Money Laundering/Terrorist Financing indicator thresholds. Transactions processing may allow for further data fields, based on ISO20022 messaging standards, to explain transactions that may exceed limits (*e.g.*, large purchases, small business transactions, types of merchants, etc.) and to enhance the automation of the analysis. All transactions undergo AML/CFT compliance checks at the NB to ensure compliance with the 2001 Proceeds of Crime (Money Laundering) and Terrorist Financing Act. Records that are not required to be kept under AML/CFT regulations are to be destroyed once the checking process has been completed and suspicious transactions are reported to FINTRAC, which can then uncover the identities from the authenticator and investigate further following their standard protocols.

5.2 AML with Offline Payments

An offline CBDL-cash-card is an RF-storage-card that receives a capped number of CBDLs from the user's e-wallet when the latter is online. As the transmitting device is online during this exchange, the account of the recipient will be debited this amount with the NB instantaneously. The reverse process also holds, that is, users can transfer funds from the remaining balance in their RF-storage-card back to their smartphone wallet when the latter is online, a transaction that credits immediately their NB account. CBDLs transferred into these CBDL-cash-cards will come in the form of "unique" tokens, akin to the practice for physical bills. Recall that each e-wallet requires the owner to pass e-KYC. Therefore, when a card syncs with a wallet (to either deposit or redeem CBDLs by the user) there is a cryptographically-protected knowledge of the wallet owner (and respective sync-transaction) to the NB.

Evidently, it is possible that somebody (Alice), who just synced her card with her phone transferring a number of CBDL tokens, passes it to another person (Helen), who again passes it to another person (George) and it ends up in the hands of a fourth person (Bob) who syncs this card to his card, and then later syncs it with his online device to collect the money. In this chain of events, only the activities (*i.e.*, identities) of Bob and Alice will be recorded by the NB. Respectfully, we do not believe that this a drawback of our proposal. In fact, this characteristic replicates the real-life use of physical bills in Canada and internationally. Although one may argue for laws to prohibit individuals from

passing CBDL-cash-cards to one another, we find this a futile practice in view of how cash has been historically used. Moreover, such laws may significantly limit the appeal of those cards or their use for tourists/visitors to Canada. Finally, it would also be a practice that goes against the overall tone of our proposal for the BoC that emphasizes the protection of privacy of CBDL users/transactions (subject to AML/CFT screening).[24]

Further, we suggest that every e-KYC registered device can be associated only with a single CBDL-cash-card. Additionally, such cards can be programmed so they can be synced to work with only one device, that is, with the smartphone it was first issued for. As such, a card can be disabled if it is lost or stolen. Compounded with the limited CBDL storage in such cards, these measures should limit, if not vastly alleviate, most concerns for CBDL-cash-card illicit trafficking so as to promote CBDL transfers *only* between "legitimate" e-KYC-ed users. In contrast to online CBDL transfers, the offline CBDL transfers would, however, be untraceable because records are only established when the offline wallet is loaded with funds or when funds are redeemed. We do not expect this to violate any AML/CFT record keeping requirements as the CBDL-cards will be programmed to prohibit transactions of a size that would trigger certain AML/CFT obligations. Please note, under the current regulatory regime, banks are not required to keep records for certain electronic fund transfers under $1,000 either. Hence, roughly speaking, limiting offline CBDL transfers and holdings to similarly low monetary thresholds ensures harmonization and compliance with existing laws.

6 System Architecture vs. Policy Objectives

As discussed in Section 2, the BoC identified five key policy features: *privacy, universal access, security, resilience,* and *performance*. In this section, we revisit the key components of our proposed CBDL design in light of these requirements.

6.1 Privacy Protection

Without loss of generality, and for the sake of brevity, in this subsection we touch upon privacy concerns for Phase 2. This is because that phase executes a "superset" of tasks and operations when compared to the centralized tightly-knitted first phase.

As extensively discussed in subsection 4.4.2, CBDL transfers are between wallet addresses and we separate transaction processing from authentication so that transfers remain quasi-anonymous and validator nodes do not know the underlying identities of the

[24]We understand that in recent announcements, the Digital Dollar Project and the ECB painted for the development of CBDCs that have no, or very limited, privacy so as to ensure that CBDCs cannot be used by "bad actors". In our view, unpacking the privacy of payments has its own risks, and the decision to do so requires a broad political and social discussion that is beyond the scope of this paper. Completely de-anonymizing CBDLs (apart from AML/CFT) would also encourage the proliferation of alt-coin alternatives that defy this practice. Stopping such developments has proved to be impossible no matter the regulation; one example is the "bittorrent" media evolution, *e.g.,* see [39]. Our preference is to lead global practice with a "Canadian solution" that has strong user privacy protections with embedded *privacy-by-design* [40].

transacting parties or the flow of information into the ecosystem. In that subsection, we also described special provisions for overnight checks by the NB to homomorphically parse the data so to trigger potential AML/CFT and other regulatory red-flag conditions. The mechanisms described in subsection 4.4.2 add negligible overhead vs. the relatively low scale in amounts of transactions expected by CBDLs. Another alternative to further enhance privacy and make transactions virtually anonymous are zero-knowledge proof techniques (*e.g.,* zkSNARK) that we touch upon a bit more here. In our context, processing a transaction is equivalent to validating the following three statements: 1) the transaction signature is compatible with the respective public-key; 2) the public-key has been whitelisted; and 3) there is a sufficient balance associated with the public-key wallet to enable this transaction. When we apply zero-knowledge proofs to CBDL, instead of sending normal transaction information, users will act as the prover to generate a proof for the above three statements in the transaction. Here, the NB could act as the validator to the proof statement. Although a zero-knowledge proof transaction is fully private, there is a trade-off: it involves a significant computational overhead on the user/prover side and substantially more time than the processing of a simple homomorphically encrypted transaction (*i.e.,* CBDL users would need tens of seconds per transaction rather than a few milliseconds).

6.2 Universal access

A key component of our design proposal is the integration of offline cards. This process allows for individual e-KYC registered users to transact when there is no access to the cellular network. This makes our design suitable irrespective of geographic location. It also allows unbanked, or individuals with no electronic devices such as a smartphone, to transact in the CBDL ecosystem.

6.3 Security

CBDL account balances will be maintained by the NB/validator network, and e-wallets require biometrics/PIN to operate, similar to credit card- or smartphone-based transactions today. As such, CBDL wallet security will be based on the built-in security of the user's device that today handles remote accounts with much larger limits than CBDL e-wallets do. Finally, as noted earlier, the security of offline cards presents a desirable trade-off with their capped limits.

6.4 Performance

According to Payments Canada's latest 2019 report, there were 21.1B transactions in Canada in 2018, out of which 21% were in cash. This adds up to around 12 million cash transactions per day. Payments Canada's current dated systems process less than 30M transactions per day (debit/Interac) on average. Even if CBDLs subsume all cash transactions and a portion of debit/credit transactions, the total number of daily transactions is quite manageable. Although CBDL transfers by the NB would require different

processing architecture (*e.g.*, because they involve record-keeping), the volume of CBDL messages appear comparable to what Payments Canada currently manages. As another point of reference for message-heavy systems, consider Nasdaq Canada, Canada's second-largest equity trading provider. According to IIROC data, its systems currently process approximately 100M messages per day — yet it employs less than 20 people including staff for sales and administration. Finally, in having to keep track of the data-usage of cellphone customers, telecommunications providers process numbers of transactions that are orders of magnitude larger than those of the payments system. Therefore, the requirements for the NB's CBDL settlement system in both phases do not appear to be overly onerous.

6.5 Resilience

Disaster scenarios and the handling of system downtimes is beyond the scope of this proposal. However, we note that these questions touch upon standard problems in networks and distributed system fault-tolerance, and they can be addressed within existing typical industrial standards/literature/solutions.

6.6 Minimum Functions

As onboarding relies on existing commercial and government infrastructure, this will immediately enable all Canadians who have an account with a Canadian regulated financial institution to use CBDLs. Once a user passes e-KYC, they can register, and subsequently fund, their e-wallet from commercial bank accounts by a simple EFT. Following, they can start using the bare-bone functionality of their e-wallets and offline cards to compensate merchants or to send/receive money to/from other peers. Evidently, this is no different to what they are already doing today with their credit cards, Google/Apple Pay, PayPal, WeChat, etc. accounts.

7 Alignment with BoC's Business Plan

7.1 The CBDC Contingency Plan

As noted in Section 2, the BoC made it clear in its contingency planning that it would (seriously consider to) issue a CBDC if one of the following conditions applies:

- the use of bank notes were to continue to decline to a point where Canadians no longer had the option of using them for a wide range of transactions; or
- one or more alternative digital currencies —likely issued by private sector entities— were to become widely used as an alternative to the Canadian dollar as a method of payment, store of value, and unit of account.

In this subsection, we discuss how CBDLs promote Canada's prosperity, social values and global competitiveness when the above condition(s) are triggered. In the remainder of

this introduction, we further respectfully amend them with *three additional issues* that the BoC may want to consider for triggering the need for a digital currency. First, in a digital economy, physical cash is obsolete: one needs to convert cash into a digital format to use it. For instance, some online merchants accept only credit cards, and only a subset of people have access to credit cards. With the recent pandemic, this trend has already spilled to real-life/physical merchants. As such, regretfully, people who have no access to affordable electronic means of payment are already de facto excluded from the digital economy.[25]

Second, Canadians continue to show a preference for cash payments over credit or debit payments when cash is available. More than 20% of transactions today still happen in cash even though it has been reported that more than 99% of Canadians have a bank account and therefore, they can presumably pay with a debit or credit card. There are a number of reasons for this preference (see [35] and [41]). For instance, more than 30% of Canadians carry a balance on their credit cards and by using cash to manage their finances, they can avoid incurring overdraft charges and adding to their debt. For these people, cash is critical; after all, it is an open-kept secret that in today's world of banking, low-income folks who carry credit card balances and pay fees galore subsidize the free perks of those who don't [13].[26] By using cash, people can also protect their transaction data from private third-parties that may want harvest it. Finally, as the BoC already acknowledges, implementing CBDCs is a multi-year process that requires both expertise and experimentation. Once cash is naturally no longer accepted in a wide range of transactions, as we argue below, it may be too late or mundane to establish CBDCs as a new payments method.

7.2 Contingency Conditions Triggered: Now What?

The Bank of Canada defines a *CBDC business model* in terms of its value proposition to key stakeholders (namely, individuals and merchants), its ecosystem robustness, its interrelationships/interoperability, and its alignment on the specified public policy goals.

Canada's banknotes are currently distributed through Canada's major financial institutions. *Can this model form the basis for the distribution of a candidate CBDC?* The practical implication of this approach is that the BoC would issue digital tokens that would be distributed to the public but transferred on a system operated by the existing major commercial financial institutions. Respectfully, we are skeptical that this approach may work once the contingency conditions for a CBDC are met. Arguably, at that point it would certainly not be in the "best interest" of financial institutions to proliferate a system that runs parallel to the existing payments network.

Namely, if the first condition of the BoC's contingency planning is triggered, then it must have been the case that the private sector, including financial institutions, were successful in convincing consumers and merchants to transition to electronic payments (electronic funds

[25] There are some work-arounds such as purchasing a pre-paid credit card with cash from private vendors. Converting physical cash to digital money in this way, however, may be prohibitively expensive (current activation fees for such credit cards are between 12-20%). Thus, it stands to reason that these high fees hit those the hardest who already face high barriers to participate in the digital world.

[26] See the Brookings Institute's research or for a lighter fare, Michael Lewis's newest podcast series.

transfers, debit cards, credit cards, Google/Apple Pay, WeChat, Facebook Diem, etc). In that case, why would those same institutions want to distribute to the public –let alone bear the cost to run– a CBDC system that has the potential to cut profits from existing commercial e-payment channels? By definition, when cash usage declines, which is the trend in the past two decades, the revenue streams from e-payments services increases. It is therefore difficult to see how commercial entities could earn new revenues when operating a CBDC system with nominal fees alongside their existing payments channels without also fearing to cannibalize their existing revenues.

If the second trigger condition applies, then one of two things will have happened. In the first case, commercial banks are the source (or they are simply deeply involved) in the production/dissemination of this new digital currency. This case duplicates the concerns in the paragraph above. The alternative case is one where commercial banks are not at all involved and have therefore been unsuccessful in convincing customers to continue using their existing e-payments systems and/or their in-house digital alternative(s). The likely scenario for this outcome is one where an alternative digital currency provider has developed a business model, likely involving add-on services just like those that Facebook's Diem has announced or that PBOC's DCEP is rumoured to be doing, that users find superior to what the traditional financial sector offers [13]. It is not clear why a "bare bone" CBDC offered directly by legacy financial institutions would be now a catalyst for a "competitive new CBDC ecosystem" that tackles this "super-currency" that made those same legacy institutions obsolete in the first place.

A key principle of commercial banks (or colloquially, of any corporation) is to prevent "anyone from getting between them and their customer". Under established business models, a key benefit for a bank is the ability to cross-sell services and products. By their own estimates, Canadian banks already have almost full coverage of the Canadian population and businesses. Hence, there is a fair argument to be made that CBDCs would not enable them to add more customers or cross-selling opportunities. Therefore, it is difficult to imagine a model that incentivizes them to establish a new parallel system.

In summary, we strongly believe that for the benefit of the Canadian public/economy, it is both *sufficient but also necessary* that the BoC undertakes *solely* the investment to build a CBDC payment system that does not require legacy components. This is our Phase 1 design. We also believe that *only* such a route can set the well-needed disruption to the "legacy" status quo so to enable a plethora of new incentives for commercial participants innovate, proliferate and compete in a fast-paced new global economy, as set out below.

7.3 The Incentives Embedded in Our Design

The proposed two-phased CBDL approach has a "carrot and stick" approach to positively disrupt established practices for the benefit of the Canadian public in a new global economy where one urgently needs to remain competitive in the AI/5G-and-beyond/IoT era so to remain both lucrative but also relevant [31]. Phase 1 establishes a benchmark with a user-friendly, fast, cost-efficient, bare-bone payment infrastructure accessible to all. It also sets CBDLs as the de facto payment tool for cash-like transactions. Phase 2 gives the private

sector an opportunity to innovate "fairly" yet competitively.

Our design provides incentives to collaborate with the commercial sector in several ways. First, in Phase 1 the FIs can assist by verifying the KYC that they have already performed. Next, FIs or other major corps could sponsor branded CBDL wallets/offline-cards as an advertising opportunity (this will not intrude any of the established technology and operation of those instruments). Third, Phase 1 provides entry-level APIs for the commercial sector to build rudimentary FinTech services. In Phase 2, the private sector benefits by participation in additional ways. Initially, entities can convince customers to provide them with access to their data, which would allow businesses to better understand their customers' spending behavior and thus make better product decisions. Next, Phase 2 provides a platform to build new markets based on IoT/AI technologies, all of which are not enabled by the existing infrastructure today. As those economies may involve cross-border applications one can only envisage the vast amount of new by-product business opportunities generated by CBDLs. Finally, FIs would be able to earn income from enabling access to the non-validating service providers.

To further incentivize participation from the banks, we have suggested several measures. To start, the initial allocation of CDBLs (during distribution) should be made in such a way that the conversion of deposits to CBDLs has no notable effect on banks' balance sheets (and thus funding costs); this would require an expansion of the BoC's balance sheet (*e.g.*, by endowing users with seed funding). Next, we suggest that licensing for the second phase is predicated on compliance and active support of CBDL distribution in Phase 1. As noted in Section 4.4, the introduction of a permissioned network in Phase 2 provides an exciting new set of opportunities for the private sector to innovate and generate new revenue channels *both* domestically and internationally, either as service providers, or as validators in the NB/BoC-supervised consortium. Further, the BoC can ensure policy-driven features (including CBDC interoperability [42]) through technology standardization and by its supervision of the validator consortium, but also through its membership in the CPMI's Cross-border Payments Task Force and through Canada's membership in the G20.

As also further elaborated in the next subsection, CBDLs are *not competition* to the existing banking world, but an *opportunity* for the "traditional" Canadian FIs to adapt in this new reality, innovate, and "not be left behind." To further validate this argument, just a handful of days before the publication of this manuscript, on January 29, 2021 the Korea Internet & Security Agency (KISA), in collaboration with other domestic government and private organizations, issued a 245-page market-report profiling the fast growing field of Decentralized Finance (DeFi), or as they coin it, this of blockchain-fintech [27]. To the best of our knowledge, this is the first government-funded research report for the DeFi sector. As a small economy next to a very large one, the Republic of Korea will likely soon feel the impact of China's forthcoming DCEP payment system; *thinking ahead*, Korea recognizes the need to "evolve" if they want their economy to remain competitive. In conclusion, there are many exciting reasons why the proposed CBDL design promotes healthy competition and state-of-the-art innovation in the Canadian private sector at both a domestic and global scale, as the BoC mandates in their business plan requirements.

[27] For the actual report (currently only in Korean language) see here.

7.4 Is the NB/CBDL System Competition to Commercial Banks?

We recognize that any new form of e-payment can be perceived as competition to existing payment channels by some incumbents, unless private FIs start running this system from the very first day. As argued above, this latter practice raises a plethora of concerns.

By concept and by architecture, CBDLs are intended as a digital complement for *cash* and therefore, it is only *proper* to be advertised as a competition to current *cash payments*. Our Phase 1 has a narrow use case, namely, the processing of CBDL payments. This is no different from physical cash today, which is a payments system that has competed with other means of payment for hundreds of years without imposing any significant direct costs on merchants unlike credit cards. CBDLs therefore need to replicate the minuscule-cost of cash operation. Cash is currently disseminated to the public via banks, and this is a costly process that they offset by the cross-selling of services. Similarly, the introduction of CBDLs will lower the need for cash and in effect, lower those costs for private banks.

Transaction processing itself is a commodity, not a valued-added service, and it should be provided to the public at (or close to) zero-cost. As such, pragmatically, CBDLs should not add competition in simple payments — any argument that asserts that this system changes the competitive landscape would implicitly need to assume that commoditized payments allow for "bank rents". In our highly competitive banking world, that is unlikely. The processing of payments by FIs today is arguably only a small portion of their payments value chain. The most critical service that commercial banks provide is liquidity to the market through credit arrangements (*e.g.*, credit cards, overdraft arrangements on chequing accounts, and lines of credits, etc.). Merchants benefit from this value-added service because credit enables users to make purchases even if they do not have the necessary funds at the time of the payment. Merchants who refuse credits cards in favour of CBDLs would most likely stand to lose customers. Also, by-definition, CBDL wallets and the NB do *not* provide credit. In Phase 2, FIs and other related entities can use the publicly-developed CBDL functionality to provide and facilitate more such value-added services.

7.5 Revenue Sources for the BoC

Our design enables three major sources of income/cost recovery: transactions processing fees; licensing fees for Phase 2 service providers; and, seigniorage income.

In more detail, according to Payments Canada's latest 2019 report, 21% of the 21.1B annual transactions in Canada in 2018 were in cash. The NB may want to consider a nominal, very small (that is, significantly smaller than the current credit cards) transaction fee that covers operating and financing costs on par to, or below, the fees by existing permissionless blockchains today. As a back of the envelope computation: suppose that 50% or 2.2B of the current cash transactions will be made in CBDLs, and that the NB charges a nominal amount of $0.01 per transaction (this fee may be paid by merchants, as it happens with credit cards today). Then the system will create annual revenues of over $20M, in perpetuity. This amount scales linearly in the fee and can therefore be adjusted accordingly. Phase 2 service providers benefit from the e-KYC process as well as the existing infrastructure, including this of smart contract auditing. Hence, the BoC/NB

should therefore be able to charge them an access fee that helps to recover ongoing costs of the operation. In addition to transaction revenue, just as with bank notes, CBDLs afford the BoC to earn *seigniorage*: CBDLs will be issued at face value in return for funds transferred by commercial banks. The BoC could invest these funds in securities issued by the Canadian government such as bonds and treasury bills earning interest; notably, in contrast to bank notes, the marginal cost of producing a CBDL is nominally zero.

7.6 Cost Sources for the BoC

7.6.1 Costs for the BoC

Roughly speaking, the BoC will have to set up three systems: the whitelisting for authenticated wallets on a highly secure government-distributed database; the NB that processes/settles transactions and account balances and anti-fraud checks; and, the new system and processes for monitoring CBDL transactions to ensure AML/CFT compliance. The system also needs to be engineered to allow ongoing maintenance and sufficient redundancy resources. This is clearly a major undertaking that requires significant upfront expenses.

Although a new ecosystem, none of the proposed architecture components require radical new inventions as they emulate daily routine operations by financial institutions and utilize existing technology. Additionally, the BoC will have to fund the development of the e-wallet app, entry-level APIs, offline cards, and update existing message transfer functions for point-of-sale merchant/smartphone transactions. If the BoC allows existing FIs to issue branded wallets, it may be able to convince these entities to contribute to the upfront development costs. Finally, the BoC needs to develop a licensing and system/service provider auditing system; it may be possible to outsource these activities to entities that have experience with audit-type activities such as accounting firms.

7.6.2 Costs for Other Entities

The e-wallet will be available free of charge for all users, individuals and businesses alike, in popular standard app stores and government websites. Whether existing PoS technology can accommodate the CBDL messaging functions is a discussion that the BoC needs to have with the providers of PoS devices. Since these providers will likely receive some of the revenue, they would have an incentive to update their existing technology to accommodate a new form of payment, and therefore, merchants should see only a limited impact on their operations. The NB will be a member of the payments network,[28] and therefore interacting with this new institution will generate no incremental costs for commercial banks and payments providers. Finally, we expect that the vast majority of users can be onboarded using existing systems. For instance, seven major financial institutions offer e-KYC via the Verified.Me app, and several start-up firms are working on digital ID solutions. Using these applications for e-KYC authentication should come at low cost. Likewise, businesses

[28] This may require amendments to the Canadian Payments Act to include the NB as a member of Payments Canada

with bank accounts would be authenticated by their banks. Our system also calls for authentication via public service entities. This process would require the development of separate, albeit simple systems, such as dedicated websites and smartphone applications.

8 CBDL Legal Considerations

In this Section, we present an overview of our preliminary legal considerations for the CBDL technical proposal. We identify aspects of the technical plan that raise legal issues, but also suggest possible approaches and solutions for the BoC to consider.

At early CBDL design stages, the BOC should focus on addressing the following issues:

1. The legal authority of the BoC to issue CBDLs;
2. Regulation and oversight of CDBL e-wallets and their exchange/settlement network; and
3. Considerations relating to AML/CFT financing regulations.

These three issues are discussed in Sections 8.1–8.4. Section 8.5 briefly outlines other legal issues for the BoC to consider at later stages of the design process.

8.1 Legal Questions: A Closer View

This subsection expands on the three legal questions identified in the introduction above. The first question asks whether the BoC has explicit authority to issue digital currency under the current version of the Bank of Canada Act.[29] Any legal or political challenges to the BoC's authority to issue CBDL may result in significant reputational damages for the BoC and the CBDL project. Averting this risk is discussed further in Section 8.2.

The second question pertains to the appropriate regulatory body to oversee the CBDL network. Phase 1 of our two-phased proposal includes the establishment of a single centralized entity (namely, the "NB") that manages end-user CBDL-wallets and is responsible for verifying transactions/settlement between wallets over a centralized network. The NB will be a separate legal entity from the BoC, but subject to BoC oversight. After end users complete the necessary e-KYC, they receive access to their personal CBDL e-wallet managed by the NB. This grants them access to the CBDL network and allows them to transact with other CBDL e-wallets. Each transaction is verified by the NB on the centralized platform, which will be responsible for confirming that every transaction is between verified CBDL e-wallets and that each party to the transaction has a sufficient balance associated with their CBDL-wallet. Notably, Phase 1 only contemplates basic CBDL transactions across the centralized network managed by the NB and the issuance of entry-level APIs.

With the above in mind, Phase 1 presents two critical legal issues. First, to support CBDL transactions, our model envisions the need for the BoC to issue CBDLs to the NB,

[29] Bank of Canada Act, RSC 1985, c B-2.

or equivalently, issue the NB a reserve account with the BoC.[30] Section 8.2 discusses the legal authority of the BoC to provide these reserve accounts. Second, the NB should be subject to regulatory oversight. Section 8.3 discusses options for the preferred regulatory body to oversee the NB. Finally, Phase 2 contemplates expanding the network to include service-wallets and the introduction of a permissioned DLT infrastructure. This raises the issue of which governing body should be responsible for approving and regulating network participants on the permissioned DLT network. Section 8.3 also presents four options for regulating these entities.

Phase 2 also involves expanding the CBDL network to include BoC/NB-licensed private service providers. These private service providers will be permitted to develop innovative fintech/data services on top of the existing network by creating proxy/service-wallets that connect with the end user verified CBDL-wallets with the NB. We envision that service-wallet providers will only act as custodial agents or provide data/payment services to end users; but there is also the option for the BoC to expand the scope of permissible services by allowing service-wallet providers to provide traditional banking services using CBDL. We discuss the legal implications of both alternatives throughout this Section of the Report. In both scenarios, however, no new CBDL will be issued directly from the BoC to private service providers and no additional KYC will be required. These licensed service providers and licensed network validators, however, should still be brought into the regulatory framework. Canada's current AML/CFT regulatory regime may also require amendments to support the introduction of service-wallet providers in Phase 2. Sections 8.3 and 8.4 discuss both issues accordingly.

AML/CFT requirements under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act[31] must also be considered. We have previously discussed our recommendation for an e-KYC process. Section 8.4 discusses some of the legal issues pertaining to our e-KYC recommendations in the context of Canada's current AML/CFT regulatory regime. Further, parallel to our phased account-based approach to CBDL, the model also needs to support offline CBDL payment methods that are either built into the processing units of end users' devices or facilitated via CBDL-debit-cards. This introduces a quasi-token-based approach to CBDLs that allows users to transact offline using CBDL-debit cards, as opposed to online transactions between CBDL e-wallets. As such, our offline CBDL-debit-card solutions presents additional BoC issuance considerations as well as new AML/CFT concerns that are addressed in Sections 8.2 and 8.4, respectively. Lastly, Section 8.5 provides a brief overview of additional legal considerations that the BoC should be mindful of in later stages of the design process.

[30] Alternatively, the NB could be funded by the federal government and could, in turn, purchase CBDL from the BoC.

[31] Proceeds of Crime (Money Laundering) and Terrorist Financing Act, SC 2000, c. 17 [*PCMLTFA*].

8.2 Legal Authority Of BoC To Issue CBDL

It is critical from the outset that the BoC ensures it has explicit legal authority to issue CBDL and oversee a CBDL payment network. Any legal or political challenges to the BoC's authority may lead to legal and reputational risks for the Bank stigmatizing the project. There are two aspects of legal authority that the BoC should consider: First, whether the implementation of a digital currency network is within the BoC's statutory-defined and politically accepted mandate; and second, whether the BoC has express legal authority under its governing statute to issue CBDLs [43]. We explore both those issues below.

The BoC's governing statute provides it with a broad mandate to "regulate credit and currency in the best interests of the economic life of the nation" and to "promote the economic and financial welfare of Canada."[32] The Payment Clearing and Settlement Act[33] confirms as well that the BoC has the authority to oversee payments and other clearing and settlement systems in Canada. The preamble of the Payment Clearing and Settlement Act and the definition of "clearing and settlement system," however, explicitly reference "Canadian dollar" payments.[34] To mitigate the risk that the BoC's authority to oversee a digital payment system is challenged in the future, *the* Payment Clearing and Settlement Act *should be updated to explicitly include oversight of "digital Canadian dollars" or, in the alternative, to expressly include "CBDLs."*

The second consideration for BoC's legal authority to issue CBDLs is whether the Bank of Canada Act provides the Bank with the legal authority to issue CBDLs. This requires a different assessment for token-based or account-based digital currencies [43]. Arguably, our proposal requires the BoC to comply with both sets of requirements. The issuance of token-based CBDL, which in our model provides the backbone for offline payments, requires the BoC to have express authority to issue digital currency, as opposed to physical bank notes [43]. The Bank of Canada Act provides the BoC with sole authority to issue "notes" that represent a "first charge on the assets of the Bank."[35] "Notes" is broadly defined as "notes intended for circulation in Canada,"[36] but sections 25(3) and (4) of the Act both reference requirements that notes be "printed."[37] Further, the Royal Canadian Mint Act defines "circulation coin" as a coin "composed of base metal."[38] While the BoC may have an implied authority to issue CBDL regardless of the statutory definitions [43], for greater certainty and to avoid any risk of a legal challenge that could cause reputational damage to the BoC, *it is recommended that relevant sections of the* Bank of Canada Act *are updated to expressly permit the BoC to issue "digital currency."*

In addition to token-based CBDL, our approach contemplates the use of account-based CBDL transacted over a centralized platform by the NB. This will require the NB to have a reserve account with the BoC. The Bank of Canada Act authorizes the BoC to accept

[32] Bank of Canada Act, *P*reamble.
[33] Payment Clearing and Settlement Act, SC 1996, c. 6.
[34] Payment Clearing and Settlement Act, s. 2 "clearing and settlement system" definition.
[35] Bank of Canada Act, s 25(1).
[36] Bank of Canada Act, s 2 "notes" definition.
[37] Bank of Canada Act, s. 25(3),(4).
[38] Royal Canadian Mint Act, RSC 1985, c R-9, s. 2 "circulation coin" definition.

deposits from a bank licensed under the Bank Act,[39] from a Government of Canada corporation or agency, or in a manner that is authorized by an Act of Parliament.[40] The BoC does not, however, have legal authority to grant accounts to individuals. Our approach introduces the NB as an *intermediary* between individual wallet-holders and the BoC so that the BoC does not need to directly interact with, or open accounts for, individuals. To facilitate this approach, the NB must be included within one of the authorized groups of entities that can open a reserve account with the BoC. Depending on the final governing structure of the NB, *the BoC should ensure that the NB fits within one of these categories to ensure that it is able to both accept deposits and issue CBDL to the NB.*

8.3 Regulation/Oversight Of CBDL e-Wallets/Exchanges

Phase 1 requires the creation of a centralized platform where the NB is responsible for verifying end user identities and managing transactions between CBDL e-wallets. This requires an assessment of how the NB should be constituted, but also for the appropriate regulatory body to oversee its operations. The appropriate regulatory body will depend on the scope of the NB's operations. Among other things, the regulatory body will be responsible for overseeing the NB's risk management procedures. In Phase 2, the network will be expanded to permit NB/BoC-licensed private entities to provide new innovative services via service-wallets and to add licensed third-party verification nodes to a permissioned DLT network. In theory, these network participants could be regulated under a different regulatory body than the NB. To promote a *holistic* approach to regulation, however, *it is recommended that a single regulatory body be responsible for overseeing all CDBL network participants.* Accordingly, if the BoC decides to adopt our two-phased approach, *the regulatory approach selected for the initial NB should be scalable to include Phase 2 network participants.*

The BoC should consider the following four alternative approaches to regulating the NB. First option is to regulate the NB and CBDL e-wallet (or service-wallet) providers as banks (*i.e.*, deposit-taking institutions) under the Bank Act. Second alternative is to regulate the NB as a crypto-asset exchange platform under provincial securities laws and *Investment Industry Regulatory Organization of Canada (IIROC)* rules. A third option is to develop a customized regulatory/governance framework under the current payments regulations regime, namely the Canadian Payments Act and Payment Clearing and Settlement Act. A fourth route involves a novel regulatory framework designed under the federal *Department of Finance*'s recently proposed retail payments oversight framework [44]. For the reasons that follow, *we recommend regulating both the NB and future network participants as payments providers (*i.e.*, the third option).* The remainder of this subsection discusses each of these alternatives in greater detail and highlights policy perspectives that the BoC should consider when evaluating each alternative.

[39] Bank Act, SC 1991, c. 46.
[40] Bank of Canada Act, s. 18.

8.3.1 Regulation under the Bank Act

One regulatory approach is to incorporate the NB as a registered bank under the Bank Act. The scope of banking activity that is authorized under the Act is broad and includes "providing any financial service" and "issuing payment."[41] Accordingly, the expected scope of services provided by the NB is expected to fall within the scope of permissible banking activities under the Bank Act if this is the desired incorporation method for the NB. In particular, if the NB is incorporated under the Bank Act, it will be subject to regulation by the *Office of the Superintendent of Financial Institutions (OSFI)* [45]. This approach is recommended if the BoC has plans to expand the scope of CBDL to permit CBDL-denominated lending in the future — although, neither the BoC in its objectives nor this proposal speculate this avenue as a possibility. OSFI specializes in monitoring solvency, liquidity and systemic risk in relation to deposit-taking institutions [46]. If the BoC expects to permit financial institutions to take deposits and make loans in CBDLs in the future, and if there is a good reason to protect CBDL e-wallets with deposit insurance under the Canada Deposit Insurance Corporation Act,[42] then these institutions should be subject to OSFI regulation. Under this framework, the NB could also provide loans in CBDLs. If this is the vision of the BoC, it should begin by incorporating the NB under the Bank Act.

Our model, however, was developed on the assumption set out by the BoC in its contingency planning that all CBDL e-wallet providers would be fully funded and prohibited from lending in CBDL. End user CBDL e-wallet balances will be separated from the assets and liabilities of the NB. Accordingly, the NB and subsequent service-wallet providers can all be thought of as "narrow banks," in the sense that they only provide data or payment/settlement services. As discussed earlier, the term "narrow bank" is a non-legal term for a bank with limited operations. Narrow banks are typically categorized based on the fact that they are 100% fully funded and are prohibited from lending against deposits under the traditional fractional reserve banking system.[43] Canadian banking regulations do not currently provide for a separate regulatory regime for narrow banks. Accordingly, if the NB is to be regulated under the Bank Act, it would either be subject to standard Bank Act requirements, or specific amendments to the Bank Act would be required to develop a new narrow bank regulatory framework. OSFI is currently considering introducing new regulations for small and medium-sized deposit-taking institutions. [48] This revised framework may be more viable for the NB or service-wallet providers in Phase 2 if the BoC would want these entities to be regulated by OSFI.

While the restricted role of the NB does not necessarily rule out OSFI as a potential regulator, it reduces the applicability of OSFI's core competencies in regulating solvency and liquidity risk. A fully funded entity also reduces the need for deposit insurance. OSFI does, however, have experience regulating and monitoring cyber-security risk [49, 50] that would offer valuable oversight for the NB. Even though the NB may initially be a good

[41] Bank Act, s. 409(1),(2).
[42] *Canada Deposit Insurance Corporation Act*, RSC 1985, c. C-3.
[43] See generally [47].

candidate for regulation by OSFI, this may be less so for future service-wallet providers in Phase 2. Requirements that future third-party service providers incorporate under the Bank Act may create a regulatory burden that acts as a barrier to innovation. If the BoC determines that the NB and private service-wallet providers should be regulated by OSFI under the Bank Act, the regulatory burden could be reduced by introducing a new narrow banking regulatory framework under the Bank Act, or by incorporating the service-wallet providers into the above-noted proposed small and medium-sized deposit-taking institution regulatory regime. [48] This would result in CBDL service-wallet providers being regulated by OSFI but subject to different regulatory standards than traditional deposit-taking institutions.

Our recommendation is *that neither the NB nor third party data and payment service providers in Phase 2 be regulated as banks under the* Bank Act. This implicitly assumes that the NB and e-wallet providers will be prohibited from taking CBDL deposits and offering CBDL loans using the deposits as a source of financing (*i.e.* CBDL fractional reserve banking). Provided that e-wallets remain fully funded and third party service providers merely act as custodians, proxies or provide data/payment services for end users (*i.e.*, the end user CBDL wallets remain separated from the assets of the service-wallet provider), we do not foresee a need to subject them to banking regulations. Instead, as discussed further in later sections, we foresee these entities being regulated under existing payments regulations. Our Phase 2 approach, however, is designed to be flexible and present the opportunity for future expansion of services provided be third party e-wallet providers. If the BoC determines based on policy considerations, that Phase 2 e-wallet service providers should be permitted to provide traditional banking services (such as CBDL deposit-taking and fractional reserve lending) then these select service providers should be subject to standard banking regulation in addition to being required to register as a payment entity (as discussed below). This requirement should not apply, however, to the NB or other e-wallet service providers that merely act as a custodian or provide proxy/payment or data services. This represents a flexible approach to regulation, where service-wallet providers are subject to more or less regulations depending on the types of services they provide.

8.3.2 Regulation as a Crypto Asset Platform Under Provincial Securities Laws

A second approach to regulating the NB is to incorporate the NB under the Canada Business Corporations Act,[44] or as a crown corporation under a separate Act, and subject it to provincial securities regulation as a crypto-asset trading platform. Recent publications by the *Canadian Securities Administrators (CSA)* have referenced "digital assets" or "crypto assets" broadly with respect to their proposed regulation of crypto-asset trading platforms [51]. Even if CBDL fits within the broad definition of a "digital asset" or "crypto asset," as it's used by securities regulators, it has to be considered a "security" for securities regulations to apply. For this to be the case, either the underlying asset (CBDL), or the contract with the custodial platform, must be considered a "security" [52]. Given that the value of CBDL is tied to the Canadian dollar and it is fully backed by the

[44] Canada Business Corporations Act, RSC 1985, c. C-44.

BoC, we do not expect CBDL to be considered a "security" for the purposes of securities regulations. The CSA has indicated that "well established crypto assets that function as a form of payment or means of exchange on a decentralized network" are not in and of themselves securities as they are more analogous to "commodities such as currencies and precious metals" [51]. Further, as discussed in more detail below, the contract with the NB, which will act as the trading platform in Phase 1, is also not expected to be considered a "security" under the CSA's current guidelines, given that the NB will facilitate the immediate transfer of CBDL between wallets. [52].

There is an opportunity, however, for the BoC to work with securities regulators to bring the NB and the CBDL network within the scope of the CSA's crypto-asset trading platform regulatory regime. In the absence of sufficient regulation for current private cryptocurrency trading platforms, the CSA and IIROC have developed a useful framework for regulating crypto-asset trading platforms [51]. Their approach involves a joint-regulatory initiative between provincial securities regulators and IIROC whereby provincial regulators oversee, among other things, certain risks associated with the trading platform including cyber security, risk management and platform liquidity; and IIROC monitors network participants as registered IIROC dealer members [51]. The CSA is further ahead of other regulatory bodies in Canada in developing an approach for regulating crypto-asset platforms. It has developed a comprehensive risk management approach that includes monitoring:[45]

1. Platform security measures for safeguarding investor crypto assets;
2. Internal platform processes, policies and procedures to establish an internal system of control and supervision;
3. Disclosure of risks to investors;
4. Mitigating conflicts of interest;
5. Monitoring manipulative and deceptive trading techniques;
6. Platform transparency; and
7. System resiliency, integrity and security controls to manage cybersecurity risks.

As referenced above, CBDL is unlikely to be considered a "security" under the Ontario Securities Act,[46] so provincial regulations with respect to "clearing agencies," "marketplaces" and "dealers" would not be expected to apply to the NB.[47] Some crypto-asset trading platforms, however, still fall within the scope of provincial securities laws if the platform provides users with a contractual right or a claim to the underlying crypto asset

[45] [51], Part 3 "Risks related to Platforms".

[46] Ontario Securities Act, RSO 1990, c. S.5.

[47] See Ontario *Securities Act*, s. 1(1) definitions of "marketplace," "clearing agency" and "dealer" reference the exchange of "securities."

held by the platform, as opposed to actually transferring crypto-assets between counterparties [52]. Under this regulatory approach, the contract between the user and the crypto-asset platform is considered a "security" as an "investment contract" for the purposes of securities regulation [52]. This does not apply, however, for crypto-asset exchanges where no obligation is created and the crypto-asset is immediately exchanged between counterparties [52] (p. 1-3.) Our approach involves peer-to-peer transaction of CBDLs between wallets over a distributed ledger; and therefore, provincial securities regulations with respect to crypto-asset trading platforms are not expected to apply. Hence, if the BoC wishes to bring either the NB or future Phase 2 service-wallet providers under the regulatory purview of provincial securities regulators or IIROC, it would likely require amendments to relevant provincial securities acts to specifically include and specify CBDLs as a "security".[48]

The benefits of adopting the crypto-asset platform approach is that provincial securities regulators have already started developing protocols for assessing and regulating crypto-asset trading platforms. This approach may present issues in Phase 2 of our model, however, with the network expansion. Securities regulation in Canada is governed by provincial regulators, with the CSA acting as a consortium of provincial regulators for harmonization purposes. As the CBDL network expands in Phase 2, it is expected to include service providers from different provinces. There are certain risks associated with relying on a consortium of provincial securities regulators (the CSA) and a self-regulatory organization (IIROC) to oversee a critical national clearing and settlement network. To improve regulatory harmony across the CDBL network, *it is recommended that that the BoC adopts a national regulatory approach under a federal regulator*, as opposed to outsourcing regulation across provincial securities regulators.

There is a risk, however, that third party e-wallet providers in Phase 2 may be subject to securities regulations if the contracts between the service provider and the wallet holder is considered an "investment contract" for the purposes of securities regulation. Under the current regulatory regime, each third party service-wallet contract would be assessed on a one-off basis to determine whether it falls within the scope of crypto-asset trading platform regulations. This would place the burden on third party service providers to design the scope of their services in a manner that avoids securities regulations, or to seek an exemption. To avoid this regulatory burden, *it is recommended that a broad exemption from crypto-asset platform regulations is implemented for CBDL e-wallet providers that are registered with the NB and subject to BoC oversight.*[49]

8.3.3 Regulation Under the Existing Payments Regulatory Framework

The third option is to regulate the CBDL network under the existing federal payments regulatory regime. The current Canadian payments system is managed by the *Canadian Payments Association (CPA)*, or simply, *Payments Canada*. Payments Canada was in-

[48] Or an alternative method that subjects the centralized platform to securities regulation without classifying CBDL as a security.

[49] Similar to how the Ontario *Securities Act* excludes insurance contracts and bank deposits from the definition of "security" (s. 1(1)).

corporated under the Canadian Payments Act[50] to establish a "national system for the clearing and settlement of payments."[51] Payments Canada is a unique organization in the sense that it is a non-profit corporation that is not considered a government agency, but is subject to significant government oversight [53]. It is managed by a board of directors elected by its members, the majority of which must be independent of the CPA and its members.[52] CPA members include the BoC, commercial banks, credit unions, trust companies, and others who apply/meet the membership criteria.[53]

Payments Canada is regulated by both the federal government and the BoC.[54] The Payment Clearing and Settlement Act gives the BoC responsibility for the oversight of payment and other clearing and settlement systems in Canada for the purpose of controlling systemic risk.[55] The federal government also has a direct role in regulating Payments Canada. The Governor in Council has the authority to make regulations that, among other things, provide for the mandate of committees established by Payments Canada, prescribe the form and content of Payments Canada's corporate plans, and to enact general regulations for "carrying out the purpose and provisions" of the Act.[56] In addition to regulating Payments Canada, the Minister of Finance also has the authority to designate any payment system that is of national importance as a "designated payment system" for the purpose of regulating it under the Canadian Payments Act.[57] In doing so, the Minister is able to provide written directive to managers or participants of the designated payment system with respect to its operations.[58]

The benefit of regulating the NB under the current payments regulatory regime is that it would be subject to an existing established federal regulatory framework with experience regulating clearing and settlement institutions. The BoC would have jurisdiction to oversee its operations to mitigate systemic risk and the federal government can use its authority to ensure that operations of the NB, and the larger CBDL network, are conducted in a manner that supports the overarching policy goals underlying the issuance of CBDLs. Regulating all market participants under a single payments regulatory regime that is headed by the BoC also empowers the BoC to identify circumstances where the CBDL network will convert to a centralized system run by the BoC/NB in times of systemic crisis. This is necessary for Phase 2 where transaction processing will be performed by third party validator nodes.

There are two alternative methods of regulating the centralized platform under the current national payments regulatory framework. First, the NB could be developed by Payments Canada. Payments Canada's mandate is broad and includes "the development of new payment methods and technologies."[59] Accordingly, it certainly appears to be

[50] Canadian Payments Act, RSC 1985, c C-21
[51] Canadian Payments Act, s. 5(1)(a).
[52] Canadian Payments Act s. 8.
[53] Canada Payments Act, s. 4(1),(2).
[54] Canadian Payments Act, s. 4(1).
[55] Payment Clearing and Settlement Act, Preamble.
[56] Canadian Payments Act, s. 35(1).
[57] Canadian Payments Act, s. 37.
[58] Canadian Payments Act, s. 30(1).
[59] Canadian Payment Act, s. 5(1)(c).

within the scope of the CPA's mandate to establish and manage the NB. The benefit of this approach is that the NB would be governed by a board of directors with experience managing large-scale payment and settlement systems. Payments Canada also has a well-established governance system under the Canadian Payments Act. This approach may also improve the interconnectedness between the CBDL clearing and settlement system and the existing large-scale payment system. It should be noted, however, that our proposed approach involves the development of a new CBDL network architecture that sits outside of the current payments system. Accordingly, while partial integration with the payments network will be required to permit users to purchase CBDL for their CBDL e-wallets through EFTs, as noted earlier in this proposal, the transactions between CBDL e-wallets can exist outside the current large-scale payments system infrastructure. This approach may also create a conflict of interest for the existing Payments Canada board of directors, no different than what is noted in other parts of this proposal. Specifically, the current members of Payments Canada, which include domestic Canadian banks, may view CBDL as a competitor and be reluctant to incorporate CBDL into the existing Canadian payments network.

The second approach involves regulating the NB as a "designated payment system" under Part II of the Canadian Payments Act and as a clearing and settlement system under the Payment Clearing and Settlement Act. The definition of "payment system" under the Canadian Payments Act is broad and includes "a system or arrangement for the exchange of messages effecting, ordering, enabling or facilitating the making of payments or transfers of value."[60] The Minister of Finance has a significant degree of discretion to designate a payment system as a "designated payment system" if it is of the opinion that it is in the public interest to do so, the payment system is national in its scope, and the system plays a major role in supporting transactions in the Canadian economy.[61] Accordingly, the NB is expected to meet this criteria. The purpose of Part II of the Act is to provide an option for the Minister of Finance to regulate entities other than Payments Canada that provide payment solutions.[62] Together with the BoC's authority to designate any clearing and settlement system to be within its regulatory authority under the Payment and Clearing Settlement Act,[63] the Minister of Finance and the BoC appear to have the authority to bring any payment system within their regulatory purview. This provides a method for the BoC and the Minister of Finance to regulate a new payments entity (such as the NB) that is not operated by Payments Canada.

To our knowledge, the Minister of Finance has not utilized its authority under Part II of the Canadian Payments Act to designate an entity as a "designated payment system" [54] (§. 7:104). It has been considered, however, that this particular legislative scheme may be viable to extend to virtual currency payment systems [54]. This approach may be applicable if a new entity is incorporated, either as a crown corporation or a private entity, to operate the NB. Under this approach, the Minister of Finance could

[60] Canadian Payments Act, s. 36.
[61] Canadian Payments Act, s. 37.
[62] [54], ch. 7, Part IX.
[63] Payment Clearing and Settlement Act, s. 4.

use its discretion to regulate validator nodes and service-wallet providers as "participants" in the CBDL payment system. This would permit the Minister of Finance to introduce varying levels of regulation for the NB and different third-party e-wallet providers. The BoC could also provide oversight of the entire system under the Payment and Clearing Settlement Act.

The downside to this approach, however, is that the regulatory regime is based on discretionary ministerial orders. This creates a risk of unreasonable or excessive action from the Minister of Finance [54] (§§ 7:113-7:114). Accordingly, this approach would likely require further regulations or policy guidance from the Minister of Finance, or, in the case of a crown corporation, under its constituting legislation. These risks could be mitigated by incorporating the entity responsible for managing the centralized platform (*i.e.*, the NB) under a new legislative regime, similar to how Payments Canada is incorporated under the Canadian Payments Act. Similar to that Act, the new legislation could impose a clear mandate and governance structure for the entity responsible for establishing the centralized platform. Depending on the level of oversight desired by the BoC, the new legislation could either give authority to the BoC to appoint directors and chair the NB's board, or it could include a greater number of independent directors (similar to Payments Canada). The Minister of Finance could then designate the entire CBDL system as a "designated payment system" in order to permit it to impose regulations on system participants, such as service-wallet providers in Phase 2. The Canadian Payments Act could also be amended to include the new entity as a member of Payments Canada to promote synergies across the two payments systems. To promote consistent application of regulations applicable to e-wallet providers in Phase 2, new regulations could be introduced, as opposed to relying on ministerial discretion under the Canadian Payments Act.

In our proposed model, *we recommend a modified version of the latter approach*. Specifically, that the NB be incorporated by a new federal statute, similar to how the Canadian Payments Act establishes Payments Canada. The governing statute should set out the NB's mandate and governance structure, including designating the BoC with broad oversight authority. The governing statute should include a process for appointing the NB's board of directors based on the desired level of BoC representation and control over the NB. It should also establish a process for registering and monitoring validator nodes and third party service providers. This will provide the BoC with oversight over all network participants under a single regulatory regime. It also permits the BoC to identify circumstances, either specifically within the governing statute or through a broad mandate that is clarified by BoC guidance papers, of times when the CBDL network will convert to a a centralized system run by the BoC/NB during times of systemic crisis in Phase 2. In normal times, the level of BoC and federal government oversight can also be set out in the governing statute. For a less-stringent regulatory approach, the NB could be subject to broad oversight from the BoC under its authority granted by the Payments Clearing and Settlement Act. For a more stringent regulatory regime, the federal government could appoint the NB as a "designated payment system" under the Canadian Payments Act, which would permit the federal government to establish new regulations for the NB and other network participants in Phase 2. As discussed further in Section 8.5, e-wallet proxy providers in

Phase 2 that provide certain payment services may also be required to register with FINTRAC as a money services business to ensure they comply with AML/CFT requirements. Private entities that don't qualify as a money services business will only be required to register with the NB/BoC (using the process established in its governing legislation).

8.3.4 Regulation Under a New Retail Payments Regulatory Framework

The fourth alternative for the BoC to consider is regulating the NB and Phase 2 network participants under a novel retail payments regulatory regime. In July 2017, the Department of Finance released a consultation paper on the proposed regulation of retail payments in Canada, outlining the components of a novel federal oversight framework for retail payments [44]. The federal government's proposed retail payments regulatory regime was a response to the rapid growth of electronic retail payment innovation and the perceived need to introduce federal oversight to "ensure the retail payments ecosystem evolves in such a way that payment services remain reliable and safe for end users and the ecosystem is conducive to the development of faster, cheaper and more convenient methods of payment" [44]. The current payments regulatory regime is based on an "institutional approach where rules target specific types of payment service providers such as banks and card network operators."[64] Based on this approach, retail payment providers that provide similar services may be regulated differently depending on how they are classified [44]. The new proposed retail payments regulations introduces a functional approach to payments regulation where "risks associated with a particular payment function are treated similarly regardless of the type of organization provide the service" [44]. Under the proposal, retail payment providers would fall within the scope of the regulations if they perform one of the following five core functions in the context of EFTs:

1. Provision and maintenance of a payment account;
2. Payment initiation;
3. Authorization and transmission;
4. Holding of funds; or
5. Clearing and settlement.

The proposed retail payments regulations include the development of consistent regulatory standards for end-user fund safeguarding; operational standards; disclosure; dispute resolution; liability; registration; and, personal information and privacy.[65] The federal government took further steps towards introducing the Retail Payments Proposed Regulations by announcing its plans for the new retail payment regulatory framework in the 2019 budget [55]. In the budget proposal, the government recommended that the BoC be responsible

[64] [44], Part 5.1.
[65] [44], Part 5.2.

for oversight of the payment service providers to ensure participants comply with the new regulatory regime [55].

Having said this, *the proposed retail payments regulatory framework provides an opportunity for the development of a new customized regulatory framework for the proposed CBDL network*. This is particularly beneficial for Phase 2 as it facilitates the introduction of customized regulations for service-wallet providers without subjecting them to existing banking or securities regulations. Under the functional approach to regulation outlined in the federal government's proposal, different CBDL network participants could be subject to customized regulations depending on the specific functions they provide. For example, the NB could be subject to increased regulations as a clearing and settlement institution compared to the service-wallet proxy providers that only provide limited payment services. The new regulatory regime could also establish the circumstances where the CBDL network would convert to a centralized system run by the BoC/NB during a systemic crisis.

The primary risk to this alternative is that the CBDL network would be regulated under a novel regulatory framework, which presents a different set of risks compared to incorporating a new entity into an existing regulatory framework. Accordingly, the regulator, whether it be the BoC or a new regulatory body under the supervision of the BoC, may not have the same institutional knowledge as OSFI, the CSA or Payments Canada.

8.3.5 A Hybrid Solution

It should be noted that a hybrid solution is possible across the four regulatory approaches discussed above. For example, the NB could be incorporated under the Bank Act, and therefore subject to OSFI regulations, and it could also be regulated under the Canadian Payments Act or the new Retail Payments Proposed Regulations. Similarly, the NB could be regulated under the Retail Payments Proposed Regulations and also be designated as a "designated payments system" under the Canadian Payments Act. This type of hybrid "sheltering" would increase the regulatory burden for participants, but could have the advantage of leveraging institutional knowledge across different regulators. We do not recommend this approach due to the added complexities and feasibility constraints, but wanted to highlight it as an option in case the BoC preferred an additional arm's length regulatory body to have oversight over the CBDL network in addition to the BoC.

8.4 Anti-Money Laundering and Terrorist Financing

8.4.1 Introduction

Anti-Money Laundering and Combatting the Financing of Terrorism (AML/CFT) regulations in Canada are set out in the Proceeds of Crime (Money Laundering) and Terrorist Financing Act[66] and its corresponding regulations. This piece of legislation applies to money services businesses, which include entities "dealing in virtual currencies."[67]

[66] *PCMLTFA*
[67] *PCMLTFA*, s. 5(1)(h).

The definition of "dealing in virtual currencies" includes both virtual currency exchange services (*i.e.*, exchanging funds for virtual currencies) and virtual currency transfer services (*i.e.*, transferring or receiving virtual currency) [56]. The Act does not currently define "virtual currency," but an amendment to the PROCEEDS OF CRIME (MONEY LAUNDERING) AND TERRORIST FINANCING REGULATIONS that is set to come into force in June 2021 provides a broad definition of "virtual currency" as a "digital representation of value that can be used for payment or investment services."[68] Based on this broad definition, both the NB in Phase 1 and third party e-wallet proxy providers in Phase 2 of our two-phased approach are likely to be considered money services businesses subject to AML/CFT rules.

Regulated entities are required to abide by the AML/CFT provisions of the legislation and are subject to regulatory oversight by the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC). Under the relevant AML/CFT regulations, regulated entities are generally required to:

1. Register as a money services business with FINTRAC;[69]
2. Establish an internal compliance program that meets FINTRAC standards;[70]
3. Ascertain the identity of clients and account holders in accordance with the regulations;[71]
4. Report suspicious transactions in accordance with the regulations;[72]
5. Keep records of certain transactions in accordance with the regulations;[73]

The recently introduced amendments to Canadian AML/CFT regulations[74] provide further regulations for virtual currency transactions.[75] Under the amended regulations, money services businesses will be required to:

1. Report and keep a transaction record of receipts of $10,000 or more in virtual currency;[76]

[68] REGULATIONS AMENDING CERTAIN REGULATIONS MADE UNDER THE PROCEEDS OF CRIME (MONEY LAUNDERING) AND TERRORIST FINANCING ACT, 2019, SOR/2019/240 [*PCMLTFA Amending Regulations*].

[69] *PCMLTFA*, s. 11.1; See also [57].

[70] *PCMLTFA* s. 9.6; See also [58].

[71] *PCMLTFA*, ss. 6.1, 9.2; See also [59].

[72] *PCMLTFA*, ss. 7, 9, 9.5, 12(1), 28(1); See also [60].

[73] *PCMLTFA*, s. 6, *Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations*, SOR/2002-184, s. 30; See also [61].

[74] Specifically amending the PROCEEDS OF CRIME (MONEY LAUNDERING) AND TERRORIST FINANCING REGULATIONS ACT, SOR/2002-184 [*PCMLTFA General Regulations*]; and the PROCEEDS OF CRIME (MONEY LAUNDERING) AND TERRORIST FINANCING SUSPICIOUS TRANSACTION REPORTING REGULATIONS ACT, SOR/2001-317 [*PCMLTFA Suspicious Transaction Regulations*]

[75] *PCMLTFA Amending Regulations*.

[76] *PCMLTFA Amending Regulations*, s. 28 (Amending *PCMLTFA General Regulations s. 30(1)).*

2. Verify the identity of third parties that transfer $10,000 or more in virtual currency to the businesses account holder;[77]

3. Keep a detailed record of receipts or transfers of $1,000 or more in virtual currency;[78]

4. Verify the identity of a person who transfers or receives $1,000 or more in virtual currency;[79] and

5. Verify the identity of an "entity" (defined to exclude individuals) with which the money services business enters into a service agreement.[80]

The amended regulations will impose stringent regulations on all money services businesses, which are expected to apply equally to the NB and all e-wallet service providers under our two-phased approach. To reduce the cost of compliance, we have recommended an e-KYC approach where the NB can rely on legacy KYC infrastructure to support account (e-wallet) onboarding. In Phase 2, service-wallets will be linked to CBDL-wallets with the NB in order to mitigate the compliance costs associated with providing service-wallets. A number of amendments to the current AML/CFT regulations may be required to support our proposed approach.

AML/CFT legal rules impose different standards of KYC requirements for financial entities compared to money services businesses. Financial entities are required to verify the identity for every individual or entity that opens an account with the financial entity [62]; whereas money services businesses are only required to verify identities for certain transactions (*i.e.,* over $1,000) and for an "entity," which does not include individuals, that enters into an ongoing service agreement with the money services business [59]. The definition of financial entity is limited and includes organizations such as banks and other deposit-taking institutions.[81] As noted above, the NB may not fall within the definition of "financial entity." Under our proposed approach, however, we recommend that all CBDL-wallets go through the initial e-KYC process. In order to facilitate this recommendation, *the definition of "financial entity" should be amended in AML/CFT rules and regulations to ensure it includes the NB*. Further, in order to facilitate our proposed e-KYC process, *exceptions should be included in AML/CFT regulations to permit the NB to rely on identity verification completed by a third party approved authenticator*, provided the authenticator complies with the PCMLTFA and maintains KYC information that can be retrieved by the NB/FINTRAC if certain AML/CFT obligations are triggered by the NB's homomorphic encryption compliance technical process.[82]

The BoC will also need to make a policy decision about how third party e-wallet providers will be regulated under AML/CFT rules and regulations. Under current AML/CFT

[77] *PCMLTFA Amending Regulations*, s. 38 (Amending *PCMLTFA General Regulations,* s. 84).
[78] *PCMLTFA Amending Regulations*, s. 28 (Amending *PCMLTFA General Regulations* s. 36*).*
[79] *PCMLTFA Amending Regulations*, s. 39, (Amending *PCMLTFA General Regulations,* s. 95(1)*).*
[80] *PCMLTFA Amending Regulations*, s. 28 (Amending *PCMLTFA General Regulations,* s. 37).
[81] *PCMLTFA General Regulations*, s. 1(1), "financial entity" definition.
[82] Similar exceptions are included for identification requirements for certain suspicious transaction verification. See e.g. *PCMLTFA General Regulations* s. 53.

regulations, service-wallet providers are expected to be regulated as a "money services business". They will be required to register as a money services business with FINTRAC and establish an internal compliance program. It is recommended *that the registration process remains unchanged so as to ensure all e-wallet providers are subject to FINTRAC oversight.* The compliance program requirement may, however, create a regulatory burden that discourages third parties from becoming registered service-wallet providers. FINTRAC notes that the level and sophistication of compliance programs should reflect the "size, complexity, structure and risk of exposure" to money laundering and terrorist activity financing [58]. It is therefore recommended that *FINTRAC develops specific guidance for e-wallet providers outlining the expectations for CBDL service-wallet provider compliance programs.* This should include regulatory relief for e-wallet providers that provide low-risk services, such as low-value domestic transfers (similar to cash).

A decision also needs to be made as to whether third party e-wallet providers should be required to ascertain client identities, keep transaction records, and report suspicious transactions to FINTRAC. Under the current AML/CFT regulations, service-wallets that provide for transactions by individuals under $1,000 per day are expected to avoid triggering certain record keeping and suspicious transaction reporting requirements. E-wallet providers that permit transactions over $1,000 per day, however, would be required to comply with all of the identification, reporting and record-keeping requirements of money services businesses under the current AML/CFT framework.

There are *three general approaches* we recommend for the BoC to consider to ensure service-wallet providers are AML/CFT compliant. First, legal rules could be introduced that limit the daily transaction amount for all e-wallet providers to avoid triggering certain AML/CFT record-keeping requirements. This approach is recommended if the BoC wants to contain CBDL transactions to low-value transactions, similar to cash. Large-scale transactions could still be facilitated via wallets held with the NB, which would be subject to all AML/CFT record keeping and suspicious transaction reporting requirements. The second approach is to maintain the current AML/CFT regulations, which would have the effect of imposing different KYC requirements depending on the CBDL transaction size. E-Wallets that prohibit transactions over $1,000 per day are expected to avoid triggering certain AML/CFT record-keeping obligations. For these limited transaction wallets, we recommend introducing new amendments that reduce the regulatory burden for these service providers by permitting them to rely on e-KYC procedures completed by the NB. E-wallets that support transactions over $1,000 per day, however, would be required to maintain records of transactions over $1,000 and report suspicious transactions, including transactions over $10,000, to FINTRAC. We recommend adopting this approach to start. Specifically, higher risk e-wallets that support CBDL transactions over $1,000 per day should be subject to current AML/CFT obligations. A modified AML/CFT regulatory regime should be introduced, however, to better support low risk e-wallets with limited transaction sizes that are designed to replicate traditional cash-like transactions. These entities would still be required to register as a money services business with FINTRAC, but would be subject to a reduced (or relaxed) regulatory standard.

Alternatively, in the long-term, a third regulatory approach could be developed that

requires the NB (as opposed to third-party e-wallet service providers) to monitor suspicious transaction over the entire CBDL network and report suspicious transactions to FINTRAC. AML/CFT regulations currently provide exceptions to record keeping requirements if information is readily available in other records that the money services business has kept [63]. This exception could be widened to permit e-wallet providers to avoid record keeping requirements altogether if the NB keeps a record of all CBDL transactions that is available to FINTRAC upon request. This approach can be thought of as outsourcing AML/CFT record-keeping and suspicious transaction reporting requirements to the NB. This approach is beneficial if the BoC wants to ease the regulatory burden on e-wallet service providers to support large-scale transactions without jeopardizing AML/CFT compliance. This would require the NB to take an expanded role in Phase 2, as also contemplated by our technical proposal. In particular, the NB would be required to manage a blockchain containing all historic transaction records, as opposed to merely acting as a settlement service to support the decentralized permission-based network in Phase 2 of our model.

In the short term, however, we do not recommend that the BoC adopt this approach. Instead, as discussed above, we recommend that the NB only be required to comply with AML/CFT obligations for transactions that the NB is responsible for processing. In Phase 2, as transaction processing becomes decentralized across third party validator nodes and e-wallets, we recommend that these third parties also be responsible for their own AML/CFT obligations (*i.e.* record keeping and suspicious reporting obligations). Accordingly, these third parties should also be the primary contact for FINTRAC and other government bodies that are investigating potential AML/CFT risks, as it happens today. This will insulate the NB from excessive information requests that will hinder operations as the network continues to expand in Phase 2.

8.4.2 Application to Offline/Token-based CBDLs

The previously discussed AML/CFT rules and regulations apply mainly to online transactions between CBDL e-wallets. The upcoming June 2021 amendments to the Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations Act include a separate regulatory framework for "prepaid payment products" that "enable a person or entity to engage in a transaction by giving them electronic access to funds or virtual currency paid to a prepaid payment product account."[83] This regulatory framework is more applicable to digital token-based CBDL payment methods, such as our proposed offline CBDL-debit-cards.

The upcoming June 2021 amended regulations provide similar identity verification, record-keeping and suspicious transaction reporting requirements as online electronic payments for prepaid payment products, but only if the prepaid payment product is issued by a financial entity.[84] Under our model, service-wallet providers may not be considered a "financial entity" based on the current wording of the Proceeds of Crime (Money

[83] *PCMLTFA Amending Regulations* , s. 22(19) (adding the definition of "prepaid payment product" to *PCMLTFA General Regulations,* s. 1(2)).

[84] *PCMLTFA Amending Regulations*.

Laundering) and Terrorist Financing Regulations, which restricts the definition to only include certain entities, such as banks, credit unions or trust companies. Accordingly, there is a risk that service-wallet providers could offer token-based CBDL prepaid cards that evade AML/CFT requirements. Our approach attempts to partially mitigate this risk by requiring that all offline CBDL-debit-cards be associated with an online CBDL-account that has completed our proposed e-KYC process. To support this recommendation and ensure that it applies to non-financial entities that may act as e-wallet or CBDL-debit-wallet providers, prepaid payment product regulations under the Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations should be amended to include CBDL token-based wallets regardless of the entity that issues them. This is expected to result in all issuers of CBDL-debit-cards being responsible for conducting certain AML/CFT compliance obligations. To further reduce the risk of non-registered prepaid CBDL cards acting as a tool for money laundering, there should be new regulations that specifically prohibit an entity from issuing a CBDL-digital-token card that is not in compliance with AML/CFT obligations.

8.5 Further Legal Considerations

8.5.1 Do CBDL wallets require deposit insurance?

Phase 1 of of our approach requires the NB to manage end user CBDL wallets. In this sense, the NB's role is akin to a custodial agent. From a legal perspective, the individual wallet-holder is at all times the legal owner of CBDL and the CBDL held in wallets does not appear as an asset on the NB's balance sheet. The NB merely acts as a clearing and settlement agent to support the transaction of CBDLs between wallets. Accordingly, we do not foresee the need for the NB to have deposit insurance as there is no default risk. Later, Phase 2 of our approach introduces new validators and service-wallet providers into the network. As a base case, we envision those new parties as providers to merely provide custodial, proxy, payment or data services. Similar to the NB in Phase 1, we do not envision that they will ever become the legal owners of the CBDL (*i.e.* the end users' CBDL will always be separate from the assets of the service-wallet providers). Under these circumstances, there is no need for these third parties to have deposit insurance.

Our approach is designed to be flexible, however, and creates an option in the future for allowing financial institutions (or novel fintech service providers) to provide more traditional banking services using CBDL. This represents a policy decision for the BoC to consider. If this approach is adopted by the BoC, a number of legal issues arise as to whether CBDL deposits with FIs are, or should be, considered deposits that are covered by deposit insurance. The Bank Act does not define deposits, but it has generally been interpreted by Courts as "an entry... to the credit of a customer" and as "something laid up in a place or committed to the charge of a person for safekeeping" [53] (p. 239). In the context of banking activities, it is commonly characterized by its legal properties as a "loan by the customer to the bank" [53] (p. 239). The legal impact of the deposit is that the deposited money becomes the legal property of the bank, and a liability is created by the bank to the benefit of the depositor [54] (§§ 9:67 - 9:77.) Regardless of ownership rights, however,

CBDL-wallets still share certain properties with bank deposits in the sense that the bank (or service-wallet provider) is responsible for its safekeeping.

In comparison, the Canada Deposit Insurance Corporation Act defines "deposit" as the "unpaid balance of the aggregate of moneys received or held by a federal institution" ... for which the institution has "given or is obligated to give credit to that person's account..." and is "obligated to repay the moneys on a fixed day" or "on demand by that person."[85] If the BoC wishes to expand the scope of CBDL use cases in Phase 2 to permit FIs to utilize CBDL to provide traditional banking services, it may be necessary for select CBDL e-wallets to be insured by the Canada Deposit Insurance Corporation. If this is the case, certain amendments may be required to ensure that CBDL deposits fit within the definition of "deposit" in the Canada Deposit Insurance Act. First, the definition of federal institution may need to be expanded to include all third parties that are providing banking services in CBDL. And second, the definition of "deposit" may need to be amended to include the return of CBDL, as opposed to the repayment of moneys.

8.5.2 Financial Stability Considerations

As extensively discussed throughout our proposal, one of the risks of introducing a CBDL is that the transfer of deposits from bank accounts to CBDL e-wallets may disrupt the stability of the financial system through bank disintermediation and the facilitation of digital bank runs [64] (p. 8). If banks lose deposits to CBDL e-wallets over time, it may reduce their lending capacity or force them to turn to riskier wholesale financing alternatives [64]. While increased competition may lead to improvements in bank deposit products, the BoC has also recognized the risk that it could lead Canadian banks to make riskier investments that partially destabilize the Canadian financial system [65] (p. 40).

Our proposal may increase the risk of bank disintermediation as both the centralized NB-managed platform and service-wallet providers in Phase 2 could act as competitors to traditional bank deposits. We have debated in various places elsewhere that our design already "contains" this risk significantly — notwithstanding that it provides new revenue opportunities to the commercial banking sector. Here we further argue that these risks can be further mitigated through effective rules and regulations. First, if CBDL e-wallets are prohibited from paying interest, or if they are not covered by deposit insurance, it will reduce their appeal as an alternative to bank deposits. Alternatively (or complementary), regulation could be drafted to limit the value of CBDLs held in a single wallet, and/or limit the daily transaction value of CBDLs into or between wallets. These restrictions will add to our previously-discussed mitigating efforts to reduce any risk of digital banks runs or that CBDL e-wallets will become a widespread alternative to bank deposits.

8.5.3 Consumer Protection Initiatives

The Bank Act contains a number of consumer protection regulations that protect depositors [66] (p. 122). Oversight of consumer protection regulations is conducted by the

[85] Canada Deposit Insurance Corporation Act, Schedule 1, s. 2(1).

Financial Consumer Agency of Canada (FCAC). FCAC monitors financial institutions, which are defined under the Financial Consumer Agency of Canada Act[86] to include banks, insurance companies and other federally regulated financial institutions.[87] If the NB and third-party service-wallet providers are not regulated as banks, *it is recommended that the* Financial Consumer Agency of Canada Act *be amended to include the NB and other service-wallet providers under FCAC's regulatory scope.*

8.5.4 Privacy Considerations

One of the attributes of CBDLs, or any CBDC platform for that matter, is that it allows for increased traceability, and therefore increased data, across the payments industry. This can be used to support economic decisions, reduce money laundering and tax evasion, or for the development of new and innovative products/services. However, it also increases privacy risks compared to fiat currency against unwanted authoritative practices [23, 68]. The BoC has recognized an inherent public benefit for privacy in payments [69]. This trade-off represents an important policy decision that requires the BoC to determine the *level of privacy* across the CBDL-network [23], and specifically with respect to:

- Privacy from government;
- Privacy from payment intermediaries;
- Privacy from transaction counterparties; and
- Privacy from the public.

In other parts of this paper, we argued extensively why it is important for the BoC to take a *global lead* by protecting privacy for Canadians in this IoT/5G-and-beyond/AI era. In the remaining section, we elaborate on existing legal infrastructure in Canada for same.

Privacy rules in Canada are primarily contained in the Personal Information Protection and Electronic Documents Act (PIPEDA).[88] PIPEDA has a broad scope and applies to every organization that collects, uses or discloses information.[89] Accordingly, both the NB and all service-wallet providers in Phase 2 will be subject to PIPEDA regulations. PIPEDA's guiding principles are based on *responsible* collection, storage and disclosure of personal information.[90] PIPEDA does not necessarily prohibit the collection and disclosure of personal data across the payments network, but instead requires appropriate consumer disclosure before doing so.

If the BoC wishes to offer a CBDL-transaction method that is completely anonymous, or at least quasi-anonymous, which is similar to what cash offers today and aligns with

[86] Financial Consumer Agency of Canada Act, SC 2001, c. 9;
[87] *Financial Consumer Agency of Canada Act*, s. 2, definition of "financial institution"; See also [67].
[88] Personal Information Protection and Electronic Documents Act, SC 2000, c. 5 [*PIPEDA*].
[89] *PIPEDA*, s. 4(1).
[90] *PIPEDA*, Schedule 1.

what has been contemplated in our CBDL design, further regulations may be required. For example, the NB's constituting legislation could include prohibitions against disclosing data to third parties. Exceptions could be included for government warrants or FINTRAC disclosure requirements. Conversely, proxy service-wallet providers could be permitted to collect and share consumer data provided that they receive appropriate consent from the consumer based on PIPEDA standards, as described earlier in this proposal.

Due to the increased privacy risks associated with a more competitive and decentralized payments network, additional requirements to improve regulatory oversight over payment providers could also be considered. The Minister of Finance has noted that retail payment service providers may not be familiar with their obligations under PIPEDA[91] In response, the Minister of Finance proposed an increased role for payments regulators in monitoring privacy obligations in its proposed new retail payments regulatory framework [44]. Hence, if the BoC chooses to proceed under an alternative regulatory framework, it is recommended that *similar improvements in privacy oversight be included under the scope of the ultimate regulatory oversight body.*

8.5.5 Tax Considerations

The widespread adoption of CBDL as an alternative to cash has the potential to reduce the government revenue lost to tax evasion, which has been estimated to cost the Canadian government billions of dollars annually [70]. This would require, however, that the Canada Revenue Agency (CRA) and other government authorities have visibility into small-scale CBDL transaction data. This presents issues with respect to privacy. It also creates a risk that government agencies, such as the CRA, will view the NB as an extension of the government. This may result in the NB being subject to significant overhead and administrative costs in order to support ongoing and continuous requests from government bodies. The CRA currently has the authority to request bank account information and transaction statements during an audit–a power that it is expected to use with a level of restraint [71]. It should be determined whether this authority should extend to CBDL transaction records. In the alternative, CBDL transactions could be prohibited from CRA review, which would make them more comparable to cash transactions.[92] All in all, this represents a policy decision as to whether reduced tax evasion is one of the policy goals behind CBDLs. Our recommendation is that, if the CRA or other law-enforcement agencies are to be allowed to request CBDL transaction data from the NB, *it should only be granted subject to a court order*. This process should also be a last resort after first attempting to retrieve the information from the impugned party voluntarily. This will prevent the CRA or other government agencies from constantly requesting data from the NB, which would have the effect of increasing the cost and reducing the administrative efficiency of the NB.

[91] [44], Part 5.2.

[92] This privacy feature does not, however, extend to FINTRAC. Privacy from the CRA could be enforced by law without shielding the transaction from FINTRAC, which would still have access to CBDL transaction data in order to complete its AML/CFT monitoring functions.

8.5.6 Competition in Payments Industry and Service-Wallet Licensing

The introduction of a CBDL has the potential to increase competition in the payments sector. Phase 2 of our model permits private entities to offer proxy service-wallets to consumers. Under our approach, it is recommended that all third-party service-wallet providers be licensed and regulated by the NB/BoC. It should be determined whether or not competition-related factors, specifically for foreign entrants/entities, should be considered in the licensing process.

Under the current AML/CFT framework, third-party service-wallet providers will be required to register with FINTRAC as a money services business. The current framework permits both domestic and foreign entities to register as a money services business [57]. The application process is primarily based on the entity's expected AML/CFT risk [72]. To our knowledge, competition-related factors are not considered when determining whether to approve a domestic or foreign money services business [72]. If the purpose of the service-wallet registration process is only to mitigate AML/CFT risks, then FINTRAC could act as the sole licensing body for service-wallet providers. If the BoC wishes to consider additional factors, such as competition or financial stability in the service-wallet registration process, then a novel licensing body will likely be required under the ultimate regulatory framework.

9 Other Discussion Points

9.1 Risks

In contrast to the current system where the BoC maintains reserve accounts for a small number of entities, the NB will be outward facing and process transactions for millions of people. With that comes significant cyber-security and fraud risks. There is also the risk that the AML/CFT systems get outsmarted by the "programmability" of this "new money" (*i.e.*, CBDCs) and that CBDLs are used by bad actors [68]. Of course, a counterpoint to this argument is that bad actors who use this system risk being detected and face a total loss. To that end, we expect in the next few years the domestic, but also international, jurisdictions to techno-legally evolve when it comes to regulation/law for CBDCs. After all, as Law Technology Today writes on January 31, 2017 regarding the legal profession (but one could argue it fairly also applies to other disciplines):

> *The evolution of distributed ledger platforms such as blockchain will offer lawyers one of two choices: (1) disregard in an attempt to maintain the status quo, or (2) understand and adapt into the practices. I suggest (2) is the prudent course of action for those lawyers not planning to retire by 2020.*

Another concern raised with respect to the issuance of CBDCs generally is that it could lead to the depletion of consumer account balances at commercial banks because users move funds to their CBDC account [73]. CBDLs are aimed at individuals and small businesses. The deposits that are most sensitive to the introduction of CBDL are CAD-denominated retail deposits (*i.e.,* chequable deposits). However, according the BoC's internal analysis [74],

these deposits fund approximately 5% of total bank assets; savings accounts account for a further 5% of total bank assets. The authors' scenario analysis indicates that even in the most extreme scenario when retail clients move all their deposits away from commercial banks to CBDLs (a quite unlikely scenario for the specific CBDL plan here as already argued in multiple places of this proposal) banks return on equity and interest margins would experience only a minor decline [74]. Therefore, one may conclude that deposit-taking financial institutions are well positioned to absorb potential temporary negative effects on profitability and liquidity associated with the introduction of CBDL. Further, if consumer use CBDLs instead of cash, then banks may need to hold less cash, which will improve their profitability. If one factors the lucrative potential for innovation (both domestically and internationally) for Canadian FIs/businesses presented by Phase 2, but also how the present proposal shields the Canadian banking sector from foreign monetary/data digital intrusion, they all further diminish any risks to the domestic banking system, and in fact, they provide exciting new opportunities.

9.2 Alternative Solutions

Our *overarching CBDL design philosophy* anchors at the following core principles:

- CBDL functionality should be designed to be more than a digital alternative to cash, but rather "programmable money," to allow Canada to innovate in the global digital economy but also to complement/leverage its past social investments;
- CBDLs should protect Canada's data/privacy sovereignty in the IoT/AI/5G era; and,
- CBDLs should incentivize the private sector to innovate and contribute to the network operation's cost recovery.

We recognize that any CBDC proposal has implications beyond technology. As extensively discussed earlier, it is our sincere belief that novelty dynamics of CBDLs outweigh any short-term risks. At the same time, while building the proposal behind CBDLs, we also contemplated and argued amongst ourselves several alternatives, as set out below.

1. *"Add a CBDL to the Current World of Banking."* Here, the BoC works with FIs to build a platform for CBDL transfers. The BoC merely issues CBDL tokens on the platform, whereas FIs handle their distribution/transactions. The advantage of this option is that it may ensure a close relationship to the existing system of reliable partners who already keep their clients' money safe. It also reduces the minor crowding-out FI concerns while all incremental system costs are borne by them.

   However, there are fundamental downsides. Notably, the current electronic payments system is lucrative for FIs. A CBDL platform that enables cheap and fast digital payments would compete with the existing payments system, cannibalizing established profits. It is difficult to imagine that FIs today would be inclined to promote this

cheaper alternative effectively. This approach would also likely require the BoC to establish a new supervisory body to ensure universal access, a time-consuming process that may jeopardize the CBDL's timely introduction. It also requires competing FIs with different business philosophies to work collectively for a solution that adheres to new standards and/or service models. Given the disincentives to build a platform that may diminish corporate profits, one cannot be confident that a "development by committee" approach will be successful, even if the BoC takes the lead.

2. *"Add CBDLs to the current World-of-Banking via an "all-equal" permissioned DLT."* A variation of the first approach is one in which the BoC is one of several settlement nodes in a decentralized network. In principle, this approach would share several features with Phase 2 of our design. However, in contrast to our setting, where the BoC simply sets a default standard/supervision of backbone infrastructure, here it needs to coordinate with the FIs who continue to face the disincentives that we highlight in Section 7.2. This system also needs a strong technological oversight framework to ensure resiliency under stress and universal compatibility. Moreover, at the outset, the system would be restricted to a few major FIs that bear the development costs and may want to hinder the entrance of competitors into this jointly-managed network. Finally, distributed data storage over an "all-equal" participation model creates questions surrounding data security/privacy. All in all, this approach introduces a lot of friction/uncertainty to be successful or even come to some timely closure.

   In contrast to Options 1 and 2, our design explicitly allows users to circumvent FIs in settling transactions, and it inherently promotes an ecosystem of healthy competition/innovation that reflects modern technology trends.

3. *"Issue CBDL tokens on a public blockchain."* As an example, the BoC could issue tokens on the Ethereum network. Many of our proposal's components can transfer to this setup, such as restricting transactions to be only among whitelisted wallets, or our Phase 2 architecture.

   The main advantage of this approach is that the BoC may be able to avoid some costs. However, there are several critical downsides that prohibit using a public blockchain for a CBDL, *i.e.,* a system-critical government service. First, in public blockchains transaction fees are paid in the native crypto-currency; it remains unclear how this may be compatible with transfers of a sovereign currency. Second, the BoC would delegate trust to an undefined collection of (mostly foreign) miners with no oversight or resiliency/security/technology guarantees. Third, quasi-anonymous transactions are publicly visible and privacy-enhancing protocols, such as zero-knowledge proofs, in permissionless DLTs remain prohibitively costly. Fourth, foreign third-party service providers may offer banking-like services based on CDBL smart contract deposits with no oversight; this may threaten Canada's financial stability. Fifth, the governance of permissionless networks remains unclear; it would not be prudent to subject the processing of Canada's digital money to uncontrollable "exotic" entities. Finally, "all-purpose" public blockchains continue to face many technological, economic, scal-

ability, and regulatory limits and/or uncertainties. Although these technologies have come a long way, they are still in an experimentation phase.

On the other hand, we *do* believe that public blockchains may play an important role in the global digital economy. The Canadian Government may even want to consider issuing globally an *asset-based loonie-stablecoin* to enable commerce in new segments of the economy. Most importantly, as noted earlier, Phase 2 of our proposal fosters interoperability/standardization with both public/private blockchains, as well as with other potential CBDC networks built by other Central Banks.

The second core component of our design is the e-KYC. Adding to the discussion in Section 4.2.2, since 99% of adult Canadians have a bank account,[93] our approach promotes inclusion intrinsically by giving CBDL access to almost all when compared to a non-KYC alternative. The involvement of government service agencies ensures that new immigrants, minors, and the few unbanked will also have access to CBDLs.

10 Concluding Remarks

A general purpose retail-CBDC is a system-critical technology that millions of people will rely on and use. The issuance of such money is not a small task: It must work, safeguard past social investments, elicit geopolitical trends, but also provide value to Canadians. This paper proposes a design that delivers on the core requirements as recently set by the Bank of Canada: privacy protection, universal access, security, performance and value (including business opportunities) to the Canadian public. It does this by proposing a two-phased process, where a centralized solution first establishes general purpose digital money as a viable alternative to cash in that it is fast, cheap, and convenient for daily use. In this context, cryptographic principles ensure the protection of people's privacy and business secrets, while it remains AML/CFT compliant. The latter is ensured by an e-KYC process that uses existing infrastructure and promotes inclusion. Later, Phase 2 adds a permissioned yet decentralized messaging layer to enable businesses to develop innovative services and consumers to monetize their valuable data in the IoT/5G-and-beyond/AI era. Both phases are complemented by a unique technological design that permits offline transactions. The paper concludes with an extensive set of legal recommendations and legislative considerations that accommodate the different phases of the proposed technical implementation. The Bank of Canada is no novice in the area of CBDCs — in the past decade, it has emerged as a global thought leader by experimenting with DLTs and other novel channels for transmission of digital value(s). It therefore comes as no surprise that the findings here invite the Bank to continue this leadership paradigm by spearheading issuance of this new form of "e-cash" so to embrace those emerging brave new digital economies.

[93] See Canadian Bankers Association.

11 Acknowledgments

The authors gratefully acknowledge the outstanding research assistance of Ms. Anxhela Adhamidhis and Mr. Cameron Teschuk, both law students at Osgoode Hall Law School. They also thank the Bank of Canada's staff for many fruitful discussions.

References

[1] D. Tapscott and J. Euchner, "Blockchain and the Internet of Value: An Interview with Don Tapscott Don Tapscott talks with Jim Euchner about blockchain, the Internet of value, and the next Internet revolution.," *Research Technology Management*, vol. 62, no. 1, pp. 12–19, 2019.

[2] A. M. Antonopoulos, *The Internet of Money - Volume Two*. Merkle Boom LLC, 2017.

[3] S. Allen, S. Capkun, I. Eyal, G. Fanti, B. Ford, J. Grimmelmann, A. Juels, K. Kostiainen, S. Meiklejohn, A. Miller, E. Prasad, K. Wüst, and F. Zhang, "Design Choices for Central Bank Digital Currency: Policy and Technical Considerations," Tech. Rep. 13535, Institut f'ur die Zukunft der Arbeit, jul 2020.

[4] T. Adrian and T. Mancini-Griffoli, "The Rise of Digital Money," tech. rep., International Monetary Fund, jul 2019.

[5] J. G. Allen, M. Rauchs, A. Blandin, and K. Bear, "Legal and Regulatory Considerations for Digital Assets," tech. rep., CCAF, oct 2020.

[6] R. Auer, G. Cornelli, and J. Frost, "Rise of the central bank digital currencies: drivers, approaches and technologies," tech. rep., Bank for International Settlements, aug 2020.

[7] U. Bindseil, "Tiered CBDC and the financial system," ECB Working Paper 2351, European Central Bank, https://ssrn.com/abstract=3513422, 2020.

[8] P. Sandner, J. Gross, L. Grale, and P. Schulden, "The Digital Programmable Euro, Libra and CBDC: Implications for European Banks," Tech. Rep. July, Frankfurt School of Finance & Management, https://papers.ssrn.com/abstract=3663142, 2020.

[9] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," *IEEE Communications Surveys Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015.

[10] B. Ahlgren, M. Hidell, and E.-H. Ngai, "Internet of things for smart cities: Interoperability and open data," *IEEE Internet Computing*, vol. 20, no. 6, pp. 52–56, 2016.

[11] J. Manyika, M. Chui, J. Bughin, R. Dobbs, P. Bisson, and A. Marrs, *Disruptive technologies: Advances that will transform life, business, and the global economy*, vol. 180. McKinsey Global Institute San Francisco, CA, 2013.

[12] P. Rogaway, "The Moral Character of Cryptographic Work," working paper, U.C. Davis, 2016.

[13] L. Swartz, *New Money: How Payment Became Social Media*. Yale University Press, August 2020.

[14] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," whitepaper, www.bitcoin.org, https://bitcoin.org/bitcoin.pdf, 2008.

[15] V. Buterin, "Ethereum whitepaper," tech. rep., Ethereum Foundation, https://ethereum.org/en/whitepaper/, 2013.

[16] Z. Amsden, R. Arora, S. Bano, M. Baudet, S. Blackshear, A. Bothra, and G. Cabrera, "The Libra Blockchain - White Paper," tech. rep., Libra Foundation, https://www.diem.com/en-us/white-paper/, 2019.

[17] C. Barotini and H. Holden, "Proceeding with caution - a survey on central bank digital currency," *Bank for International Settlements*, vol. 101, no. 1682-7651, pp. 1–15, 2019.

[18] C. M. Kahn, F. Rivadeneyra, and T.-N. Wong, "Should the central bank issue e-money?," Staff Working Paper 2018-58, Bank of Canada, https://www.bankofcanada.ca/2018/12/staff-working-paper-2018-58/, December 2018.

[19] J. Miedema, C. Minwalla, M. Warren, and D. Shah, "Designing a CBDC for Universal Access," tech. rep., Bank of Canada, 2020.

[20] CPMI-MC, "Central bank digital currencies," Tech. Rep. March, Bank for International Settlements, 2018.

[21] E. A. Opare and K. Kim, "A Compendium of Practices for Central Bank Digital Currencies for Multinational Financial Infrastructures," *IEEE Access*, vol. 8, pp. 110810–110847, 2020.

[22] T. Khiaonarong and D. Humphrey, "Cash Use Across Countries and the Demand for Central Bank Digital Currency," tech. rep., International Monetary Fund, mar 2019.

[23] N. Pocher and A. Veneris, "Privacy and transparency in cbdcs: A regulation-by-design aml/cft scheme," research paper, SSRN, https://papers.ssrn.com/abstract=3759144, December 2020.

[24] R. Auer, G. Cornelli, and J. Frost, "Rise of the central bank digital currencies: drivers, approaches and technologies," BIS Working Papers 880, Bank for International Settlements, https://www.bis.org/publ/work880.pdf, August 2020.

[25] D. Shah, R. Arora, H. Du, S. Darbha, J. Miedema, and C. Minwalla, "Technology approach for a CBDC," Staff Analytical Note 2020-6, Bank of Canada, https://www.bankofcanada.ca/2020/02/staff-analytical-note-2020-6/, February 2020.

[26] H. Chen, W. Engert, K. P. Huynh, G. Nicholls, M. Nicholson, and J. Zhu, "Cash and COVID-19: The impact of the pandemic on the demand for and use of cash," staff discussion paper, Bank of Canada, 2020.

[27] R. Litan, "What should banks do?," tech. rep., Brookings Institution, 1987.

[28] J. Pierce, *The Future of Banking*. Yale University Press, 1991.

[29] S. Kobayakawa and H. Nakamura, "A Theoretical Analysis of Narrow Banking Proposals," *Monetary and Economic Studies*, vol. 18, pp. 105–118, May 2000.

[30] R. Abraham, E. S. Bennett, N. Sen, and N. B. S. S. Francis, "State of adhaar report 2016-17," tech. rep., ID Insight, May 2017.

[31] M. Ricks, J. Crawford, and L. Menand, "Fedaccounts: Digital dollar," Research Paper 18-33, UC Hastings Research Paper No. 287, Vanderbilt Law, https://ssrn.com/abstract=3192162, 2020.

[32] Canadian Banker Association, "Canada's Digital ID Future - A Federated Approach," whitepaper, Canadian Banker Association, https://cba.ca/embracing-digital-id-in-canada, Spring 2018.

[33] K. Yang, D. Blaauw, and D. Sylvester, "Hardware Designs for Security in Ultra-Low-Power IoT Systems: An Overview and Survey," *IEEE Micro*, vol. 37, pp. 72–89, 2017.

[34] ECB, "Exploring anonymity in central bank digital currencies," Tech. Rep. 4, European Central Bank, https://www.ecb.europa.eu, 2019.

[35] K. P. Huynh, G. Nicholls, and M. W. Nicholson, "2019 cash alternative survey results," Staff Discussion Paper 2020-8, Bank of Canada, 2020.

[36] T. Philippon, "The fintech opportunity," Working Paper 22476, National Bureau of Economic Research, August 2016.

[37] European Central Bank and Bank of Japan, "Balancing confidentiality and auditability in a distributed ledger environment," Tech. Rep. February, European Central Bank, 2020.

[38] P. Li, G. Wang, X. Chen, F. Long, and W. Xu, "Gosig: A scalable and high-performance byzantine consensus for consortium blockchains," in *Proceedings of the 11th ACM Symposium on Cloud Computing*, SoCC '20, (New York, NY, USA), p. 223–237, Association for Computing Machinery, 2020.

[39] U. Dolata, "The digital transformation of the music industry. the second decade: from download to streaming," Discussion Paper 2020-04, SOI, 2020.

[40] A. Cavoukian, "Privacy by design: Origins, meaning, and prospects for assuring privacy and trust in the information era," in *Privacy Protection Measures and Technologies in Business Organizations: Aspects and Standards* (G. O. Yee, ed.), (http://doi:10.4018/978-1-61350-501-4.ch007), pp. 170–208, IGI Global, 2012.

[41] A. Shah, J. Bettman, and J. Payne, "How the pain of payment can magnify and mitigate choice overload effects," discussion paper, Rotman School of Management, 2019.

[42] D. Duffie, "Interoperable Payment Systems and the Role of Central Bank Digital Currencies," *Finance and Insurance Reloaded, Institut Louis Bachelier Annual Report*, 2020.

[43] W. Bossu, M. Itatani, C. Margulis, A. Rossi, H. Weenink, and A. Yoshinaga, "Legal aspects of central bank digital currency: Central bank and monetary law considerations," Working Paper 20/254, IMF, November 2020.

[44] Department of Finance Canada, "A new retail payments oversight framework: Invitation for comments," tech. rep., Government of Canada, October 2017.

[45] OSFI, "Deposit-taking institutions," tech. rep., Office of the Superintendent of Financial Institutions, January 2020.

[46] OSFI, "Table of guidelines," tech. rep., Office of the Superintendent of Financial Institutions, November 2020.

[47] G. Pennacchi, "Narrow banking," *Annual Review of Financial Economics*, vol. 4, no. 1, pp. 141–159, 2012.

[48] OSFI, "Smsb capital and liquidity requirements- consultative documents," tech. rep., Office of the Superintendent of Financial Institutions, January 2020.

[49] OSFI, "Cyber security self-assessment guidance," memorandum, Office of the Superintendent of Financial Institutions, October 2013.

[50] OSFI, "Technology and cyber security incident reporting," advisory, Office of the Superintendent of Financial Institutions, January 2019.

[51] Canadian Securities Administrators, "Proposed framework for crypto-asset trading platforms," consultation paper 21-402, Canadian Securities Administrators / Investment Industry Regulatory Organization of Canada, March 2019.

[52] Canadian Securities Administrators, "Guidance on the application of securities legislation to entities facilitating the trading of crypto assets," staff notice 21-327, Canadian Securities Administrators, January 2020.

[53] M. Ogilvie, *Bank and Customer Law in Canada, 2nd Edition.* Irwin Law Inc, 2013.

[54] B. Crawford Q.C., *Law of Banking and Payments in Canada.* Thomson Reuters Canada, 2020.

[55] Bank of Canada, "Retail payments supervision," tech. rep., Bank of Canada, 2019.

[56] FINTRAC, "Money services businesses (msbs)," tech. rep., Financial Transactions and Reports Analysis Centre of Canada, November 2020.

[57] FINTRAC, "Register your money services business (msb) or your foreign money services business (fmsb)," tech. rep., Financial Transactions and Reports Analysis Centre of Canada, March 2020.

[58] FINTRAC, "Compliance program requirements under the proceeds of crime (money laundering) and terrorist financing act (pcmltfa) and associated regulations," tech. rep., Financial Transactions and Reports Analysis Centre of Canada, December 2017.

[59] FINTRAC, "When to identify individuals and confirm the existence of entities-money services businesses," tech. rep., Financial Transactions and Reports Analysis Centre of Canada, June 2017.

[60] FINTRAC, "Transaction reporting requirements," tech. rep., Financial Transactions and Reports Analysis Centre of Canada, December 2020.

[61] FINTRAC, "Record keeping," tech. rep., Financial Transactions and Reports Analysis Centre of Canada, August 2019.

[62] FINTRAC, "When to identify individuals and confirm the existence of entities- financial entities," tech. rep., Financial Transactions and Reports Analysis Centre of Canada, June 2017.

[63] FINTRAC, "Record keeping requirements for money services businesses," tech. rep., Financial Transactions and Reports Analysis Centre of Canada, February 2020.

[64] Bank for International Settlements, "Central bank digital currencies: foundational principles and core features," CBDC report no 1, BIS, 2020.

[65] S. Mohammad and R. Davoodalhosseini, "Central banking digital currency and monetary policy," staff working paper 2018-36, Bank of Canada, July 2018.

[66] S. Hyman, C. Pennycook, D. Vesey, and N. Williams, "Canada," in *The Banking Regulation Review- Edition 6*, Law Business Research Ltd., May 2015.

[67] Government of Canada, "Who FCAC regulates," tech. rep., Government of Canada, June 2019.

[68] Y. J. Fanusie, "Central Bank Digital Currencies: The Threat From Money Launderers and How to Stop Them," *The Digital Social Contract: A Lawfare Paper Series*, pp. 1–23, November 2020.

[69] S. Darbha and R. Arora, "Privacy in CBDC technology," staff analytical note 2020-9, Bank of Canada, June 2020.

[70] Office of the Parliamentary Budget Officer, "Preliminary findings on international taxation," tech. rep., , June 2019.

[71] B. Ball, "CRA requests for personal banking info: Out of line?," tech. rep., Chartered Professional Accountants Canada, January 2019.

[72] FINTRAC, "Who is not eligible to register?," tech. rep., Financial Transactions and Reports Analysis Centre of Canada, March 2020.

[73] L. Schilling, J. Fernández-Villaverde, and H. Uhlig, "Central bank digital currency: When price and bank stability collide," working paper, SSRN, https://ssrn.com/abstract=3606226, May 2020.

[74] A. García, B. Lands, X. Liu, and J. Slive, "The potential effect of a central bank digital currency on deposit funding in canada," Staff Analytical Note 2020-15, Bank of Canada, https://www.bankofcanada.ca/2020/07/staff-analytical-note-2020-15/, 2020.

About the Authors

Professor Andreas Veneris is a Connaught Scholar and Professor at the Department of Electrical and Computer Engineering, cross-appointed with Computer Science at the University of Toronto. He obtained a Ph.D. from the University of Illinois, Urbana-Champaign in 1998. He was a joint faculty at the Athens University of Economics and Business (2006-16) and at the University of Tokyo (2010-11). His research in blockchain focuses on mechanism/system design, formal methods, IoT, techno-legal questions and cryptoeconomics. He has published more than 140 papers, received a 10-year Best Paper Retrospective Award, and other best paper awards and patents. He was member of the team in the first webcast ever (37^{th} Grammy Awards, 1995), an event acknowledged by the American Congress.

Professor Andreas Park is an Associate Professor of Finance at the University of Toronto Mississauga and cross-appointed to the Rotman School of Management. He received his Ph.D. in Economics from Cambridge University in 2004, and he visited Copenhagen Business School 2014-15. He currently serves as the Research Director at the FinHub, Rotman's Financial Innovation Lab, he is the co-founder of UTLedgerHub, the University of Toronto's blockchain research lab, a lab economist for blockchain at the Creative Destruction Lab, and a consultant to the OSC and IIROC. Andreas teaches courses on FinTech, decentralized finance, and financial market trading, and his current research focuses on the economic impact of technological transformations such as blockchain technology.

Professor Fan Long is an Assistant Professor at University of Toronto, Department of Computer Science cross-appointed with the Department of Electrical and Computer Engineering. He obtained a Ph.D. from MIT in 2017. His research interests include blockchain systems, consensus algorithms, programming languages, systems security, and software engineering. He is a recipient of the ACM SIGSOFT Outstanding Dissertation Award and the MIT Best Dissertation Award. He has won several gold medals in world programming contests (IOI 2005/2006 and ACM/ICPC 2008). In parallel of his academic duties, he also leads the Conflux Network, a project that builds a next generation blockchain platform.

Professor Poonam Puri is a Professor at Osgoode Hall Law School at York University and one of Canada's leading experts in governance and financial regulation. She is Founder and Director of the Business Law LL.M. and Co-Founder and Academic Director of the Investor Protection Clinic at Osgoode, the first of its kind in Canada. Co-author of Back from the Brink: Lessons from the Canadian Asset-Backed Commercial Paper Crisis, Poonam has written numerous books, book chapters, scholarly articles and commissioned research reports on corporate governance, securities, and capital market regulation. Poonam currently serves on the board of the Canada Infrastructure Bank and is a former Commissioner of the Ontario Securities Commission. Poonam is a recipient of a 2016 Trudeau Foundation Fellowship, has been also recognized as one of the top 25 most influential lawyers in Canada by Canadian Lawyer Magazine, and she has been selected as one of Canada's Top 40 under 40. She is a graduate of the University of Toronto (LL.B) and Harvard Law School (LL.M).