Best Before? Expiring Central Bank Digital Currency and Loss Recovery[1]

Charles M. Kahn[a,c] Maarten R.C. van Oordt[b] Yu Zhu[c]

[a]University of Illinois

[b]VU Amsterdam

[c]Bank of Canada

Crypto Asset Lab Conference

[1]Views expressed do not necessarily reflect official positions of the Bank of Canada.

Introduction

An important advantage of physical cash: Payment can be made when internet is down.

- Remote locations
- Natural disasters
- Cyberattacks or technical failures
- Temporary lack of connectivity

Want similar offline capability in electronic cash substitute. Argues for device based storage.

The Double-Spending Problem

Why not store a backup of the money?

- Customer will want to spend his offline balances, claim his device was lost, and go back to reuse his online balance.
- Ruling out double-spending requires
  - storing balances uniquely in (tamper-resistant) device, and
  - separation of funds that may be spent with device

Consequence: Loss of device implies loss of funds...

Loss recovery to reduce the risk

- Can we reduce the cost of losses in case of a digital cash substitute?
- **This paper:** Yes, we can do so seamlessly with an expiry date
- Automatically reimburse consumers for expired offline balances
- Some interesting economic questions:
  - Information sharing between devices and the central bank?
  - How to optimally set the expiry date?

Summary of results

- Loss recovery based on introducing an expiry date could have a substantial positive impact on consumer demand for offline digital currency balances.
- More information-sharing between consumers and the central bank can improve loss recovery but has an ambiguous impact on social welfare and may actually reduce it.
- The cost of setting a longer than optimal expiry date is small; setting an expiry date that is too short has a large negative impact.

Small model

Goal: Illustrate trade-offs of expiry date in an outage event.

Cash: ("offline money") a bearer instrument that can be used for offline payments

- e.g., stored-value in a payment card or smartphone chip

Cash allows for payments during outages, but is subject to losses.

Timeline: $t = 0$

At $t = 0$, the consumer decides how much cash to hold

- Online balances pay interest i but offline ones do not

A random preference shock realized:

- Consumer may want to consume 1 or 2 units

Timeline: $t = 1$

Two independent random shocks realized

- An outage disrupting network connection may occur
- Consumer may loses offline money.

The consumer buys the good from the producer

- Use online deposit if no outage, only offline cash if outage
- Consumption bounded by balances

Consumer can deposit the offline cash back if no outage

Timeline: $t = 2, 3$

At $t = 2$:

- Outage ends if there is one
- Producer may lose offline cash with probability η
- withdraw/deposit cash and online payments arrive

At $t = 3$, everybody enjoys counting their money

No expiry date (physical cash)

Cash holdings

Hold cash to purchase 1 or 2 units if the benefit exceeds the cost.

- Benefit comes from consumption in the outage
- Cost includes forgone interest and costs from a loss

Bring enough for the second unit is more demanding

- Only with some probability one wants to consume 2

Social welfare (expected # units consumed per consumer)

Cash expires quickly (shelf life: 1 period)

Offline cash expires in period 2 before producer can deposit

- Automatically reimburse to the consumer

Producers reject cash and no transactions occur during outages...

Social welfare (expected # units sold per consumer)

- Same as no-cash

High privacy and slow expiration (shelf life: 2 periods)

Acceptance: All offers as if there is no expiration date.

Cash holdings:
May hold more cash because the cost of loss is reduced

- One can get the money back but with some delay

Social welfare improves under certain parameters

Low privacy and slow expiration (shelf life: 2 periods)

Consumer's device reveals where he spends the money

After an outage, would consumers be willing to reconnect?

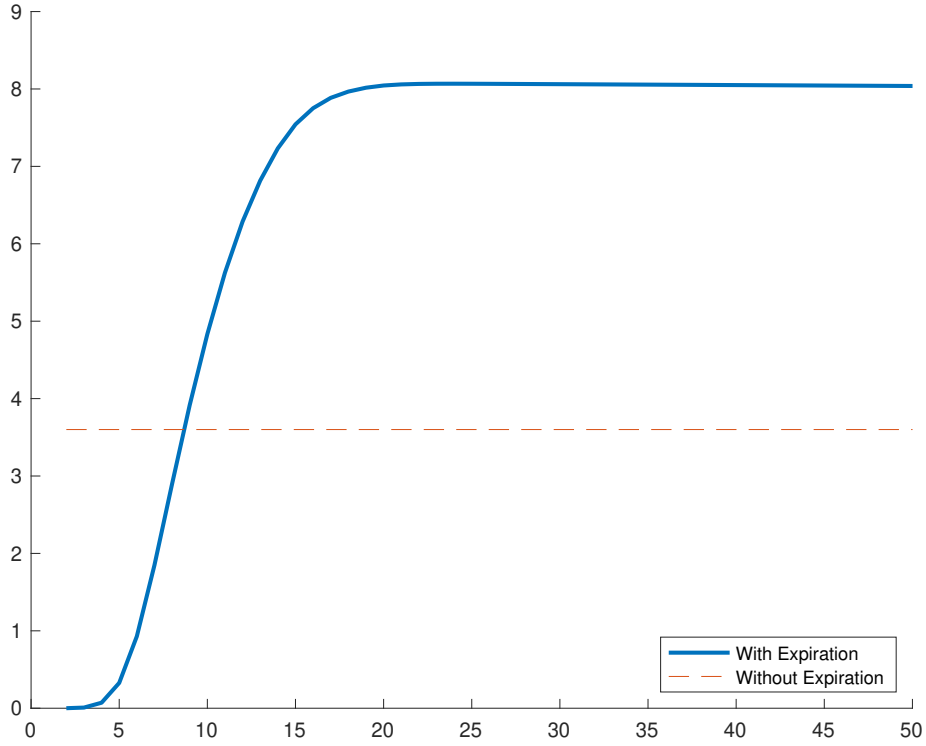
- Consumers who spent all offline cash do not reconnect
- Consumers who have unspent cash reconnect iff $i \geq \eta$.

Two situations:

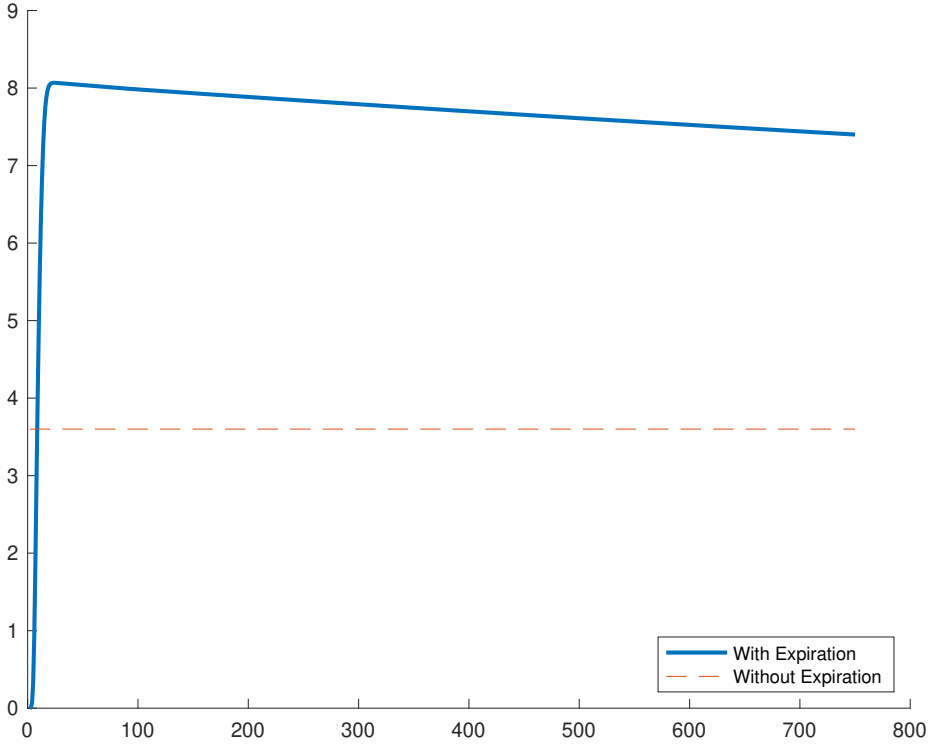
- If $i \geq \eta$, some producers charge lower "cash" prices because of reimbursement for cash losses: *may improve social welfare*
- If $i < \eta$, increase in cost of precautionary cash holdings... *reduce social welfare*

Cash holdings with expiry date and privacy

Shorter expiration dates (0-50 days)

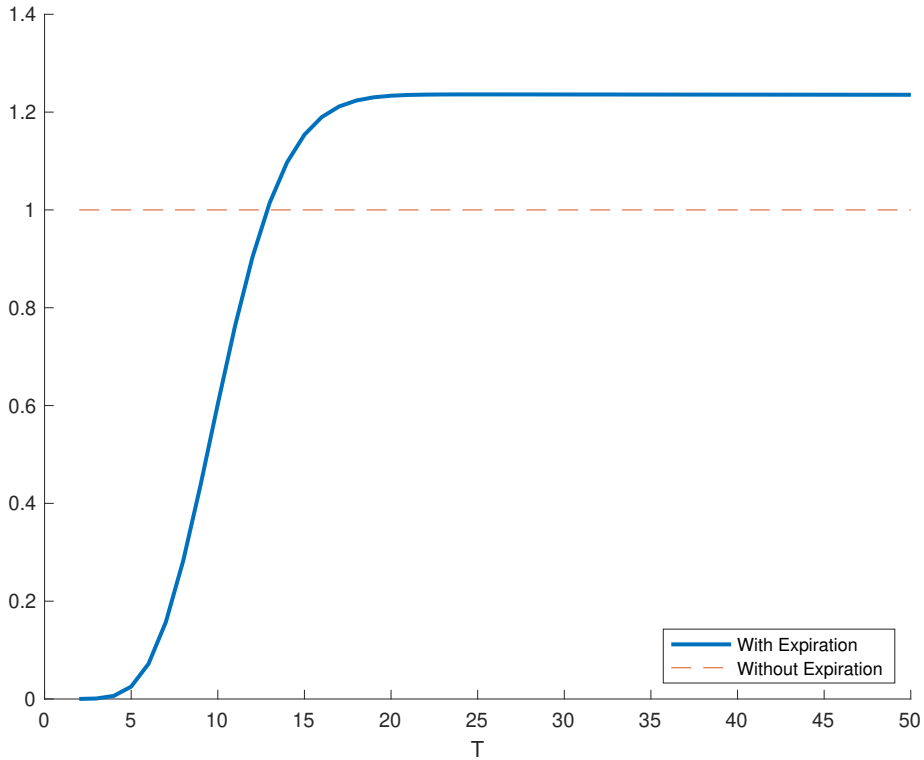


Longer expiration dates (0-750 days)

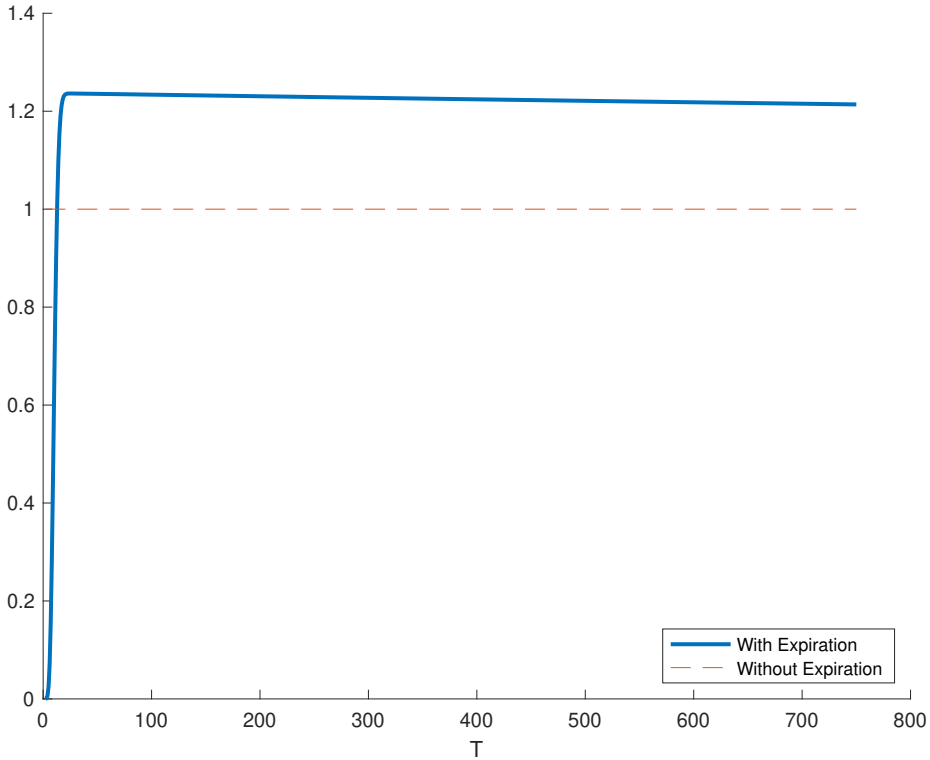


Consumer welfare with expiry date and privacy

Shorter expiration dates (0-50 days)



Longer expiration dates (0-750 days)



Concluding remarks

- Loss recovery based on introducing an expiry date could have a substantial positive impact on consumer demand for offline digital currency balances.
- The cost of setting a longer than optimal expiry date is small; setting an expiry date that is too short has a large negative impact.
- More information sharing between consumers and the central bank can improve loss recovery but has an ambiguous impact on social welfare.