How are payment accounts special?

Charles M. Kahn[1]

Prepared for the Payments Innovation Symposium
Federal Reserve Bank of Chicago
October 12-13, 2016

It has long been noted that payments arrangements can, generally speaking, be divided into two categories: token-based and account-based systems. The fundamental distinction between the two is *identification requirements*. In a token-based system, the thing that must be identified for the payee to be satisfied with the validity of the payment is the "thing" being transferred—"is this thing counterfeit or legitimate?" In an account-based system, however, the identification is of the customer—"Is this person who he says he is? Does he really have an account with us?"[2]

From this perspective, the arrival of the National Banking Era during the American Civil War, represented a radical change in banks' payment business, as they moved from being the providers of a token payment arrangement (bank notes) to the providers of an account based arrangement (bank drafts and checks). Things have gotten a lot more complicated since then, but banks remain at the center of the payments system, in their joint role as custodian of payments accounts and providers of the access and infrastructure for their use in payment. Although the mixture of types of payments used in Europe is different, the same underlying structure is apparent, with banks playing the dual role of custodian and provider of supportive infrastructure.

We are now, however, in the middle of a series of technological and institutional innovations in the payments system which could change the existing structure. New, hopeful, (and generally internet-based) providers are constructing services which sometimes complement and sometimes provide alternatives to bank-based payment accounts. In response new regulatory structures are being examined and adopted.

---

[1] Professor Emeritus of Finance, University of Illinois, Urbana-Champaign. I thank Brian Mantel for valuable advice and feedback.

[2] Or in more complex cases, "…an account with our intermediary?" Or even, "…an account with our intermediary's intermediary?"

The questions these changes pose are enormous. For example, new payments systems will generate their own information about transactions. Who is responsible for the protection of this information, the new service provider or the legacy account provider? Who is permitted access to this information and for what purposes? How are disputes to be settled, and what will happen when the conditions, terms and warranties between providers are incompatible?

The regulatory change is most apparent in the Eurozone, where officials have provided at least the framework by which new payments service providers are to be given access to their customers' accounts at banks. In the US the boundary lines and the direction are less clear. In both places however, the ultimate outcomes are very much in doubt: Will the new technologies succeed in bypassing the banking system entirely? Will the banks adapt, as they have in the past, to maintain their centrality to the structure and their concomitant benefits, while incorporating the new technologies? Or will some of the aspects of banks' responsibilities as account custodians be separated from other aspects of account infrastructure?

Conceptually dividing the process of servicing an account into a bunch of different specialized bits sounds like an exercise in hairsplitting. And if we were considering a bank's servicing of accounts, say, even thirty years ago, such a separation would indeed have been pointless. But the new technologies for computation, communication and encryption mean that ever finer niches are opening in the process of making and managing payments, and so this separation now becomes relevant and in fact begins to describe some of the specialized activities of new companies.

So I want to take this opportunity to lay out for you some of the considerations that make accounts special—and some of the multiple uses to which accounts are put. This will, I hope enable us to get a better handle on what part of banks' defense of their positions in the payment system is simply special pleading, and what part is indicative of important but previously insufficiently regarded aspects of their job.

What accounts do: credit, aggregation, information collection

The first thing that an account does is to allow for a credit relationship. The account must be linked in this case to the identity of the individual, so that the creditor can have recourse to the individual if repayment is not made. Of course account based systems do not have to be credit arrangements, but without an account, a payments system must be based on upfront pay-ins, as, for example, with prepaid cards.

A payment system linked to purchaser credit is inherently a little more flexible than one linked to pre-paid amounts. With a pre-paid card I can't go below zero; with a credit card I can go down as far as my line of credit. In fact the distinction is a little more subtle than that: we could imagine a bank providing consumer loans to fund pre-paid cards, but a credit card allows the interest charges to adjust to the credit actually used for making payments, a flexibility which has so far not been available under non-account based payment arrangements.[3]

The second thing an account does is to serve as an aggregator—a "wallet." Rather than keep track of individual tokens, the account owner only needs to keep track of the account itself. In fact, this benefit of accounts can be traced back to the very origins of banking in the business of medieval goldsmiths:

Consider the problems of a medieval merchant, worried about the theft of his coins. He can hide them, perhaps bury them. Someone of course might still find them, so perhaps it would be safest, if extremely inconvenient, to bury each one in a separate place. But as an alternative, he can give the whole pile over to the goldsmith. Because of the nature of his business, the goldsmith is also a specialist in protecting valuables. The goldsmith's strongbox was a logical place for a customer to aggregate and store his coins. The good news is that the coins are now conveniently collected in a single location, and that location is much more secure than they would have been otherwise. The bad news, of course, is that if a thief does gain access, the entire pile is lost.

In modern day systems the equivalent problem arises in terms of codes—bits of information rather than pieces of eight. In electronic-money token systems, there is a separate identification for each token, which must be stored, presented, and verified in any exchange, just like each unit of money—each bill or coin— should in principle be checked for legitimacy. In contrast, with an account, you only need to check once per transaction. The seller needs to verify that the buyer is who he says he is, and is indeed connected with the account (and, less importantly, that the account has enough in it). Moreover, the same credentials can be presented to the next seller, leaving the buyer with less to keep track of.

This benefit of convenience of course comes with a downside: access to the account information leaves the purchasing power as a whole vulnerable. Multiple use of the information by the account holder leaves him vulnerable to multiple use by thieves or by unscrupulous merchants. Otherwise put, if I lose a dollar bill, it doesn't leave my other dollar bills vulnerable; if a thief gains access to an individual stored-value card, it doesn't leave my whole bank account compromised.

[3] Some of the latest proposals for e-moneys may make it possible to blur this distinction by allowing for interest payments (and even negative interest payments) on cash holdings.

It might be thought that this difficulty is less importance in modern electronic systems, and to a certain extent that is true: the advantages of economizing on remembering and inspecting all the codes are diminished by the availability of computer memory, and so tokenization arrangements have developed in order to isolate the codes associated with one transaction from the codes associated with the account and other potential transactions. But this advantage is not as complete as might be imagined. After all, in Bitcoin, in principle each token can be kept in an individual wallet separate from its fellows, but individuals still find it useful to consolidate them for ease of handling, and thereby make themselves a little more vulnerable. As we noted, principle a holder of gold coins could bury each one in a different location, but this makes their use much more difficult than keeping them all together, so that anyone who manages to steal one of them probably can get them all. Similarly, the plethora of passwords computer users are faced with nowadays leads them to consolidate their cache of passwords into a single password-holding account—and to vulnerabilities associated with that account.

Thus aggregation into accounts has a real convenience associated with it offsetting the dangers. And any heavy-handed attempt to force disaggregation is likely to lead only to the adoption of aggregators outside of the jurisdiction which is demanding the extra stringency (just like an overzealous IT personnel's mandates for monthly resets of users' password leads individuals to find even less secure bypasses to the decree).

There is an important side benefit to the payment system provider when it links individual identities to an aggregation of payments activity: the information collected becomes a valuable commodity in itself.

The traditional argument in banking studies was that there was a natural complementarity between providing credit and handling checking accounts: by keeping tabs on the inflows and outflows from the depositor's checking account, the bank could get a sense of the creditworthiness of the customer and, just as important, get an early warning of possible credit problems. Similarly, credit card companies can base their extensions of lines of credit on the purchase and payment experiences of their customers. And more significantly, payment systems of the future might be expected to engage in esoteric forms of data mining of payers' payment records to provide ever more complex forms of cross-selling and discount offers—turning payments arrangements into loyalty cards on steroids. Thus access to this raw account information is an asset that the system providers are going to be increasingly loath to give up.

Responsibility for identity verification

Because of the differences in the threats to the user of a token-based system versus an account-based system, we would expect accountability and liability rules to differ for the two types of payment arrangement. And in general they do. For the most part, tokens are bearer instruments—the provider of goods or the redeemer of the token only has to verify the legitimacy of the token; it is not his responsibility (at least traditionally) to question the legitimacy of the source of the token. This makes life simple: the token will become the asset of the recipient (or the reduction of his own liability in the case of inside money) all the incentives are aligned for him to verify it properly.

However when the payment system provider is also custodian of the account of the buyer, the incentives become different. In the absence of other rules, the loss from incorrectly verifying the legitimacy of the check or credit would fall on the depositor or account holder. Thus the custodian must take some responsibility for that verification—is the check good, is the endorser who he says he is? In the case of bearer tokens it is easy enough to put responsibility for their theft entirely on the holder. In the case of accounts, with the possibility of illegitimate reuse of credentials it is much more difficult to allocate ultimate responsibility to the account holder, and so liability is divided in a complex way among buyer seller and account provider.[4]

Thus identification of sellers, and standards placed on them (or on their representative intermediaries) become an important part of an account based system. Because of this there becomes a natural linkage between provision of credit and provision of account based payments arrangements: the identification requirements for the two are complementary. We might even argue that one of the fundamental skills that makes banks banks is their facility at identity establishment and verification. (From this point of view, the provision of letters of introduction and letters of credit and underwriting services are natural complements to the account services.)

Network effects

Network effects are key to the value of a payment system, both to its users and to the system provider. Network effects offer the provider of payments services additional returns: if

[4] In this respect, an account based system actually becomes a little *less* flexible than a token based system. An account-based system requires greater connectivity than a traditional token based system, because the recipient of the payment has to be in closer communication with the account provider, in order to make the necessary verifications. However, this distinction becomes clear with electronic token systems where, because of the problem of reuse of the electronic token, the recipient must also communicate quickly with the payment system.

the system is supported based on his initial wealth, then the extra convenience value of the arrangement is greater the more reusable payments media are. Otherwise put, a bank in the 19th century was happy for its notes to circulate far and wide, putting off the requirement to redeem them and enabling him to hold fractional liquid reserves.

Because of the network effects, a payment provider's fame and reputation are important determinants of the value of his payment mechanism. This is true in both account and token based systems, but with slightly different implications.

In a token based system, fame and reputation affect the likelihood that the recipient will accept the token. Is it easily recognized? Are we confident of its legitimacy? Are we confident that, 1) it is useful in itself 2) someone else will take it or 3) that it can be redeemed easily from the issuer? Fame and reputation (and indeed longevity) factor into acceptability.[5]

When a new token payment arrangement is established, the requirement of acceptability mainly focuses on the third of these options: the system needs to be designed such that the recipients of the tokens have confidence in their easy redemption. But it is the dream of the designer of every new payments arrangement that its stuff circulate far and wide. Once that happens, recipients no longer even worry about the details of the redemption, and the designer begins to reap the seigniorage of the system.

In an account-based system additional considerations arise, because in an account-based system, for the most part, the recipient of the payment must already have an account before any transaction takes place.[6] The fixed costs of identification mean that setting up an account for a single redemption in will be prohibitively expensive. For example, cashing a check when I don't have a bank account is an onerous business; as a result there are companies which (for a hefty fee) specialize in providing such services to the unbanked in this country.

So in these systems it is important for payments system providers to amass large numbers of accounts, because the value of an account to a customer depends on the likelihood of the next person that the next transaction is with someone who *already has* a compatible account. And given the fixed cost of establishing accounts, agents will be uninterested in establishing multiple incompatible accounts.

---

[5] The importance of network effects and recognizability of tokens is carefully examined in many recent papers in the money search literature.

[6] This distinction is not absolute—even cash arrangements require some set-up costs: training at recognizing counterfeits, or at the very least, storage facilities. (So that when space for infrastructure is at a premium, the vendor is likely to concentrate on a single form of payment arrangement, think for example of in-flight beverage service).

Therefore there arises either a single universal arrangement provided by a monopolist, public or private, or a complex combination of cooperation and competition among a set of providers with interoperability of their systems. Indeed often the arrangement is a tiered arrangement: a single, centralized backbone, with individual payments institutions competing and cooperating in their serving of the ultimate customers, who can only access the backbone system through the member institutions—an arrangement that describes both bankcard systems and check clearing.

Admission to the network

Now not every member is equally valuable to the network. A big new member who brings in lots of new accounts provides a big positive externality to the existing membership, making the system more valuable for their customers and therefore for existing membership as well. A small new member—not so much. (In the case of credit cards the situation is slightly complicated by the two-sided nature of the market: banks which specialize in acquiring merchants value the introduction of banks with large numbers of consumer accounts and vice versa, but the general idea continues to hold).

Meanwhile, the members of the network bear responsibility for maintaining the verification of the identities of their customers, and most particularly for the validity of transactions introduced into the system in the name of their customers.

This therefore sets up a very tricky set of questions: Who bears what risk for failures within the system? What are the standards for verification of payment messages, and what are the penalties for failures to meet those standards? An interrelated set of questions arises in the matter of membership in the system: What are the requirements for membership? Who gets to set the requirements? Who gets to make the final determination about who joins the system and under what conditions?

Note that the answers to these questions are likely to be very different if based on political decisions or on profit maximization, and both sets of results are likely to differ in essential ways from what might promote greatest economic efficiency. On the one hand adding members to the group increases the usefulness of the system to the final customers and increases competition among the service providers. On the other hand the additional membership may reduce the incentives of the members fully to monitor and verify payments messages and may make maintenance of standards for protecting the system harder. As aggregators of transactions in accounts, new members may reduce the ability of existing members to mine the payments data they receive for valuable information. New members may not have the financial strength to bear the risks imposed on them by the system's rules for

resolution of errors. With all of these considerations, there is no a priori argument in favor of having the membership rules set either by the regulator or the members themselves; weighing the specific issues becomes necessary.

The other tricky issue is the possibility of secession: Subgroups of the membership (most likely consisting of the largest members) may find it advantageous either to establish independent networks, or to provide a specialized class of services built on existing networks. Again, effects on economic efficiency work in both directions, through a plethora of cross-subsidies.

Summary

When an agent—sovereign, financial institution, or technological startup—establishes a token-based payments system, it must overcome a set of economic hurdles to become successful. The value of the system comes from the seigniorage it provides and that requires widespread acceptance. Widespread acceptance is a bootstrap process: for me to be willing to accept the token I need to be confident that others will be willing to accept the token as well. This in turn requires at first, confidence in the ability to redeem the token and in all cases ease of recognition of the validity of the token.

When an agent establishes an account-based payment system he undertakes an additional set of responsibilities and receives an additional set of privileges. The responsibilities include verification of identities of account holders and their transactions. The privileges include access to more detailed information regarding the customer's transactions, with the opportunities provided for cross-selling and credit monitoring. The account arrangement also provides greater assurance of repeat business from payments customers because of the scale economies and set-up costs in establishing the account relationship.

In comparison with token-based providers, account-based providers have greater incentives to arrange themselves in alliances, taking advantage of interoperability while saving on the costs of identification and verification of customers. The success of these alliances will be dependent on the ground rules established for liability in case of error or fraudulent behavior, and the confidence of the members of the alliance in each others' ability to maintain the necessary standards.

If the members of these alliances have the power unilaterally to block entry of new members, their decisions will be based on a mix of considerations, some based on economic

efficiency and some based on market power. The challenge for the regulatory authorities is therefore to sort through the valid and invalid reasons for account providers to resist entry of new institutions into the payments networks.