Eggs in one basket: Security and Convenience of Digital Currencies By Kahn, Rivadeneyra, and Wong

Financial Intermediation

Econ 590

Introduction: Tokens vs Accounts

Useful distinction for traditional payments methods

- Verifying a “thing” is not counterfeit vs.
- Verifying the payer’s identity as the account-holder

Relevance for traditional payments technologies

- Not perfect distinction (Swiss Bank Accounts?)
- Nonetheless useful because institutional norms built around 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 (leads to the Fed's "air force")

- Relevance in world of Digital Currencies

- New technologies blur the distinctions
- But institutional norms still active
- So better understanding crucial for establishing new norms

- Modeling Account vs Tokens

- Issues:
  - Who bears cost of protection against malfeasance?
  - Who bears liability in event of malfeasance?

This Paper: Dangers of “Contagion” in Loss

- When bad guy hijacks a token payment, he only gets the token
- When bad guy hijacks an account payment, he gets access to the whole account.

- Level of Aggregation

- Could bury my coins in a single spot in my yard. Or each coin in a different location.

- Separate tokens like “mini-accounts,” each segregated from the next.
- For convenience customers prefer some aggregation into accounts (“wallets” or “purses”)

Application to Digital Currencies

"Addresses": Associated with long private keys, inconvenient but safe (in Bitcoin, part of the underlying structure, containing "UTXO")

"Wallets": Manage private keys of addresses, provide additional convenience (typically competitively operated)

Fundamental tradeoff for customer:

Convenience vs safety

But what is safe?

> 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),
adapted from a speech by Andrew Carnegie, 1885
(source: quoteinvestigator.com)

- Fundamental Questions

- What determines the level of aggregation of customer accounts?
- Are customer and bank incentives for protection of digital currency in alignment?
- As technologies appear for improving convenience or safety will they be adopted or blocked?

The Framework

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

The Framework

- *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

The Framework

The paper considers a variety of specialized models illustrating the framework

First model in detail

Banks: competitive,
N number of accounts, s average size of account
Accounts protected by q-bit passwords.

Total costs of bank:

$$K(N, sN) + C(qN)$$

First model in detail

Customer:

Fixed wealth W received per month, divided among n accounts.

Fixed number of T of equal-sized payments per month.

Cost to customer: $\alpha n + c(Q)$ where Q is total number of bits in all passwords.

Defending against Hackers

An attempt against a bank costs h.

Success occurs with probability $N2^{-q}$

Payoff is s.

- Deterrence requires

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

Consequences

- The bigger the bank's *total* holding, the longer the passwords necessary
- If hacking is the only concern, then a customer's assets should be consolidated in a single account under a long password.

Password Theft and Contagion

Probability of theft is π per withdrawal.

(Assume constant for each withdrawal).

Depositor has n accounts.

Depleted sequentially, with T/n withdrawals per account.

Password Theft and Contagion

Expected amount stolen:

$$\frac{W\pi}{2}\left(\frac{T}{n}-1\right)$$

(The larger the number of accounts, the less is in any account to be stolen).

Password Theft and Contagion

Customers minimize total costs by choosing

$$n = \sqrt{\frac{\pi WT}{\alpha + q^* c'(nq^*)}}$$

Number of accounts increases with wealth, frequency of withdrawal, likelihood of theft, and decreases with cost of handling accounts.

Alternative arrangement: Account hierarchies

Wealth held in “investment account” and regularly transferred to “transaction account” from which multiple payments are made until account exhausted.

Account Hierarchy

Frequency of withdrawal from investment account is approximately

$$\sqrt{\frac{T\pi_t}{\pi_i}}$$

where probability of theft from transaction and investment accounts are π_t , π_i .

(Extensions consider differential costs to withdrawals, and more general hierarchies)

Basic Point

- Thus customer choice of accounts and number of accounts depends on likelihood of theft and costs of protecting the account, (including stringency of password protection)

Endogenizing Probability of Theft

Assume two bank accounts, each accessed once per period.

Probability of theft depends on care taken by customer and protocols demanded by bank.

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

Customer level of care in general not observable by bank, but protocol terms are observable by customer.

Thus a simple moral hazard problem with bank as principal and customer as agent.

- Result

Provided it is feasible to charge the customer the full costs of a theft from his account

- The customer can be induced to take efficient levels of care
- As a result the bank will set efficient protocols, (including taking into account costs the protocol imposes on customers).

But generally full cost cannot be imposed on customer

- Regulatory limitations
- Risk aversion
- Additional incentive problems
  - Moral hazard of bank actions
  - Asymmetric information of cost of breach to bank

Result

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

With multiple accounts at different institutions

- Same conclusions hold independently and separably for each account.
- Even if customer costs of care in the two accounts are interrelated, efficiency is maintained if customer faces entirety of costs of theft, and reduction of costs to customer reduces level of care.

Password aggregation programs

- These reduce cost to customer, by holding passwords in a common location, backed by another password.
- In effect they consolidate separate accounts into a single account.

Password aggregation programs

Multiple channels for interrelation; focus on interrelation of probability of theft.

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

Moral hazard and password aggregation

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.

Cooperative and Non Cooperative Bank Behavior

- If banks choose protocols cooperatively, achieve second best
- If banks choose non-cooperatively
  - may under-invest in protection
  - may over-invest in deterrence of password aggregation

Summary

- Digital currencies do and will generate environments in which wallet providers trade improved convenience for reduced security
- In this environment consumer choice will recapitulate an existing problem of determining the level of aggregation appropriate for accounts.

- Summary

- When customers bear full cost theft from their accounts, they trade off convenience and safety efficiently.
- When they do not (for reasons of risk aversion or because of incentive problems within the payments service providers) they undervalue safety.
- Customer behavior then induces externalities among competing service providers in their own standard setting.

College of Business at Illinois