A Proposal for a Canadian CBDC

Model X Final Report

Kyoung Jin Choi
Haskayne School of Business
kjchoi@ucalgary.ca

Ryan Henry
Department of Computer Science
ryan.henry@ucalgary.ca

Alfred Lehar
Haskayne School of Business
alehar@ucalgary.ca

Joel Reardon
Department of Computer Science
joel.reardon@ucalgary.ca

Reihaneh Safavi-Naini
Department of Computer Science
rei@ucalgary.ca

February 11, 2021

Executive Summary

Undoubtedly inspired by recent advances in technology-driven payment systems such as mobile payment systems, cryptocurrencies, and blockchain technologies, recent years have seen central banks worldwide explore the possibility of issuing digital forms of fiat money called *central bank digital currencies* or *CBDCs*. A thoughtfully designed CBDC can help satisfy numerous policy objectives, improve economic efficiency and inclusivity, and serve as a platform for economic innovation. However, the vast CBDC design landscape, coupled with its potential to massively disrupt the financial system and broader economy, warrants caution, calling for a careful and methodical analysis of various designs' strengths, weaknesses, and risk profiles.

At this time, the Bank of Canada (BoC) has not committed to issuing a CBDC; nevertheless, it does rank among the more than 80% of central banks globally who, according to a recent survey by the Bank for International Settlements (BIS) [1], are at least contingency planning for the eventuality of doing so. This report details and analyzes the authors' vision for a hypothetical BoC-issued retail CBDC for use in the Canadian context, taking into account both (i) the "business case" for its adoption from the perspective of BoC, policymakers, the financial services industry, and the Canadian economy more generally and (ii) how its widespread adoption would impact ordinary Canadians.

The design considered in this report leverages a mix of *distributed ledger technologies* (*DLTs*) and electronic cash ("e-cash") schemes with advanced cryptographic primitives. The confluence of these building blocks results in a scalable, resilient, privacy-centric, and universally accessible design that strives to bring added value (a Pareto improvement) for all stakeholders in Canada. In light of the abundance of CBDC designs in circulation, this report emphasizes aspects and implications of the design specifically tailored for Canada, such as ensuring universal access

for remote communities and strong privacy protections consistent with Canada's role as a world leader in civil liberties and human rights. Likewise, some core aspects of the proposed architecture reflect characteristics of Canadian law and the Canadian financial system, which may differ substantially from other countries. While specific design choices discussed herein have benefited from discussions with economists and technologists at BoC, the system is entirely hypothetical. Except where explicitly stated otherwise, no aspects of this work reflect the stated intentions or official policy goals of BoC—all views and opinions expressed are those of the authors alone.

Contents

FRONT MATTER

MAIN MATTER

1 Introduction

Recent years have seen advances in technology-driven payment systems such as mobile payments, cryptocurrencies, and blockchain technologies, coincident with central banks worldwide exploring the possibility of issuing digital forms of fiat money called *central bank digital currencies* or *CBDCs*. A CBDC is an electronic payment instrument that can substitute cash in daily transactions, offering enhanced functionality to foster economic growth and efficiency. Existing means of digital payments, such as debit or credit cards, are inadequate substitutes for digital cash because they (i) provide scant privacy protection from card issuers and merchants, (ii) reinforce inequality through their limited accessibility for certain marginalized groups, (iii) facilitate the accumulation of high-interest consumer debt, and (iv) have a high market concentration that limits competition and innovation, resulting in high transaction fees disproportionately borne by small merchants.

The Bank of Canada (BoC) has expressed interest in exploring the design space for a hypothetical Canadian CBDC and has publicly stated several design goals [5, 3, 6, 8]. Their design goals include (i) *security and privacy* with support for privacy-preserving online retail payments, (ii) *universal access* including for those in underbanked communities and without access to reliable, always-on Internet, (iii) *resiliency and robustness* against accidental and intentional failures, (iv) *legal compliance* with national and international obligations, and (v) *performance and scalability* commensurate with Canada's large and geographically dispersed economy.

While laudable, these design goals are clearly in tension. For instance, unrestricted anonymity is at odds with legal compliance for anti-money laundering regulations, and it presents challenges for mitigating the threat of fraud in offline transactions. The CBDC design proposed herein tries to strike a balance between the BoC's design goals through an open and modular architecture leveraging the latest cryptography and security technologies.

Our proposed design revolves around Banking$^+$ and Cash$^+$, our vision for "smart" alternatives to traditional banking and cash. For Banking$^+$, we contemplate an account-centric view that replicates routine commercial banking but adds novel components made possible via so-called *smart contracts* that can settle natively in both CBDC and bank-generated money (i.e., commercial bank liabilities). For Cash$^+$, we contemplate a cash-centric view of CBDC with anonymous tokens exchangeable both in person or online and offering a rich new feature set unimaginable with physical coins and banknotes. Legal compliance requirements are enforced within the Banking$^+$ realm and at the interface between Cash$^+$ and Banking$^+$.

Cash$^+$ tokens are legal tender and, as such, are fungible with coins, banknotes, and commercial bank money. Users can withdraw Cash$^+$ tokens from their Banking$^+$ accounts, purchase them (much like SIM cards, gift cards, or prepaid credit cards) from convenience stores or currency exchange kiosks at airports, or receive them in exchange for goods and services rendered. They provide significant advantages over traditional cash, such as being usable (anonymously) for online purchases, inputtable to smart contracts, and potentially recoverable if it is lost.

Both Cash$^+$ tokens and funds held in CBDC-denominated Banking$^+$ accounts (herein referred to as "*CBDC accounts*") are direct central bank liabilities. Banking$^+$ accounts can also hold commercial bank money; indeed, Banking$^+$ smart contracts can transact both with CBDC and with commercial bank liabilities by purchasing CBDC using bank money (and vice versa) as needed. This interoperability is crucial to realize the economic gains that motivate adoption.[1]

While Banking$^+$ and Cash$^+$ are mutually complementary ideals, neither is inherently dependant on the other. Banking$^+$ services could easily exist without support for anonymous Cash$^+$ tokens; likewise, the BoC could provide standalone mechanisms using which banks could allow users to withdraw and deposit Cash$^+$ tokens using traditional, non-Banking$^+$ accounts.

[1] See Figure 4.1 in Section 4 for an overview of this architecture's essential components.

1.1 Benefits of a CBDC

We consider the voluntary adoption of a CBDC by all stakeholders crucial to its success. A CBDC that fails to add value, improve efficiency, benefit consumers, simplify commerce, and reduce financial friction will not succeed. We strive to design a system that makes banks enthusiastic about supporting it while providing consumers with greater access to efficient financial products.

From a consumer perspective, we envision CBDC underlying an ecosystem of efficiency-increasing, cost-saving, and accessibility-improving financial products that go beyond supporting traditional retail payments. For just a few examples, individuals might use Banking$^+$ facilities to hold rental security deposits in an interest-accruing escrow, replace expensive payday loans with employer-provided advances for hours worked, disburse benefit payments like Health Spending Account (HSA) funds and Canadian Emergency Response Benefit (CERB), and augment automated bill payments to settle from lines of credit when liquid funds are insufficient. Financial intermediaries and entrepreneurial fintech companies could build these and other innovative financial instruments using a mix of advanced cryptographic building blocks and smart contracts that settle natively in CBDC. Thus, CBDC scalability—from micropayments to million-dollar transactions—will be a crucial driver of innovation in the CBDC ecosystem.

From a corporate and banking perspective, we envision the automation and enhancement of routine transactions via smart contracts built on trusted and reliable distributed ledgers. Examples include automated insurance, assurance contracts, foreign exchange hedging, and bond coupon payments. Several innovative solutions along these lines are already in nascent stages of deployment. However, an inability to settle financial claims arising from smart contracts using central bank currency presently hinders their widespread adoption. A CBDC will preserve Canadian monetary sovereignty by directly underpinning these crucial applications.

1.2 Roadmap

Chapter 2 reviews and expands the BoC's design goals for a Canadian CBDC. Chapter 3 presents our proposed architecture. Chapter 4 analyzes the business case for our design. Chapter 5 revisits the design goals and analyzes our design with respect to them. Finally, Chapter 6 concludes.

2 Design Goals

This chapter enumerates the design goals for a Canadian CBDC, as stated in Bank of Canada publications [5] and considered in staff technical notes [3, 6, 8].[1] We accompany each goal with a discussion of our interpretation, which contextualizes the design we give in this report.

Besides the five BoC design goals listed in this chapter, we evaluate the viability of our design against two further economic goals:

1. *Economic value creation:* A CBDC should create overall economic value for Canadians, i.e., it should be a "positive net present value" project; and
2. *Universal adoption:* All stakeholders in Canada should have incentives to participate in the CBDC ecosystem—it does not make sense to build a technically sophisticated system that nobody uses.

These economic design goals are discussed further in Chapter 4.

2.1 Security and privacy

A viable CBDC design requires long-term security against well-equipped adversaries and in the face of advances in computing and cryptanalysis. Maintaining the requisite security level will require a robust "defence-in-depth" strategy (wherein multiple independent safeguards must fail in unison for an attack to succeed) and mechanisms for both for recovering from successful attacks and for evolving protection mechanisms in response to technological advances.

While the need for robust security protections in financial systems is universally acknowledged, the high degree of privacy that BoC is targeting differentiates a

[1] We emphasize that BoC staff technical notes are *not* official Bank policy positions.

hypothetical Canadian CBDC not only from those contemplated by the central banks in some other countries but also from all but the most privacy-centric of cryptocurrencies. Realizing strong privacy protection in tandem with the other design goals presents nontrivial technical challenges, yet BoC has identified support for private retail payments as a crucial public good [3, 5].

Privacy is an essential prerequisite for other fundamental rights, such as *freedom of expression* and *freedom of association*. Privacy for retail CBDC transactions can reduce chilling effects, such as for those wary of purchasing from online cannabis shops [2] or donating to unpopular political causes [4]. Privacy further prevents private entities from unilaterally imposing unofficial moratoria on transactions involving specific individuals or organizations (as Visa, Mastercard, and PayPal famously did with donations to Wikileaks in 2010 [9]).

2.2 Universal access

A crucial feature of cash is that everyone—including members of unbanked or underbanked populations—can participate with virtually no legal or technological impediments. A digital replacement should go beyond merely replicating this essential property by expanding it to allow universal participation in Canada's increasingly digital economy. If CBDC were to largely supplant physical banknotes as a medium of exchange, it would present new opportunities to decrease Canada's digital divide and bolster economic inclusion for marginalized populations.

An acute concern, particularly in the context of an "online-only" CBDC, is how to support those in remote and underbanked communities having only sporadic, high-cost, or low-bandwidth Internet access as well as no cellular service. Indeed, even in major population centres, some segments of the population (e.g., those experiencing homelessness) lack access to smartphones or bank accounts. Therefore, universal access to a hypothetical Canadian CBDC cannot assume universal access to the Internet or Internet-enabled mobile devices. Other groups requiring access to a Canadian CBDC would include transient populations, such as migrant workers and tourists, who are unlikely to hold CBDC-aware bank accounts or the

legal status required to open conventional bank accounts. Such transient populations may also lack convenient, low-cost access to the Internet during their time in Canada.

Other groups epitomizing the need for universal access include vulnerable populations like incarcerated individuals (who are forbidden from using personal electronic devices), undocumented immigrants (who might not have entered Canada via a standard port of entry, where CBDC onboarding for visitors may typically occur), and survivors of domestic abuse or human trafficking (whose finances may be surveilled or controlled by an abusive or coercive force).

We further note that CBDC should be accessible to persons with disabilities (be they visual, motor, cognitive, or otherwise), which may necessitate the development of specialized hardware or software systems implementing accessibility features like voice recognition, text-to-speech, or digital braille. Such accessibility systems are mostly orthogonal to the underlying CBDC design proposed herein.

2.3 Resiliency and robustness

Financial institutions and payment-processing facilities are critical infrastructures that must maintain availability in the presence of accidents and natural disasters, electrical blackouts, transient network failures, and deliberate sabotage or cyberattacks, notably including those perpetrated by well-funded, state-sponsored foreign actors.

Presently, Canadians can use cash if some critical financial infrastructure becomes temporarily unavailable. Likewise, a robust CBDC design must allow for, at a minimum, the continued operation of some minimal subset of vital financial services if BoC or one or more financial intermediaries is temporarily unavailable. To this end, a Canadian CBDC design should leverage technologies that provide precise and explicit guarantees that the system can continue to function usefully despite periodic failures, provisioned with ample and redundant networking and hardware resources, and deployed in a geographically distributed manner across all regions of Canada. Furthermore, the design must incorporate well-defined, action-

able policies and procedures that allow financial institutions to continue servicing basic CBDC transactions if confronted with an unexpected connectivity loss or partitioning of the network.

From the CBDC holders' perspective, a resilient CBDC should include features to deal gracefully with, for example, the unplanned-for need to access CBDC in remote areas lacking online connectivity, misplacing of account credentials like passwords and cryptographic keys, and perhaps even device failures that result in the loss of "offline" CBDC holdings.

At the intersection of security, privacy, and resilience is the need for cryptographic agility: a CBDC design must provide mechanisms to seamlessly upgrade cryptographic primitives in response to a steady stream of cryptanalytic and technological advances. The system should employ forward-secure design patterns to ensure that newly discovered weaknesses have minimal impact on past transactions' security and privacy. Moreover, cryptographic primitives should be readily "hot-swappable" in near real-time in response to policy directives from lawmakers or BoC.

2.4 Legal compliance

A Canadian CBDC must comply with anti-money laundering (AML) and combating the financing of terrorism (CFT) regulations and requirements, all relevant federal, provincial, and territorial privacy legislation, and international agreements (e.g., GDPR, international treaties, sanctions). In addition to these regulations—which are, at least theoretically, enforceable via automated means—any CBDC would require mechanisms through which authorized agents can "unmask" some otherwise private transactions in response to warrants or subpoenas. The main challenge will be reconciling the need for robust legal compliance with security and privacy requirements. Optimally balancing these conflicting ideals will require a Privacy-by-Design (PbD) approach at all CBDC design and development stages.

Transparency will be a crucial component of compliance: a hypothetical Canadian CBDC should reinforce—not undermine—Canada's position as a world leader in civil liberties and human rights. Lawful access, fraud detection, and AML/CFT

requirements all necessitate means to circumvent privacy protections in specific, legally prescribed scenarios. Nevertheless, the design should ensure that these mechanisms cannot be misused as general-purpose "backdoors" that allow certain entities to subvert security and privacy arbitrarily; indeed, the general public should have (trustworthy) visibility into the use of these mechanisms.

2.5 Performance and scalability

Any deployed CBDC must be fit for purpose—it must be useful and function while processing transactions for millions of Canadians. Published BoC literature contemplates a minimum of 1,000 transactions per second, which they equate to "25 million people making 2 payments per day spread evenly over 12 hours" [8]. However, if CBDC becomes a ubiquitous form of retail payments in Canada, the need to support significantly higher transaction throughput (e.g., more than 10,000 transactions per second) could arise within a decade or less. Transaction throughput is not the only performance constraint for a CBDC: transaction latency (i.e., the amount of time that payees must wait for transactions to clear) will be vital for CBDC's acceptance.

Achieving high throughput, low latency, and robust security and privacy at the same time is nontrivial. The need to ensure compliance with all applicable laws and regulations only compounds the difficulty, suggesting that the need for compromise is unavoidable. Yet there is no "one-size-fits-all" compromise to make. Instead, a CBDC must provide a portfolio of transaction types offering a spectrum of privacy, performance, transaction cost, and compliance profiles, together with a fast and frictionless way for CBDC holders to choose the most appropriate transaction type for any given scenario.

3 Proposed Architecture

This chapter describes our proposed architecture for a hypothetical Canadian CBDC.

3.1 Entities

Our proposed CBDC architecture comprises three main types of entities: (i) the central bank, (ii) financial intermediaries, and (iii) users. Each entity runs a software agent supporting interaction between that entity and other entities in the CBDC ecosystem.

3.1.1 Central bank

The *central bank* (in this case, BoC) is the sole issuer of CBDC. It maintains its balance sheet on a so-called *core ledger* that holds the ultimate record of (transactions involving) central bank liabilities, whether stored in CBDC accounts or drawn down as offline Cash^+ tokens. While it is technically possible for users to hold CBDC accounts directly on the core ledger, we do not imagine this to be the typical use case. Instead, we envision a core ledger primarily reflecting (i) balances and transactions for reserve accounts held by licensed financial intermediaries (FIs) and (ii) any offline Cash^+ tokens presently in circulation.

Core ledger: The core ledger is an ordered, timestamped, and tamper-resistant list of transactions among FIs or between FIs and the central bank. Essential properties of the core ledger include:

1. *Resilience and robustness:* As the CBDC infrastructure's backbone, the core ledger's continuous operation and availability are imperative. It must be able to withstand network and hardware failure and cyberattacks under high traffic volume without any loss of availability or improper accounting of

central bank liabilities. While the central bank is the ultimate custodian of the core ledger, each FI should hold an up-to-date and publicly verifiable replica of all ledger entries about its own claims on the central bank. The replicas may allow FIs to perform certain operations locally, reducing the load on the core ledger; however, their primary purpose is to ensure resilience in the face of transient failures at the central bank. Indeed, it should be possible to reconstruct the entire core ledger in a verifiable way by piecing together the replica fragments held by each FI reflected on it.

2. *(Long-term) security:* The core ledger must guarantee integrity, immutability, and privacy of current and past transactions over long periods (i.e., over several generations). While we do not envision that ledgers will store detailed transaction records indefinitely, it remains prudent to hedge against the risk of cryptographic advances that might make it feasible to retroactively "undo" or deanonymize transactions—even years after the fact. A direct threat to long-term cryptographic security comes from research advancements in computing and cryptanalysis (e.g., developments in quantum computing); thus, the core ledger must allow for the seamless updating of security parameters and replacement of algorithms as security requirements evolve.

3. *Other properties:* The core ledger must also be (i) scalable enough to service tens of thousands of retail transactions per second[1]; (ii) fast enough to process transactions with nearly imperceptible latency (e.g., at most tens of milliseconds); and (iii) extensible enough to allow overlay services that will undoubtedly arise with changing demand and service updates.

The core ledger must provide privacy for CBDC account holders via effective access control mechanisms that govern each FI's authority to read ledger entries following a "need-to-know" policy. The central bank grants CBDC account holders access to the core ledger through standardized Application Programming Interfaces (APIs).

[1]Most retail transactions need not be reflected directly on the core ledger; rather, we mean that the core ledger must be able to keep pace with the CBDC settlement among FIs who collectively process tens of thousands of retail transactions per second.

3.1.2 Financial intermediaries

Financial Intermediaries (FIs) are authorized and regulated entities that use the core ledger's APIs and provide interfaces for users' payment and financial services. These services include the clearing and settlement of Banking$^+$ transactions involving users serviced either by the same FI or by peer FIs (requiring CBDC transfers between FI reserve accounts on the core ledger), the deployment and execution of smart contracts, and the drawing down of funds as offline Cash$^+$ tokens. We identify three classes of FI:

1. *Chartered:* The chartered banks (including the "big five"), who have special legal status and obligations under Canadian law;
2. *LVT:* A superset of chartered FIs consisting of all FIs that qualify to participate in Canada's large-value transfer (LVT) system; and
3. *Other MSBs:* All non-LVT FIs, including credit unions, insurance issuers, credit providers, fintech companies, brokerages, and other money services businesses (MSBs) that directly hold claims against the central bank. For universal access, we also envisage some indigenous tribal councils and municipal governments from remote communities acting as FIs.

In addition to holding a replica of core-ledger entries relating to its claims against the central bank, each FI will hold its own (segregated) ledger, reflecting its clients' holdings, internal transactions, and any transactions with other FIs that do not directly map to CBDC transfers on the core ledger. Where legally applicable, FIs are responsible for following proper KYC regulations when onboarding new users.

FIs extend the functionality of CBDC in response to the users' needs; for example, they may provide

1. user-friendly interfaces for users on web or mobile devices to allow them to buy, sell, and use (both online and offline) CBDC holdings;
2. physical "GUI-less" devices to hold and use offline Cash$^+$ tokens;
3. menus of "vetted" smart contracts that leverage the API exposed by the core ledger and other FI's ledgers to automate financial and economic processes.

We envision the "chartered FIs" playing a vital role in the CBDC ecosystem due to their unique status under Canadian law. Specifically, we propose that any legislation enacted to authorize the deployment of a Canadian CBDC also updates the legal mandate of the chartered banks to require interoperability—i.e., by requiring them to expose the same, standardized API as the core ledger. The goal is to ensure that innovative financial instruments based on smart contracts can seamlessly cross the boundary between chartered FIs,providing a legislative solution to what may otherwise be an insurmountable coordination problem. Legislation might also amend the requirements for participating in a CBDC-specific analog of the large-value transfer system to include supporting (a subset of) the core ledger's API, ensuring further coordination. Such legislated coordination will provide strong incentives for non-LVT FIs to adopt interoperable technology stacks that can fully participate in the CBDC ecosystem.

3.1.3 Users

The *users* encompass all of the other non-FI economic actors, be they actual people, corporate entities, trusts, merchants, or any other legal entities that hold or use CBDC without holding a CBDC account on the core ledger. We identify two distinct classes of users:

1. *KYCed users:* Users that interact with CBDC through accounts held by regulated FIs and subject to Know-Your-Customer (KYC) requirements; and
2. *Non-KYCed users:* Users that interact with sufficiently small amounts worth of restricted-functionality CBDC, exempting them from KYC requirements.

There is no one-to-one mapping between economic actors and users: a single actor may hold multiple KYCed accounts with different FIs while simultaneously handling small quantities of CBDC as a non-KYCed user. Both user classes will receive credentials, and possibly hardware devices or software, from one or more FIs, with which they will access and use CBDC.

KYCed users have Banking$^+$ accounts with one or more FI to buy, sell, and transact with both bank-issued money and CBDC. In most cases, we envision such users

participating in the familiar fractional-reserve banking system, with accounts that hold claims on the FI rather than true CBDC (a central bank liability). However, FI-hosted smart contracts' ability to seamlessly and transparently leverage the core ledger's API to exchange between bank money and CBDC enables a host of unconventional financial products that rely on native settlement in central bank currency. Beyond simple retail payments and balance transfers, we envision early options that will include (i) repeated micropayments for on-demand usage-based charging (e.g., taxis, metered utilities), (ii) one-off micropayments for access to a single item (e.g., creative works or news articles), and (iii) conditional payments that clear if and only if certain observable conditions are satisfied. As CBDC adoption grows, we believe that FIs, both old and new, will begin to offer innovative new products that automate, improve, or enable a host of financial and economic functions.

KYCed users can also draw down their holdings as offline Cash^+ tokens—digital loonies. We envision CBDC tokens that are completely anonymous unless misused (e.g., double-spent), in which case BoC and the FIs can trivially link them to the user's KYCed identity. If such tokens are misused, the FI can leverage this KYCed identity to seek reimbursement or legal remedies. Non-KYCed users can likewise purchase offline Cash^+ tokens, subject to certain restrictions on values and ways to use these tokens. If merchants (or other payees) cannot deposit non-KYCed Cash^+ tokens in real-time (e.g., due to a lack of connectivity), then they may refuse to accept them—even where they would happily accept KYCed Cash^+ tokens—in order to insulate themselves from the risk of fraud. Insurance markets might emerge to help merchants better manage the risks associated with transacting with offline Cash^+ tokens in low-connectivity environments.

3.2 Core technologies

As detailed above, the BoC in our design bears sole responsibility for (i) maintaining a core ledger that interfaces with multiple FI ledgers and (ii) issuing CBDC and setting monetary policy. This core ledger must be resilient, secure, efficient, and provide timely responses to requests. The FIs will provide the bulk of retail pay-

ment services and consumer-facing technologies required for payment, account management and enforcement of rules and regulations concerning KYC, AML, and CFT.

The core ledger and the ledgers belonging to chartered FIs (and, probably, most other FIs) will expose a standard API allowing FIs and their users to transact with CBDC, most notably via smart contracts.

3.2.1 Core (permissioned) DLT

One could implement the core ledger using a variety of distributed-database technology stacks. We recommend distributed ledger technology (DLT), which has received significant attention and enjoyed focused research and development toward financial applications and smart contracts. Specifically, we propose using a "permissioned" private ledger (akin to Corda or Hyperledger Fabric) that is sufficiently expressive to implement a Turing-complete virtual machine such as the Ethereum Virtual Machine (EVM). Such DLT-based ledgers provide a robust, timestamped, tamper-resistant, and ordered log of transaction data. Essential properties of DLT for core ledger include providing reliability through the use of multiple (redundant) synchronized copies, flexibility in defining policies (consensus algorithms) around accepting and recording transactions ("writing" to the database), well-defined approach to creating an immutable sequential log of transactions, and support for smart contract.

The BoC-run core ledger will interact with (segregated) ledgers maintained by the FIs, forming a tiered permissioned ledger whose topology resembles a shallow-tree rooted at the core ledger. We do not prescribe a specific technology stack for FI ledgers;[2] instead, we merely insist that the FIs' ledgers (i) expose a standardized API to ensure interoperability with the core ledger and other FIs, and (ii) support a means to non-repudiably "commit" to snapshots of the ledger at a given point in time. The FIs interact with the core ledger and peer FIs' ledgers exclusively through the standardized API, which is accessible to all entities holding claims

[2]Nevertheless, we expect that most FIs would opt for a DLT-based backend, for precisely the same reasons we advocate using DLTs for the core ledger.

on the ledger. Any API calls that might trigger inter-ledger transactions will use snapshot commitments to "pin" transacting ledgers together, providing a point of synchronization and "ground truth" in case of future disputes or for routine auditing. This approach ensures equitable access to all FIs, making it difficult for a coalition of large FIs to hold a monopoly over the CBDC ecosystem.

3.2.2 The core API

APIs define the methods and abstractions that form the connecting tissue of software systems, allowing designers to control and restrict access to system resources in a modular way. As discussed above, both the core ledger and the ledgers held by the FIs will expose a standard API—herein referred to as *the core API*—and all transactions involving CBDC will occur through this core API.

Semantically, the core API comprises four sub-interfaces:

1. *Internal core:* A subset of methods and abstractions used *internally* by BoC or an FI, and not directly exposed to other FIs or users entities;
2. *Interbank core:* A subset of methods and abstractions used by BoC and FIs for inter-FI account maintenance, smart contracts, and transaction processing;
3. *Public core:* A subset of methods and abstractions exposed (indirectly, via the FIs) to users to provide $\mathsf{Banking}^+$ services (i.e., software hooks for CBDC settlement of smart contracts); and
4. *Offline core:* A subset of methods and abstractions to facilitate the withdrawal and deposit (and, in some cases, tracing or recovery) of offline Cash^+ tokens.

The interbank core API might expose wrappers around specific internal core API methods, providing external entities with access to internal data in limited cases. Depending on the request's nature, such wrappers might require the external entity to provide evidence of abuse, legal documents like a subpoena, or explicit consent from a user before they will be honoured. They may even require explicit authorization via a human-in-the-loop at the FI receiving the request.

A systematic, stakeholder-driven design of the core API, providing precise semantics and formal verification, will be essential to minimizing the risk of vulnerabilities

or loopholes in the CBDC platform, resulting in security failures or unwanted economic implications.[3] Ideally, we envision the core API specification (and reference implementations thereof) arising through an open stakeholder-driven "competition", modelled after those employed by the US National Institute of Standards and Technology (NIST) for standardizing cryptographic primitives.

3.2.3 Identity and fraud detection

Because end-users in our design will not typically hold CBDC accounts directly on the core ledger, the FIs will be responsible for onboarding users consistent with KYC rules and providing authentication services for them. We envision that existing FIs will leverage preexisting relationships to automate onboarding for their active clients and that they will adapt their legacy identity management infrastructure and workflows to support CBDC.

The core API must expose a set of identity-specific methods to facilitate CBDC-specific features like interbank fraud and anomaly detection, smart contracts with privacy, and double-spending mitigation for offline Cash^+ tokens. BoC, the FIs (including the smart contracts they run), and regulators will use the identity-specific core API methods to transact with specific users' accounts without necessarily learning their identities. For instance, the public core API should provide users with a mechanism to request (arbitrarily many) random pseudonyms that appear unlinkable but ultimately reference the same underlying account. Such on-demand pseudonyms allow users to participate in many transactions and smart contracts while resisting outsiders' attempts to profile and track their financial actions.[4] Users could further impose simple access control policies on pseudonyms, ensuring that others cannot co-opt a pseudonym created for transacting with a specific

[3] For example, Ethereum *flash loans* are useful for overcoming financial constraints while swapping collateral; however, they can also be abused to attack weaknesses in other protocols. In the context of CBDC, the core API might expose methods that are ultimately used for economic activities that BoC finds undesirable. Thus, the core API must be vetted from both technical and economic standpoints.

[4] Several for-profit companies (e.g., privacy.com, Blur, Revolut, and Entropay) presently offer similar "pseudonymous" access to traditional chequing accounts, which they market as *virtual cards* or *burner cards*.

entity—even if that pseudonym leaks in a data breach.

The transaction data and metadata stored between the core and FI ledgers contain a wealth of information useful for detecting patterns indicative of anomalous and fraudulent behaviour. New advances in machine learning and deep neural networks, for example, provide ample opportunities to design targeted- or general-detection algorithms that analyze this data and patterns of users' interactions with the system. To support fraud detection and compliance with lawful access requests while respecting privacy, the API should provide (meticulously audited) methods through which BoC, regulators, or law enforcement can run specific, targeted queries using users' pseudonyms or attributes of their KYCed identities as selectors.

As explained above, we defer to a formal process to specify an appropriate API; however, we note that a privacy-respecting API should leverage advanced cryptographic primitives where possible. Examples of this might include methods that (i) return zero-knowledge proofs instead of cleartext evidence, (ii) return secret-shared or encoded answers suitable for inputting to *secure multiparty computations* (*MPC*), (iii) generate bucketized, anonymized, or *differentially private* figures and statistics, or (iv) allow law enforcement to fetch account details obliviously using *private set intersection* (*PSI*) or *private information retrieval* (*PIR*) protocols.

3.2.4 Programmable CBDC and smart contracts

We use the term *smart contract* in a broad sense to reference "programmability" of CBDC payments in the Banking$^+$ realm, in the form of conditions that govern if, when, and how much CBDC to transfer from one or more source accounts into one or more destination accounts. Ensuring that a Canadian CBDC provides a platform for innovation for all segments of the Canadian economy—not just an entrenched coalition of influential FIs—will require a core API that is sufficiently expressive to support a wide range of useful smart contracts.

On one hand, fulfilling the conditions specified in a valid smart contract must *guarantee* the settlement of any resulting transactions. On the other hand, it will

be prudent to preserve the present-day practice of "netting" CBDC transfers among FIs for optimal efficiency and privacy. FIs might be required to store sufficient CBDC to settle all (or a portion of all) outstanding smart contracts in a designated reserve account on the core ledger to reconcile these conflicting goals. Additionally, third-party insurance might arise to help manage liquidity in an ecosystem of ubiquitous smart contracts.

A walled-garden approach: Smart contracts must balance the API's expressiveness with the need for secure execution, free of unforeseen loopholes or unintended side effects. Balancing these requirements will require (i) well defined operational semantics and correct implementation of those semantics, and (ii) verifiability of inputs. Thus, we envisage the development and deployment of smart contracts to be—at least in most instances—the purview of FIs rather than users. For example, FIs may provide a menu of carefully vetted *contract templates*, which their clients can deploy by specifying relevant "variables" through user-friendly interfaces provided by the FI. Such a menu might include smart contracts to automate everyday transactions where human intermediaries can be replaced with secure computer programs, such as holding rental security deposits in an interest-accruing escrow, replacing predatory payday loans with employer-provided advances for hours worked, disbursing benefit payments like Health Spending Account (HSA) funds and Canadian Emergency Response Benefit (CERB), or augmenting automated bill payments to settle from lines of credit when liquid funds are insufficient. We envision a thriving ecosystem of fintech companies offering innovative smart contracts, custom smart contract-development services, and insurance policies for smart contracts, which will emerge as awareness and comfort with cost-saving smart contracts grows among consumers and businesses.

A significant challenge in managing complex smart contracts is ensuring the validity of inputs from third parties called *oracles*, whose "off-ledger" data enhance smart contracts' functionalities by allowing transactions to trigger based on real-world events. Oracles obtain external data, verify them, and then provide them as input to smart contracts through the core API or other (market) data feeds. They can provide a broad range of context and auxiliary information such as weather

data, market data, price information, or random numbers for running simulations and other probabilistic computations. The veracity of any information provided by oracles is essential for the correct functioning of smart contracts; thus, we recommend that smart contracts access oracles from a menu of vetted, trustworthy sources in much the same way as the smart contracts that use them. Moreover, the central bank should restrict smart contracts that can trigger CBDC transactions on the core ledger to using only pre-approved oracles, ensuring that the BoC can independently verify if all conditions are satisfied as a prerequisite for automated settlement.

3.3 Users and accounts

We expect that most users will interact with CBDC through KYCed accounts with FIs but that a nontrivial portion of CBDC transactions will occur via (not-necessarily-KYCed) offline Cash$^+$ tokens.

3.3.1 Online Banking$^+$ accounts

For KYCed users transacting online, we suggested in Section 3.2.3 that the public core API should expose methods with which users can generate pseudonyms on demand. These pseudonyms would enable users to, e.g., interact with different merchants using merchant-specific pseudonyms or make all of their interactions with a given merchant fully anonymous using single-use (ephemeral) pseudonyms. Not only does this pseudonyms-on-demand approach protect privacy concerning users' interactions with merchants, but it also makes it trivial for FIs to revoke privacy when doing so is legally warranted.

We also suggested that the interbank core API expose methods for interacting with Banking$^+$ accounts based on data collected as part of KYC enforcement. These API calls will support distributed algorithms for, e.g., cross-bank fraud and anomaly detection, cross-bank AML enforcement, and proofs of solvency, among other things. Maximizing privacy and transparency necessitates that these core API methods (i) enforce strict access control policies, (ii) generate detailed audit logs for all

queries, and (iii) prescribe the use of privacy-preserving cryptographic techniques like zero-knowledge proofs, secure multiparty computation, and differential privacy wherever appropriate and feasible.

For example, an API method intended for cross-bank AML enforcement might (i) enforce access control policies that grant access only to approved regulators, (ii) produce an (immutable) audit log of each invocation on the core ledger, and (iii) leverage cryptography to answer specific questions (e.g., "yes, cumulative transactions for this individual exceed CA$10,000" or "no, cumulative transactions for this individual do not exceed CA$10,000") without revealing additional information to any entity. The outputs of such an API would constitute evidence with which the regulators might compel (perhaps with judicial oversight) the disclosure of otherwise private information. For added transparency, the core API might include methods with which the general public can request transparency reports summarizing the use of such API methods, as reflected in the audit logs on the core ledger.

3.3.2 Offline Cash$^+$ tokens

In addition to Banking$^+$ services, the CBDC ecosystem will include mechanisms through which users can withdraw, use, and deposit offline Cash$^+$ tokens—true central bank liabilities with semantics and privacy guarantees analogous to cash. Users may use Cash$^+$ tokens both for online transactions (e.g., Internet commerce) and for in-person transactions in low-connectivity environments. When the payee has Internet connectivity (e.g., Internet commerce or brick-and-mortar stores that accept chip-and-pin Interac and credit card transactions), such tokens can be deposited, cleared, and settled in real time. Thus, always-on connectivity eliminates the risk of double-spending fraud and precluding payees' need to possess specialized hardware or software to securely store Cash$^+$ tokens.

To support offline usage, we envision FIs supplying hardware and software "*wallets*" that manage the storage and use of Cash$^+$ tokens for their users. Such wallets will automate obtaining and transacting with Cash$^+$ tokens and prevent the inadvertent "double-spending" of tokens. They may employ cryptography to protect

Cash^+ tokens at rest, requiring password- or biometric-derived keys to unlock the tokens (particularly for KYCed users). Nevertheless, offline transactions come with inherent and unavoidable risks of double-spending: digital information is trivially replicable, while software and hardware safeguards are notoriously fragile when devices are in the hands of a malicious user. Therefore, we cannot expect secure wallets to provide the full breadth of security protections necessary to rule out fraud. Instead, FIs must detect and mitigate potential fraud at the interface between the Banking^+ and Cash^+ realms. Consequently, absent third-party insurance or liability protection offered as a value-added service by an FI, users who accept offline Cash^+ tokens will bear (at least part of) the risk.

The precise risk profile will depend on the semantics of the Cash^+ tokens, e.g., whether they are associated with KYCed identities, how long they can exist offline, and how many "hops" they transit before being deposited into a Banking^+ account, and so on. We use the term *hops* to reference the number of times that a given Cash^+ token changes hands before it is deposited into a Banking^+ account, an important metric owing to the fact that digital information is trivial to duplicate. To ensure that Cash^+ tokens are useful in a broad range of scenarios, we envision a CBDC ecosystem that supports a handful of distinct Cash^+ token types that offer different risk–usability tradeoffs. For example, we believe that the lifetime of both KYCed and non-KYCed Cash^+ tokens should *typically* be limited to a short time period and a single hop, so as to limit the potential for abuse. Indeed, typical FIs (who shoulder the burden of validating Cash^+ deposits) might *only* support withdrawing single-hop, short-lived tokens. They might even charge "sliding-scale" transaction fees for depositing Cash^+ tokens, with fees being commensurate to the inherent complexity of doublespending mitigation that vary depending on a given token's KYCed vs non-KYCed status, the length time since it was withdrawn, the number of hops it has since transited, and so on.

However, in the case of remote communities with sporadic Internet connectivity, the ability to exist offline for extended periods and to pass through multiple hops before being deposited might be an essential feature. Indeed, such remote, tight-knit communities may place greater emphasis on social structures and trust borne

of personal relationships to mitigate the threat of fraud. To accommodate such cases, we envision local authorities (e.g., tribal councils or municipal governments) acting as limited-capacity FIs (potentially automated via BoC-curated smart contracts), allowing their constituents to withdraw and deposit Cash^+ tokens with semantics tailored to their communities. Such tokens might not be universally accepted outside of the remote community, but would be statutorily fungible with "standard" Cash^+ tokens by any regulated FI (possibly subject to waiting periods or other abuse-mitigation requirements).

3.3.3 Trade-offs and system roll-out

Programmability of CBDC opens a plethora of opportunities that may be considered while weighing and balancing functionality, throughput, and privacy. Different types of payments will have different requirements—even basic forms and without considering advanced features such as programmable anonymity. For example, the speed of payment *clearing* for low-value transactions such as a customer's payment at checkout may matter more than how long it takes for the actual money to be delivered into the merchant's account, i.e., when the payment is *settled*. For high-valued transactions with no possibility for reversing the transaction, however, real-time settlement of payment is important, while the transaction may take more time overall.

The proposed ecosystem will provide sufficient flexibility for FIs to balance functionality versus resiliency, security and privacy for their offered service. Functionalities such as programmability of payments and privacy and anonymity of transactions, must be balanced with complexity of the system that will lead to increased number of bugs and software flaws, increased attack surface, and possibility of subverting and bypassing protection mechanisms of the system.

The roll-out of the system needs to start with simpler APIs and services with limited programmability and constraint on privacy. This will allow understanding usability, security and discovering unintended consequence of the technology.

3.3.4 Summary

Figure 3.1 illustrates the overall design of our system and shows the workings of a few important pieces. The figure is segmented vertically with four belts: the central bank at the top, the financial intermedaries below that, followed by users, and finished with Cash^+ tokens.

In Figure 3.1 (a) we see that the central bank maintains a number of geographically dispersed replicas who are responsible for the core ledger. These ledgers store transaction data involving different entities, such as FIs or the central bank itself, and communciation among the replicas maintains its consistent state.

In Figure 3.1 (b) we see that particular FIs each have their own view of the core ledger. Each entity maintains transaction data provided by the central bank's core ledger that pertains to their own positions. Different FIs thus have different views of the core ledger, but if they were amalgamated it would reflect the entirety of the core ledger. Not all transaction data must appear on the core ledger; multiple FIs may have their own inter-FI private ledger and an FI may have its own private ledger it maintains for its own purposes.

In Figure 3.1 (c) we see new transaction data being sent to the central bank. Through a well-formed API call to the Victoria replica, the leftmost chartered FI submits a payment to another entity. It first passes through a filter which decides whether legal regulations apply, in which case it is sent to the appropriate authority (in this case, a dotted line to FINTRAC).

Furthermore, the transaction being issued in Figure 3.1 (c) is greyed out in the Victoria ledger, as well as the Calgary one. This is because it has not yet replicated across sufficient replicas. In particular, the recipient of the transaction—the right-most chartered FI—has not yet seen the transaction reflected on the core ledger through its Saint John proxy.

In Figure 3.1 (d) we see the existence of a number of types of user accounts. Different FIs offer different products, including $\mathsf{Banking}^+$ as well as Cash^+ in both KYC and non-KYC varieties. Insurances, brokerages, and a wealth of other financial products

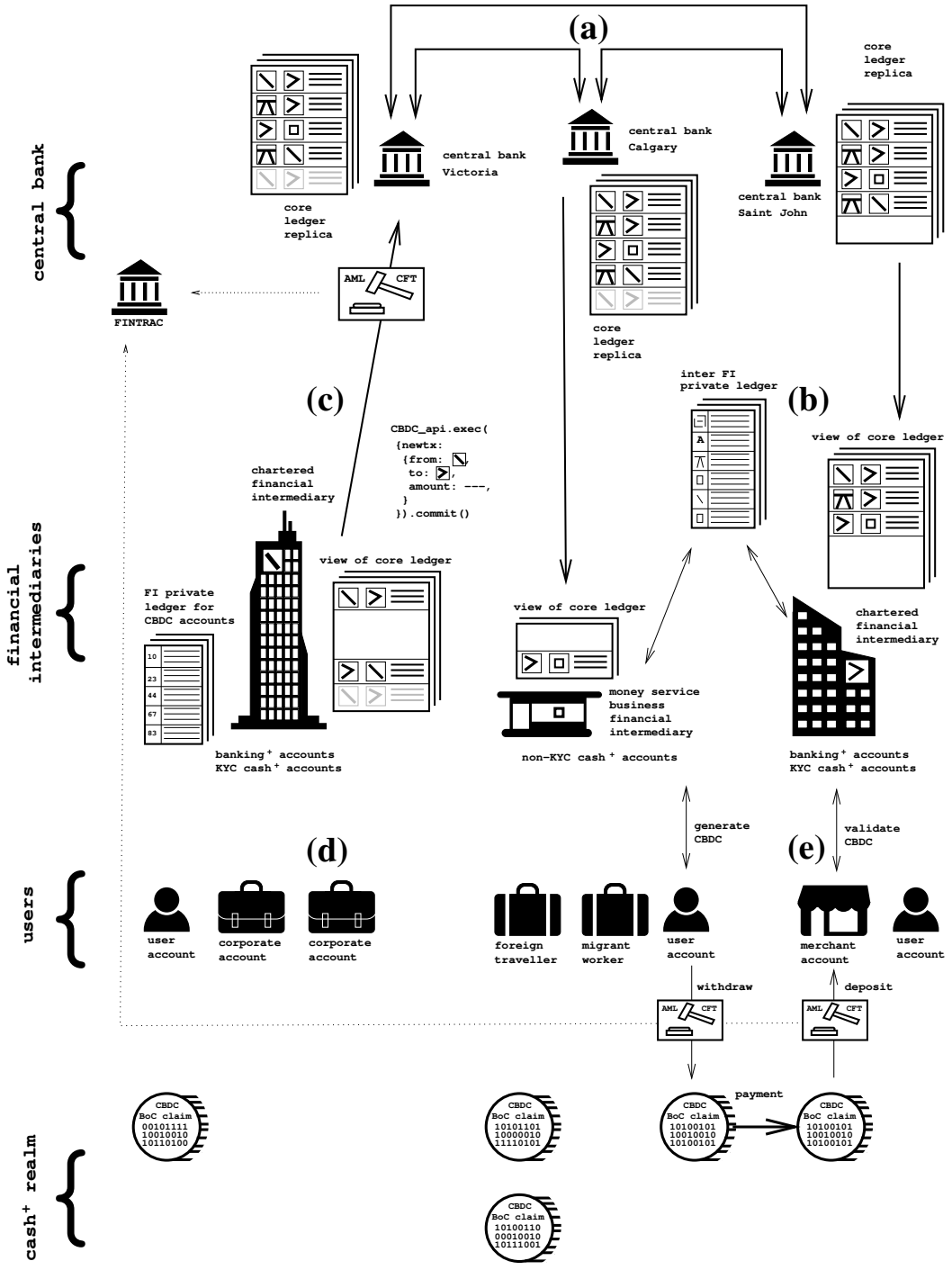

Figure 3.1: System Design illustrating (a) core ledger replicas, (b) FI's view of the core ledger, (c) updates to the core ledger through API calls, (d) users with FI-provided accounts, and (e) the creation and use of CBDC.

could also be reflected here. The users consist of actual people as well as corporate entities, merchants, and special accounts for travellers or migrants. The users can hold their assets through the FIs as reflected in ledgers or as offline CBDC holdings.

In Figure 3.1 (e) we see an example transaction in the Cash^+ realm. A user account with a non-KYC Cash^+ account with a money service business FI. The user generates a CBDC as a digital token for storage in their wallet; details for this transaction are filtered to see if legal regulations apply. After this point, the token is an anonymous digital coin held by the user; they then give it to a merchant, who in turns deposits it into their $\mathsf{Banking}^+$ account. This act of depositing also passes through a filter to determine if legal regulations apply. After this point, the merchant account validates the token (e.g., to ensure it has not priorly been double spent) with their FI account.

Our proposal for a CBDC is meant to achieve the goals stated by the Bank of Canada in published documents. These are security and privacy, universal access, resiliency and robustness, legal compliance, and performance and scalability. Further to these goals we want our CBDC to create economic value and be universally adopted. In the next chapter we present a business case that aims to satisfy these additional goals.

4 Business Case

The preceding chapter presented a high-level architecture for a hypothetical Canadian CBDC; we now focus on the "business" justification for our proposed design. Indeed, the business aspects and system architecture are inseparable—we could end up suggesting a white elephant if customers and financial intermediaries lack incentives to use such a highly advanced system.

The two most important economic concerns that drive our architecture are value creation and adoption incentives: Simply put, we measure the success of a Canadian CBDC by the extent to which it is adopted by and creates value for Canadians of all stripes. The primary source of value creation in our proposal is smart contracts that foster innovation and increase efficiency, while the primary driver for adoption by FIs is the underlying interoperable ledger technology. The design of the CBDC should also ensure that economic agents like customers, merchants, banks, and other fintech companies have incentives to participate in the new system.

The CBDC design will significantly impact money supply, liability issues, monetary policies and sovereignty, and financial system stability. Therefore, this chapter goes beyond discussing adoption incentives and concerns by further suggesting policy recommendations. Finally, many adoption incentives result from smart contracts and their universal usage in our system design; thus, we discuss the risks and challenges of using smart contracts and their necessary oversight.

4.1 Fractional-reserve banking

In the current financial system, the funds consumers hold in their bank accounts are not BoC liabilities but rather a claim on the commercial bank. When a consumer deposits a $10 bill—a BoC liability—into the checking account offered by the bank, that $10 is exchanged for bank liability. The bank can then use the deposited

funds to make loans. This notion of money creation by banks, or fractional-reserve banking, has important implications for CBDC platform design.

One option for deploying CBDC is to allow customers to hold CBDC directly in wallets hosted by banks, analogous to safe deposit boxes. This CBDC would then be "risk-free" for consumers and fully backed by the BoC. The downside of this approach is that these funds could not be invested in positive NPV (net present value) projects such as loans to businesses and, hence, this approach would hinder economic growth. Banks' balance sheets would shrink and credit supply would decrease. Banks would also have a disincentive to offer CBDC to consumers and this widespread adoption would be limited. We believe that a retail CBDC where most costumers hold CBDC directly will be a niche product with little use.

We prefer a model where, in most instances, customers do not directly own BoC liabilities. While in our setting banks are able to offer accounts where consumers can hold CBDC directly, in most cases consumers will deposit their CBDC with a bank and exchange it for bank liabilities that are not backed by the Bank of Canada, These customers own credit on the bank's ledger, similar to the process when one deposits a $10 bill in a checking account. In particular, this credit would be an entry in the bank's private ledger and *not* a liability of the BoC, just like in today's system. In our proposal the introduction of CBDC will not lead to disintermediation, i.e. the shrinkage of banks' balance sheets. The interoperability that we suggest in our platform where smart contracts can run on both CBDC and bank-created money ensures that bank-created money is as useful as CBDC is for customers.

4.2 BoC liability

Figure 4.1 illustrates how $\mathsf{Banking}^+$ and Cash^+ intersect with Bank of Canada liabilities. Tokens issued in the Cash^+ realm are clearly a central bank liability as cash is today. All Cash^+ tokens are recorded on the core ledger. The $\mathsf{Banking}^+$ realm extends over central bank generated money and over bank generated money. In most cases users will hold $\mathsf{Banking}^+$ accounts for bank generated money, i.e. they hold bank deposits like in today's system. Funds held in these accounts are not a Bank

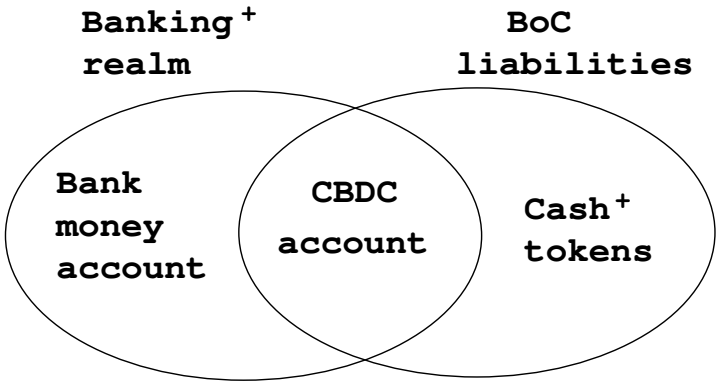

Figure 4.1: Bank of Canada liabilities in our CBDC ecosystem.

of Canada liability. The common API that extends across all of the Banking$^+$ realm ensures that users can take full advantage of the smart contract abilities. In our proposal users could also hold CBDC directly in bank issued CBDC accounts, which would also be part of the Banking$^+$ realm. CBDC held in such CBDC accounts are a Bank of Canada liability.

4.3 From Banking and Cash to *Banking*$^+$ and *Cash*$^+$

The proposed core ledger and inter-bank DLT will act as "ground truth" for all transactions involving CBDC, which is the BoC's liability. That is, by definition, an entity in our model "owns" some BoC liability if and only if the BoC-visible portion of the DLT reflects this. These liabilities will manifest as line items in a ledger, as opposed to discrete "coins" or "tokens". In some instances, customers may "withdraw" BoC liabilities (in small quantities, pursuant to FINTRAC to the Cash$^+$ realm. In such cases, their bank will "mint" an e-cash token that effectively takes said liability off-chain, reducing the issuing bank's CBDC holdings as reflected on the DLT by the appropriate amount. The BoC will know the *quantity* of "coin-based" liabilities in circulation at any given time—and will be able to verify the validity of such liabilities—but it will not necessarily learn *who holds* said liabilities. In this way, BoC remains the sole issuer of CBDC and maintains a global, universally agreed-upon view of its own liabilities, while banks can use the CBDC they hold

to finance positive NPV projects in the economy.

As an illustrative example, suppose one lost a smartphone in a deep lake when she went fishing, and this smartphone had $1,000 worth of Cash^+ CBDC stored in a private wallet. Once she proves that the cellphone is lost, she would be able to recover the lost tokens by using the transaction record identified by the interface between Cash^+ and $\mathsf{Banking}^+$. As the BoC has liability on Cash^+ realm in this way, the public will feel more secured when using CBDC than using cash. This will not only increase customer welfare, but also facilitate the CBDC adoption. Note in the example that the BoC liability does not necessarily imply that the Bank itself should help the customer to recover the lost CBDC. The wallet host can provide such a service in return for a small fee or by using insurance contracts that will be discussed in Chapter 5. The recovery may take long time until FIs' ledgers recognize the exact amount of spent tokens in the Cash^+ realm, our proposed offline transaction mechanism and the interface structure between Cash^+ and $\mathsf{Banking}^+$ can guarantee at least a partial recovery of clearly identified unspent tokens (see also the related discussion in Section 3.3.2).

4.4 Monetary sovereignty

Private money in the form of stablecoins have seen a phenomenal rise in the recent past, and it poses a competitive threat to central-bank-issued money. At the moment there are more than 25 billion USD worth of privately issued stablecoins in circulation. While this is still small, it is nen the less significant and rapidly increasing. Moreover, new stablecoins, such as Facebook's Diem, are planning to launch in the near future.

Stablecoins are typically issued in USD and a widespread adoption of such foreign denominated stablecoins in Canada would threaten Canadian monetary sovereignty. Privately issued stablecoins can increase financial fragility as they are often unregulated and it is not clear how much they are backed with real assets (e.g., Tether has more than 24 Billion USD in circulation as of January 2021, but it is unclear how much is actually backed). Were such coins to be widely used and then financially

default, it would have devastating ripple effects throughout the entire economy.

We believe that stablecoins are popular today not because because they are privately issued but because they offer functionality that does not exist in central bank or bank issued money. To offer users a viable, safe, and trustworthy alternative the CBDC or the private solutions that build on it have to offer the similar functionality as private money. Programmability of money is therefore a key aspect of our design.

4.5 Adoption

Successful adoption of a CBDC ecosystem will require widespread buying from a diverse set of stakeholders. To ensure adoption CBDC should be a Pareto improvement for the key stakeholders, such as banks, consumers, and merchants. To achieve that goal CBDC has to (i) create value that exceeds the implementation cost and (ii) provide pricing or subsidy systems in place to make everybody better off.

We see four primary sources of value creation:

(1) Reducing operational costs for banks and merchants: A system designed for CBDC can substantially reduce operational costs for banks and merchants. For example, the settlement of trades and the payment of coupons or dividends that can be implemented as smart contracts will streamline back-offices; meanwhile, banks and merchants will save the cost of transporting and handling cash, securing cash inventories, and servicing ATMs. Banks can build private sector payment solutions on top of CBDC so that CBDC is not seen as competitive threat but as an opportunity to increase efficiency. For this to work interoperability between bank generated money and Central Bank issued money is key.

(2) Fostering innovation in the finance and business sector: A CBDC will allow smart contracts to have a stable and reliable settlement instrument, which will foster innovation and grow the size of the market for financial services. A common CBDC platform that can run across all Canadian financial institutions provides interoperability in smart contracts. For example, a bond contract that

makes future payments at specific dates to the owner of the bond can run on all platforms. This way an issuer does not have to provide a different interface for bonds held by customers at different banks. Consumers can move their digital bonds from one bank to another. Common contracts that are vetted and proven to work also provide better security and legal certainty.

A CBDC platform that is universally used within the Canadian banking network opens up possibilities to interact with other ledgers for public services. For example, real estate or vehicle registries can be transacted upon electronically, which would allow, for example, to automate a real estate transaction where a land title transfers if the payment is made and vice versa. Consumers could post a damage deposit in a digital escrow account that gets governed by a smart contract.

Links with digital registries will facilitate the development of tokenization of real assets (e.g., artifacts, intellectual properties, copyrights, or real estate) with less friction and smaller transaction costs. We believe that tokenization of real assets will be more effectively performed if the corresponding smart contracts are provided within the CBDC platform, since CBDC is universally reliable; this can create greater liquidity for the individual and corporate asset management and thus provide additional incentives for financial intermediaries to participate in the CBDC platform construction. Additionally, platforms for stock and derivative exchanges can be integrated into or built on the CBDC platform, which can use smart contracts to facilitate security trading through different financial intermediaries and thus reduce costs of operating these platforms.

(3) Increasing customer base: Lower operating costs and innovation will provide opportunities for all Canadians to fully participate in the online economy, regardless of their economic status and creditworthiness. The programmability of the CBDC platform opens up possibilities to include previously unbanked populations via public services such as benefits payments of targeted social subsidies that can only be spent at certain locations (e.g. grocery stores).

(4) Reducing operational risk for banks: The secure ledger technologies un-

derlying CBDC can reduce operational risk for banks and merchants including, for example, settlement risk or fraudulent payments. The resulting reductions in fraud and money laundering activities would increase confidence in the Canadian dollar, deprive criminal organizations of important revenue streams, and ultimately reduce costs for consumers, banks, and merchants.

We believe that the economic benefits outlined above are greater than the costs of implementation of the CBDC platform. Attention must be paid in the implementation phase that pricing structures and regulations emerge that allow each individual stakeholder to benefit from the system.

While there are great incentives for the CBDC adoption described above, we are also aware that a CBDC platform will change the competitive landscape in the financial service industry. One concern is that there can be new opportunities for large financial institutions to collude for exercising oligopoly power. In particular, a CBDC adoption and its built-in infrastructure will help a group of financial institutions to set up a separate DL (distributed ledger) independent of the DL commonly shared by all the chartered banks with almost no cost. Smart contracts on such a DL cannot be run by customers of other banks or small and local credit unions. In this way, large financial institutions can increase their oligopoly power. Therefore, we think that policy makers need to ensure interoperability across banks.

4.6 Financial stability: Liquidity (bank runs), lending, and interest

While an introduction of CBDC provides greater liquidity in the economy, this can raise an concern that a possibility of bank run may increase. For example, suppose that a majority of bank customers all rapidly withdraw their bank deposits and convert them to CBDC in response to some bad news related to the bank. Such a rapid withdrawal of funding can cause the bank to collapse. In today's banking system there are physical frictions and costs that alleviate the possibility of a bank run; such frictions and costs for a CBDC are less likely exist. Nevertheless, the risk can be mitigated under similar policies that we have in our current system. For

example, customers are not able to withdraw more than a certain amount of CBDCs within several business days. This type of a forced time lag for a large withdrawal can prevent a bank run as the central bank will have a proper time to help the bank and its customers by using existing macro-prudential policies. FIs also need to consider business models that can disincentivize customers to withdraw a large amount of money.

CBDC is easier for an individual to hold than cash; there is, for example, no need to prepare a large and secure vault to save a billion CBDCs, and the costs to securely store offline CBDC do not scale with the total amount. Widespread offline holding, however, would shrink banks' balance sheets and thus reduce the amount banks can lend out. Less credit would hinder economic growth as lending for positive NPV projects becomes harder for FIs (see Section 4.1). Therefore, we suggest that there should be disincentives for individuals to hold CBDC outside of a bank account. For example, a customer holding CBDCs in their wallet will not earn interest or need to pay extra fees (increasing with the amount in the wallet) to a host bank as a service charge for Cash^+ transactions through a personal wallet. A short-term personal holding of CBDCs can be free, but the service charge can be larger as the holding period is longer (see also the related discussion in Section 3.3.2). The central bank also considers to set zero or negative interest on individual CBDC holdings (not the reserve of banks) with a certain limit. Finally, the suggested disincentive policies should be greatly relaxed or removed for the unbanked such as customers in remote communities and the poor.

4.7 Smart contracts: Challenges

The (voluntary) adoption of the proposed design largely requires support for smart contracts and the provision of BoC-issued CBDC for their settlement. Smart contracts are trusted programs that obviate trusted mediators and automate processes involving payments among multiple parties. They can be seen as an extension of conditional payments, with an enriched set of conditions and potentially taking inputs from multiple parties spanning multiple banks. We recognize the complexity

of realizing nontrivial contracts at multiple levels (technological, legal, usability); despite that, providing a platform for such contracts with built-in support for financial settlement in CBDC will spur innovation and will result in rethinking and redesigning many processes in future.

From a technical perspective, smart contracts are not essential and their basic functionality can be realized without them. We believe, however, that smart contracts will create the economic benefits that outweigh adoption costs and incentivize implementation. Not supporting smart contracts would be a major loss of various opportunities and incentives for financial intermediaries and merchants. As noted earlier, smart contracts are conditional payments with complex payment conditions and multiple actors. CBDC enables such complex payment systems to be introduced and offers a platform to settle the resulting financial obligations. We envisage smart contracts for less complex conditions to be introduced at first, with more elaborate contracts being rolled out as the knowledge and experience of using them grows.

While automation by smart contracts using blockchain technologies has been extensively discussed as an attractive feature for the business sector, real-world adoption is currently low and is likely to remain so in the near future. Some reasons for the slow adoption are:

- high overhead costs associated with creating separate DLTs for each independent purpose among a small number of interested entities
- the absence of a trusted party such as BoC in the ecosystem
- the lack of legal enforcement (or ambiguity of its responsibility) when operating smart contracts
- the difficulty of understanding what a smart contract does, which leads to low trust in it
- the lack of a reliable currency to denominate obligations.

We expect that these problems will easily be resolved in the proposed CBDC-driven banking and financial system. Thus, we highlight smart contracts not as a require-

ment for its functioning but rather as a further motivation for its adoption in the finance and commercial sectors.

4.8 Smart contracts: Oversight and regulations

Regarding legal oversight we see smart contracts as a component functioning within a greater legal framework. Our image is that legal contracts will be prepared traditionally, by human lawyers from both parties establishing a meeting of the minds. Smart contracts will simply represent a *bona fide* effort to translate the natural language description of a legal obligation into a corresponding computer program. When operating correctly, this will remove a great deal of existing human effort involved in managing what may be considered ordinary contract-protected economic activity.

Despite that, the use of smart contracts presents some risk of an error in implementation (e.g., programming bug) or may otherwise produce results that are disputed by one of the parties involved. Straightforward errors may be easily fixed if there is a consensus among all parties. Judicial oversight may be necessary otherwise. In this case, the contract written by human lawyers stands as testament to the actual intended behaviour of the smart contract, and an appropriate ruling can be made.

Note that the need for human lawyers and judges decreases with time for issues of pure programming error with regards to smart contracts. We picture the first smart contracts to be used for straightforward financial transactions: interest, bond coupons, security deposits for rent or office keys. If errors are discovered in how these smart contracts are implemented, they will be fixed and thus future uses of these contracts are not affected by these earlier errors. Long-lived and widely used smart contracts may serve as basic building blocks for more complicated contracts and a curated selection may be afforded some notion of *prima facie* for a contract dispute.

Introducing CBDC will be a gradual process, starting with stringent requirements on wallet providers and strict oversight on smart contracts. These are new technologies and their introduction could lead to unexpected usages and pattern of

behaviour that needs to be understood. Gradual introduction of these technologies will provide sufficient time to introduce the legal and liability frameworks that are required in the case of dispute.

We are hesitant to propose specific policy regulations to govern wallets and smart contracts. We envision a consortium DLT that is only directly accessed by the licensed financial intermediaries; thus, only these intermediaries would have the ability to directly run smart contracts. This enables a "wall-garden" approach similar to Google Play or the App Store, but without the potential for end users to circumvent the protections.[1] Like contracts, smart contracts exhibit privity that prevents one from running a contract that can, e.g., withdraw funds from somebody else's account without the express consent (indeed, participation) of that party; thus, with a wall-garden approach banks could reasonably restrict clients to running "vetted" smart contracts and (be required to) assume liability in the event of failure, much as they do with credit card transactions or interac e-transfers today.

In the business realm, corporations may wish to run custom smart contracts. This could be facilitated by banks (wallet hosts). Special-purpose IT or fintech intermediary firms could be licensed to support such endeavours by the BoC or the government. The risks and due diligence may be assumed by the corporation that deploys custom smart contracts; privity is again important here. In this case, an industry providing insurance contracts against such risks might emerge to mitigate risks and thus encourage innovation.

4.9 Cross-chain interoperability

Design of CBDC should be made with future interoperability with other ledger systems in mind. For example a DLT might administer tokenized stocks. The CBDC should be designed to allow for atomic swaps, where stock tokens can be exchanged for payment in CBDC in an atomic transaction. Another example would be the exchange of a title in a land registry against payment in CBDC. One way to implement such cross chain swaps would be through regulated, trusted entities.

[1] See Section 3.2.4 for the design aspects and the related discussion on the wall-garden approach.

A government regulated clearing house could, for example, perform the atomic swap of stock tokens for CBDC. While the process structure is similar to today's settlement it could be implemented in smart contracts and thus reduce settlement failures and be implemented more efficiently. Similarly smart contracts governing land title transfer could be implemented to automate tax payments and reporting requirements.

5 Meeting Design Goals

In this chapter, we revisit the design goals from Chapter 2 and highlight properties and features of our proposed design that help meet these goals.

5.1 Security and privacy

The proposed system's security and privacy guarantees stem from its modular and layered architecture, featuring components tailored toward supporting advanced cryptographic and privacy-enhancing technologies. For instance, native support for on-demand pseudonyms provides users with the flexibility to choose between "fully identified", "linkably anonymous", or "unlinkably anonymous" Banking$^+$ transactions, all the while respecting the compliance and oversight obligations of the FIs. Meanwhile, support for "fully anonymous" offline Cash$^+$ tokens provides a means for even stronger, cash-like anonymity, albeit with restrictions to mitigate fraud and AML/CFT circumvention risks. Indeed, by exposing suitable privacy- and oversight-centric methods in the core API, our design simultaneously expands the potential scope of policy-enforcement mechanisms while bolstering well-behaved CBDC users' privacy posture.

A DLT backend for the core ledger ensures high availability and integrity for transaction data against both transient failures and adversarial tampering; it also provides a precise notion of *consistency*, allowing stakeholders to establish consensus around relevant parts of the financial systems' state. The ability to establish consensus eliminates the potential for many kinds of disputes borne of information asymmetry, enabling the secure realization of programmable money and real-time settlement for smart contracts. Coupled with core API functionality, the immutability of DLT entries also ensures robust and trustworthy accountability mechanisms for law enforcement and oversight bodies, ensuring that lawful access to user data

happens in a manner transparent to policymakers and the general public.

The compartmentalization of transaction data via segregated ledgers that interact exclusively through well-defined APIs limits the scale of potential data breaches. It also facilitates the implementation of misbehaviour-detection mechanisms that disclose only the minimum amount of privacy-sensitive information necessary for effective operation. Simultaneously, having each segregated ledger replicate subsets of the core ledger provides strong robustness to temporary connectivity loss and resilience to systemic failures at the core ledger.

Offline Cash^+ tokens represent a potential weak point in the security of CBDC; however, the risks posed by offline transactions seem inherent and unavoidable for any digital currency that supports offline transactions. We propose several safeguards—including restricting most offline transactions to a single-hop, discouraging users from holding Cash^+ tokens offline for extended periods, and ensuring that non-KYCed tokens are distinguishable from KYCed tokens—to mitigate these risks. These safeguards ensure that payees can make well-informed risk assessments in deciding whether to accept offline Cash^+ tokens. Additionally, we suggest using specialized software and tamper-resistant hardware to prevent accidental double-spending and render most intentional abuse prohibitively challenging to perform at scale. In any case, we expect that the merchants in most retail Cash^+ transactions will have Internet connectivity, allowing real-time settlement that ensures such threats cannot materialize.

5.2 Universal access

A central bank currency must be accessible to all—residents and visitors alike. In the context of a CBDC, *access* refers to the ability to (i) purchase and hold CBDC in a $\mathsf{Banking}^+$ account or as Cash^+ tokens in a secure wallet; and (ii) spend those CBDC holdings at will. In most cases, CBDC users will undergo KYC identity verification with an FI and use CBDC via an Internet-connected mobile device; however, there exist legitimate exceptions. For access to be *universal*, the ability to use CBDC must extend to, e.g., remote communities with limited access to the

Internet and to individuals unable (or unwilling) to be undergo KYC verification.

The primary concern for dealing with offline transactions is the necessity to record all transactions involving central bank liabilities on the core ledger: While "wallet-to-wallet" payments can *provisionally* clear offline, true finalization requires connectivity. Accepting Cash^+ payments without connectivity exposes the payee to the unavoidable risk of fraud (due to double spending); however, absent software faults, such double-spending fraud is an *intentional* misuse of the system made technically challenging via software and hardware safeguards. Because double-spending detection will ultimately deanonymize any (KYCed) users who attempt this sort of fraud, we argue that these risks are often manageable, especially in tight-knit communities. For instance, (i) payees can leverage trust relationships to make informed decisions about whether to accept Cash^+ tokens from a specific community member and (ii) social pressures may provide disincentives to being implicated in fraud against other community members.

In Chapter 3, we suggested restricting most Cash^+ transactions to a single hop so that they can provide cash-like anonymity while ensuring that double-spending detection mechanisms can effectively hold fraudsters accountable for abuse. However, we acknowledge that in remote communities where connectivity is a luxury, it may help relax this constraint, e.g., by allowing payers to re-spend Cash^+ tokens non-anonymously via high-assurance hardware wallets that can securely attest to their identity. Conversely, offline use of non-KYCed Cash^+ tokens should be universally discouraged and prohibitions against multi-hop usage enforced by default on CBDC software and hardware wallets. One implication is that universal access will require universal access to low-cost (possibly subsidized) CBDC-aware hardware wallets that securely store and transact with offline Cash^+ tokens while automatically enforcing user- and FI-selected policies (regarding, e.g., things like accepting KYCed versus non-KYCed token without online verification, accepting multi-hop tokens from acquaintances, and so on).

Despite technological and legal controls intended to ensure the CBDC ecosystem's safety, there remain fundamental differences between CBDC and physical banknotes; indeed, these very differences are what make possible innovative CBDC-

backed products and services. It will be imperative to educate Canadians about both the risks and opportunities of CBDC to inspire confidence among and avoid harm to CBDC users.

5.3 Resiliency and robustness

Canada's finance system is a critical infrastructure with extreme availability demands. To ensure 24/7-accessibility, we have proposed a DLT backend for the core ledger with nodes geographically distributed across the nation. Beyond the core ledger, our architecture features a high degree of decentralization through segregated FI ledgers and offline Cash^+ tokens that can operate "autonomously"—albeit in limited form.

This decentralization is a primary source of robustness and resilience for the CBDC ecosystem. For example, having FIs' ledgers contain verifiable replicas of relevant core-ledger entries (coupled with clear policies and procedures) facilitates uninterrupted operations if there are network partitioning and recovery if the core ledger fails. It also ensures that remote communities without reliable Internet connectivity can use CBDC by means analogous to those available to major FIs in the event of failure.

The use of secure hardware wallets for offline Cash^+ tokens provides opportunities to manage offline CBDC holds securely and flexibly. For example, being manifestations of *digital* currency, the offline Cash^+ tokens in a secure wallet could be stored in escrow to allow for their recovery under specific, well-defined scenarios. In this way, CBDC provides notions of robustness for users that have no parallels with physical banknotes.

5.4 Legal Compliance

Our proposed design's key feature is its native support for advanced cryptographic and privacy-enhancing technologies that facilitate robust enforcement of laws and regulations (e.g., AML and CFT) without compromising privacy. For example, the

use of on-demand pseudonyms for private Banking$^+$ transactions simplifies lawful access compared with competing options employed in privacy-centric money; the inclusion of PET-aware API calls enables inter-FI fraud and abuse detection without the unnecessary disclosure of private information.

By restricting most Cash$^+$ tokens to single-hop transactions and enforcing legal requirements at the interface between Cash$^+$ and Banking$^+$, our design extends the range of enforcement options compared with traditional cash. Moreover, by clearly distinguishing between KYCed versus non-KYCed Cash$^+$ tokens, it can seamlessly enforce policies and restrictions tailored to different kinds of uses.

5.5 Performance and scalability

There are many ways to define and quantify performance and scalability. Important metrics for performance of a transaction system include transaction throughput (i.e., the *rate* at which the system clears transactions) and latency (i.e., the *delay* before transactions can clear). The decentralized nature of our design facilitates high throughput by enabling FIs to (i) clear and settle many transactions internally and (ii) employ netted settlement for inter-FI transactions. This contrasts with designs in which all users hold CBDC accounts directly on the central bank's core ledger, thereby concentrating all transaction processing to a single subsystem. Our choice of privacy mechanism for Banking$^+$ transactions ensures that CBDC users can enjoy high levels of privacy without imposing prohibitively high computation cost on the FIs.

Design of the Core DLT and its communication with FI's DLTs through APIs and using dedicated high speed communication infrastructure will be crucial in achieving the required performance.

The system scalability in general refers to the ability of the system to respond gracefully to the increased demand, and can be defined with respect to different criteria and measures. Important scalability criteria for our system are outlined below.

- *FI scalability* refers to the ability of the system to enrol new FIs seamlessly and without any interruption to the working of the system. Using well defined and well-resourced APIs, and secure identity management system allows that once an FI is approved by the BoC, its operation be integrated into the system without significant affect on other parts of the system
- *Transaction scalability* refers to the ability of the system to maintain its performance with the increase in the number, speed, and variety of transactions. Our decentralized design allows transactions to remain "local" when possible, and effectively distributes the load of the system to the "edge" of the system. FIs frequent interaction with the Core ledger and regular (high frequency) updates ensure consistent global views of all FIs. More complex transactions (e.g. smart contracts) will require maintaining consistent state across multiple FIs and lead to higher coordination and synchronization load on the Core ledger. As the number of such transactions grows, additional computation and communication capacity must be planned for the Core ledger.
- *User scalability* refers to the ability of the system to serve growing number of users. End users join the system primarily through one or more FIs, or in the case of non-KYC users, through third party identity providers. In all cases because of the variety of revenue generating services that can be designed based on CBDC, there is significant incentive for FIs and service providers to expand their computation and communication infrastructure (e.g. local DLT and APIs) to support new users. The effect of such increase will be increased load on the Core ledger and its API and the need to ramping up the infrastructure in line with the growing demand.

In all cases the decentralized design and well-defined interfaces (APIs) allow planned ramp-up of the computation and communication infrastructure to respond to the increased demand on the system.

6 Concluding Remarks

The invention of money created huge economic gains in human history. We are now at a similar inflection point where the invention of programmable money and smart contracts have enormous economic potential. A well-designed CBDC will provide the infrastructure to facilitate this transition to a "smart economy", which will create new ways of financing and risk sharing in the economy and smart contracts that will govern the interactions of economic agents.

In this work we provide our proposal for a CBDC designed to facilitate that transition and provide the infrastructure to accompany the upcoming transition and secure economic prosperity for all Canadians. Our goal is to provide the strongest possible notion of privacy inspired by today's cash, still supporting our national and international obligations regarding financial tracking. It is designed with universal access as a core requirement because it is crucial that no one is left behind in a transition towards a smart economy.

CBDC technologies, policies, and regulations form a complex ecosystem that is expected to evolve as user participation grows and new financial services are developed. The range and complexity of fraud and and misuses can increase at the same time. We note that international collaboration will be strongly required since the interoperability with other CBDCs, and possible interaction with other cryptocurrencies and tokenized systems, will raise many multifaceted challenges.

Acknowledgements

his proposal has been in response to Bank of Canada Model X Challenge [7]. We would like to thank the staff at Bank of Canada for their support and guidance.

Bibliography

[1] Raphael Auer, Giulio Cornelli, and Jon Frost. Rise of the central bank digital currencies: Drivers, approaches and technologies. Bank of International Settlements Working Papers No 880, August 2020.

[2] Patrick Cain. Will your cannabis credit card purchases be visible to U.S. border officials? (Some might, some won't.). In *Global News*. September 2018. [Online; accessed 2020-12-30].

[3] Sriram Darbha and Rakesh Arora. Privacy in CBDC technology. Bank of Canada Staff Analytical Note 2020-9 (English), June 2020.

[4] Electronic Frontier Foundation. First Unitarian Church of Los Angeles v. NSA. September 2013. [Online; accessed 2020-12-30].

[5] Rodney J. Garratt and Maarten R. C. van Oordt. Privacy as a public good: A case for electronic cash. Bank of Canada Staff Working Paper/Document de travail du personnel 2019-24, July 2019.

[6] John Miedema, Cyrus Minwalla, Martine Warren, and Dinesh Shah. Designing a CBDC for universal access. Bank of Canada Staff Analytical Note 2020-10 (English), June 2020.

[7] Bank of Canada. Bank of Canada announcement, February 2021. [Online; accessed 2021-02-10].

[8] Dinesh Shah, Rakesh Arora, Han Du, Sriram Darbha, John Miedema, and Cyrus Minwalla. Technology approach for a CBDC. Bank of Canada Staff Analytical Note 2020-6 (English), February 2020.

[9] Observer Staff. Card declined: Visa, MasterCard refuse Wikileaks donations. In *Observer*. December 2010. [Online; accessed 2020-12-30].

About the Authors

Kyoung Jin (KJ) Choi is an Associate Professor of Finance at the University of Calgary's Haskayne School of Business. His research focuses on household finance, macroeconomic impacts of consumer behaviours, consumption heterogeneity and asset returns, and fintech. Recently KJ has investigated mechanism design problems of decentralized platforms using blockchain and their welfare implications.

Ryan Henry is an Assistant Professor of Computer Science at the University of Calgary. His research explores the systems challenges of applied cryptography, emphasizing ways to use cryptography to build systems that offer strong privacy protections for their users. Ryan holds or has held several competitive research grants in cryptography, information security, and privacy, notably including a joint US–Israeli grant to support the development of scalable and private blockchain technologies.

Alfred Lehar is an Associate Professor of Finance at the University of Calgary's Haskayne School of Business. His research focuses on systemic risk, financial stability, and fintech. Using network models Alfred has analyzed how macroeconomic shocks can spread through inter-bank connections and cause contagion. In his work on fintech he analyzes international Bitcoin price differences, excessive fees and miner collusion in the Bitcoin network, and decentralized exchanges and lending in the Ethereum network.

Joel Reardon is an Assistant Professor of Computer Science and Parex Innovations Fellow at the University of Calgary. He is also a co-founder of Appcensus, Inc., which provides privacy analytics as a service in the mobile world. He studies systems security at all software layers, and has particular interest in mobile security and privacy, tools for privacy compliance, and secure storage.

Reihaneh Safavi-Naini is a Professor of Computer Science, and NSERC/Telus Industrial Research Chair and Alberta Innovate Strategic Chair in Information Security at the University of Calgary. Her current research interests are cryptography and its application to information security, information theoretic and quantum-safe cryptography, secure distributed and decentralised systems, and smart contracts and their applications.