BANK OF CANADA
BANQUE DU CANADA

# Accounts, Tokens and E-money


Charles M. Kahn
University of Illinois Urbana-Champaign

Francisco Rivadeneyra
Bank of Canada

Russell Wong
Richmond Fed


The views expressed here are those of the authors and do not reflect those of the Bank of Canada of the Federal Reserve System.

LSE Conference on Technology in Finance, Law and Regulation
May 16, 2019

## Payments arrangements as record-keeping systems

Two types of arrangements distinguished by identification requirements:

- **Account-based:** is the *individual* the owner of the account
- **Token-based:** is the *object* real or counterfeit

Helps understand the risk and efficiency tradeoffs:

- What is the cost of identifying and individual/object in a transaction?
- Who has access to the records? For safety and privacy issues
- Who bears cost of protection against malfeasance?
- Who bears liability in event of malfeasance?

# Relevance of the account v. token distinction

## For traditional payments:

- Not a perfect distinction (e.g. Swiss Bank Accounts)
- Still useful: institutional norms are built around this distinction
  - Difference in responsibility of bank for protecting holder of bank note and holder of bank account
  - Price v. Neal 1762, drawee pays forged bill at his peril

## For digital currencies:

- New technologies blur the distinctions
- But institutional norms still active
- So better understanding is crucial for establishing new norms and crafting policy response

# Should the Central Bank Issue E-money?

# E-money: should central banks issue a *new* form of e-money?

Central banks offer some payments media: high value payments systems (restricted access) and cash (universal access)

- **Have the new technologies like DLT and mobile computing changed the risk and efficiency tradeoff in the public provision of centralized and decentralized payments media?**

# Tradeoffs: costs, risks and privacy

Account-based systems track **individuals**

- Cost structure: issuer verifies identities, monitors behaviour and handles collateral. Liability usually lies on the issuer/operator
- Users relinquish some degree of anonymity

Token-based systems track the history of **objects**

- Verification of cash is bilateral; Bitcoin is distributed
- Cost structure: issuer cares about the cost of counterfeiting tokens more than the cost of verification of transactions

# Central bank e-money schemes

1. Account-based scheme: universal accounts at the central bank
2. Token-based schemes
   - Decentralized verification: like the FedCoin proposal
   - Centralized verification: transactions verified by the central bank
   - Delegated schemes: via custodians and intermediaries, like narrow banks

# Central bank e-money: account-based scheme

- Proposal: universal account at the central bank
- Requires: i) account opening; ii) processing of transactions; and iii) management of relationships with the public
- Central banks do not have the comparative advantage in any of these functions
  - Would compete directly with commercial bank deposits
  - Would require dealing frequently with the public

# Central bank e-money: token with decentralized verification

- Proposal: develop/choose tech to issue, store and transfer tokens using a decentralized ledger of tokens
- Requires: i) decentralized token verification tech; ii) underwrite safety of the system
- Example: CADcoin, Fedcoin
- Challenges:
  - Why use decentralized verification when we already have a trusted central party?

# Central bank e-money: token with centralized verification

- Proposal: develop/choose tech to issue, store and transfer tokens using a centralized ledger of tokens
- Requires: i) token verification tech; ii) underwrite safety of the system
- Example: ‘digital cash’ sacrificing some anonymity, speed or safety
- Challenges:
  - Can we develop or choose the appropriate technology?
  - Counterfeiting risk (cyber) in digital is potentially catastrophic

# Central bank e-money: delegated token scheme

- Proposal: delegate management of tokens to special set of institutions. Like “deposited currency schemes” or narrow banks
- Requires: i) institution supervision; ii) technology to prevent individuals from holding central bank tokens directly
- Accounts would necessarily emerge: need to identify owners of tokens
- Challenges:
  - Would current intermediaries have incentives to distribute tokens?
  - For institutions tokens could be inferior to reserves

# Conclusions

- New technologies have not changed the tradeoff for the universal provision of **central bank accounts**
  - System would be expensive
  - Directly compete with commercial banks
- New technologies have potentially improved the tradeoff for the issuance of **digital tokens**
  - Likely increase in the contestability of payments platforms
  - Questions remain on counterfeiting risks (cyber)

# Eggs in One Basket: Security and Convenience of Digital Currencies

# Accounts v. Tokens: relevance for the design of a CBDC

- An ecosystem with public and private solutions is likely to emerge
  - What are the risks of anonymous accounts?
  - How are risks shared between users and suppliers?
  - Are there externalities that should be addressed?
- Should specific security protocols be mandated?
  - For example: length of passwords, how frequently they should be changed, address reuse, two-factor authentication, etc.
- Should liability rules be re-examined?

# Ultimate Issue: choosing level of aggregation

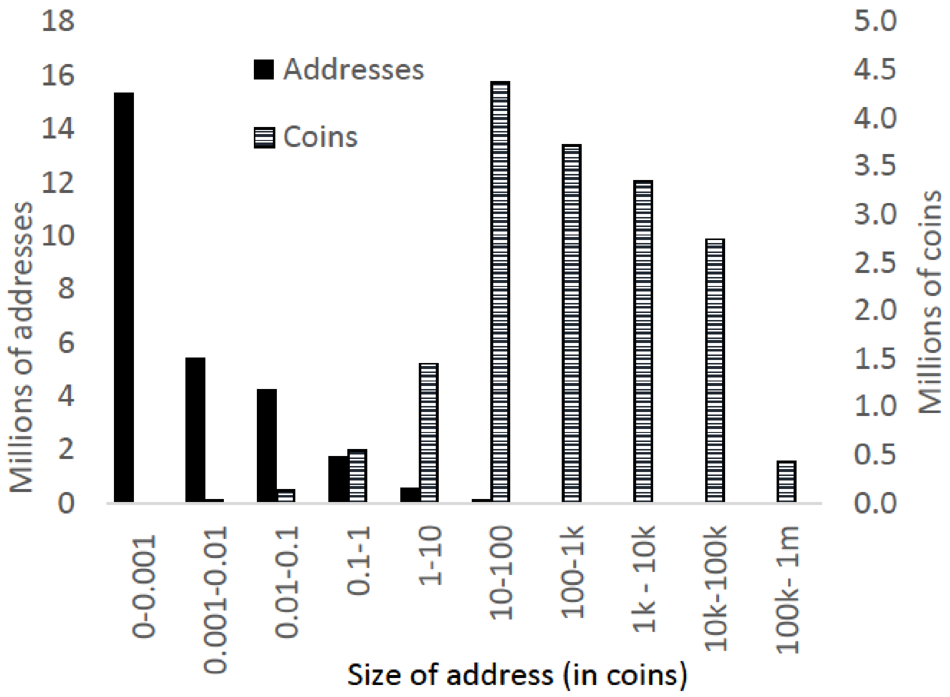
- Tokens are like "mini-accounts," each segregated from the next
- For convenience customers prefer some aggregation into accounts ("wallets" or "purses")
- Fundamental tradeoff for customer: convenience vs safety

Behold, the fool saith, "Put not all thine eggs in the one basket" … but the wise man saith, "Put all your eggs in the one basket and — WATCH THAT BASKET."

Mark Twain *Pudd'nhead Wilson* (1894)

# Empirical Evidence: Account Sizes in Bitcoin

- Bitcoin stores balances in addresses which can contain multiple coins
- Most coins are held in addresses with 10-100 coins or $50,000 to $500,000 USD
- Four addresses hold 100k coins or more, each worth >US$500M



# Empirical Evidence: Risk of Theft in Digital Currencies

- Famous hacks and breaches of wallets (exchanges)
  - MtGox in 2014, lost 750,000 bitcoins, 7% of all bitcoins in circulation (US$473m)
  - Coincheck in 2018 lost 500 million NEM tokens (US$530m)
- Losses are very common: in 2018 US$950m worth of digital currencies where stolen
- 2019: Binance (one of the largest exchanges) lost US$40m, Bithumb US$13m, …

# Framework

## Good guys

- Customers
  - divide wealth among accounts
  - withdraw with some frequency
  - exercise some level of care in withdrawing
- Banks (i.e. wallets)
  - maintain customer accounts
  - require passwords for access
  - establish safety protocols

## Bad Guys

- Hackers
  - focus on banks
  - deterred by complexity of password
- Thieves
  - focus on customers' withdrawals ("man-in-the-middle" attacks)
  - deterred by customer care and protocol complexity

# Hacking and Equilibrium Password Length

First type of risk: hackers attempt to obtain funds directly from bank by brute force

- $N$ accounts with average balance $s$. Each hacking attempt against a bank costs $h$
- Password length is $q$. Payoff of hacking an account is $s$ with probability $N2^{-q}$
- In equilibrium deterrence requires:

$$q \geq \log_2 ( sN / h )$$

- The bigger the bank, the longer the passwords are necessary.

- With Bitcoin market cap (US$1e11), cheap electricity and the best computing equipment (16Th/sec), $q^*$=93. In Bitcoin $q$=256!

# Probability of Theft is Endogenous to Customer Care

If hacking were the only concern, customers should consolidated wealth in a single account under a long password, however:

- Probability of theft depends on care taken by customer ($e_c$) and protocols established by bank ($e_b$):

$$\pi(e_b, e_c)$$

- Cost to customer also depends on care and protocols (e.g. two-factor authentication):

$$c(e_b, e_c)$$

# Moral Hazard Problem: first best

Bank/principal and customer/agent: customer level of care not observable by bank, but protocol terms are observable by customer

- Optimal arrangement minimizes:

$$L\,\pi(e_b, e_c) + e_b + c(e_b, e_c)$$

- If feasible, customer can be induced to take efficient level of care

$$L\,|\pi_c| = c_c$$

- Bank sets efficient protocols (accounting for costs the protocol imposes on customers)

# Moral Hazard Problem: second best

If costs cannot be imposed on customer (e.g. regulatory limitations)

Say losses are divided $L = L^b + L^c$

- Customer will reduces care:

$$L^c \, |\pi_c| = c_c$$

- Reaction by bank can be:
  - increase stringency of protocols (substitution for customer care) *or*
  - decrease stringency of protocols (to induce increased customer care)

# Password Aggregation Programs

- Reduce cost to customer by holding passwords in a common location, backed by a master password
- In effect consolidate separate accounts into a single account

Interrelation of probability of theft

- Theft when accessing one account leads to theft in all accounts (thus theft at frequently-used accounts imposes disproportionate risk on an infrequently-used account)

# Password Aggregation Programs: implications

- If customer bears entirety of cost of theft, his choice regarding password aggregation programs is efficient
- If he bears less than full cost, he may choose to use password aggregation despite its social costs
- Then banks will have incentive to engage in costly adjustments to block password aggregation

# Policy Interventions

- Externalities suggest a role for policy interventions like mandating certain protocols but these depend on the particular setup
- Requires a more detailed examination of liability rules  and how banks (wallets) are competing

# Conclusions

# Conclusions

- Plenty of work is needed before deciding to issue central bank digital currency (examine its implications, choose a design)
- Even without it, policy makers (consumer protection, privacy agencies) might want to examine the issues of security in private digital currencies

Thanks!

# CBDC Conference and Policy Roundtable, October 16-18, 2019

- Policy Roundtable for Central Bankers: October 16, 2019
- Conference on the Economics of CBDC: October 17-18, 2019