Transactions Using Bets

David Wheeler
April 1996

Computer Laboratory,
University of Cambridge, England;
email djw3@cl.cam.ac.uk

Abstract. Small cash transactions, electronic or otherwise, can have their overhead costs reduced by Transactions Using Bets (TUB), using probablistic expectation (betting) as a component. Other types of protocols may also benefit from this idea.

Introduction

In small cash payment systems there is a need to keep the various transaction costs to a minimum. This can be done by using betting as a component of the payment protocol. We first show the principle with physical money where it also has advantages and then consider how it can be used to enhance electronic payment systems.

Real Money

Consider a payment of 37 cents. For it to take place a minimum of four coins must be transferred. Consider how the payment can take place if the payer and seller have only dollar bills. It is assumed for simplicity we have a fair hundred sided dice, numbered 1 to 100.

After the participants have agreed on the transaction, the dice is thrown. If the result is 1-37 the payer gives the seller one dollar, otherwise he gives him nothing. If the transaction is repeated many times the average cost is 37/100 of a dollar, which is correct and unbiased.

There are well known ways of ensuring the dice is unbiased, but we will not discuss them here. Hundred sided dice are a little difficult to obtain, but 20 sided dice numbered 0-9 twice over quite easy to obtain. To use one in the example above, we just throw the dice once, if it has values 0-2 the payment is made, if the value is three we throw the dice again and pay up if it has the value 0-6. The number of times the dice has to be thrown is not much more than once. The average number of extra throws is about 1/9 even for complicated values such as 3.14159265 cents.

This transaction is just if both parties agree, and if they make many such transactions the chance of gaining or losing much is quite small.

In one hundred such transactions with the costs being 1-100 the chance of being more than 3 cents per transaction out is about 1/3 and chance of winning or losing equal. The chance of being more than 6 cents out is about 1/22.

Statistics show that as the number of transactions increase, the total gain or loss is likely to increase but the gain or loss per transaction will decrease.

			probability of one in			
transactions	prices	unit	6.3	44	740	31000
			for gain or loss			
			per transaction to exceed			
1	1-100	100	-	-	-	-
4	1-100	100	-	-	-	-
10	1-100	100	10	-	-	-
100	1-100	100	3	6	-	-
1000	1-100	100	1	2	3	-
10000	1-100	100	.3	.6	.9	-
100,000	1-100	100	.1	.2	.3	.4
1000,000	1-100	100	.03	.06	.09	.12

Table showing approximate loss or gain probabilities.

Thus if we abolish small value coins and accept the fun of betting, we can save some transaction costs. The scheme has obvious advantages for bus fares, simplifying coin machines, etc. even if we do not eliminate most coins and save the government from coining them.

In some cases more benefits can be obtained. Consider toll collection on highways and bridges. If the cost is say 50 cents, we could have one collection booth with a notice such as "toll $10 or zero, average 50 cents". Then there is almost no slowing caused by giving change. We can improve the situation by arranging traffic deflection into one of two lanes according to a "dice". In this case 19/20ths of the traffic would not have to stop, with obvious benefits to drivers feeling, fuel consumption, number of toll booths needed etc. A few old style collection booths would be needed as well, so the customer had a choice.

As in any transaction, a few obvious precautions should be taken to avoid fraud by either of the parties.

User Reaction

Whether the users will like the fun introduced into transactions is difficult to say. It ought to add interest to life like other random events, weather, lotteries etc. However, although there is a gambling element, as the number of transactions increase, the gamble becomes smaller. Bookies do not (or do not need to) gamble, because the statistics protect them. In the same way the users become protected as the system is used more and more.

There are presentation issues which we will not discuss. For example, should the promoter share the saving with the buyer by giving a "betting discount", perhaps better phrased as a "No Change Discount"?

An electronic betting protocol step

The purpose of this paper is not to design complete protocols but to give some component steps which can be incorporated in many protocols to their advantage.

In cash payment protocols, after the transaction is agreed, one step is to transfer a number of 'coins' from the buyer to the seller. In many such protocols, in order to avoid the overheads of splitting coins or giving change, the payment is made as the transfer of a large number of coins, each of which is a number with properties which allow the detection of coin duplication etc.

Such a step or steps can be replaced by a betting protocol such as the steps given below.

1) the seller sends r=h(R), the hash of a random number to the buyer.
2) the buyer sends the coin "number" to the seller.
3) the seller sends R to the buyer.
4) the buyer checks that r=h(R).
5) the buyer and seller work out R+number-cost, determine whether the charge is the coin or nothing, and take action accordingly.

The above assumes the coin number, or parts of it, are sufficiently unpredictable to be used as a random number, otherwise the the buyer can also generate a random number and send it adjoined to the coin number.
The hash is assumed to be a suitable one way function and the necessary scaling factors needed to convert the random numbers into the appropriate numbers for the transaction are also assumed.

If the above is completed satisfactorily, the modes of failure will not have increased for the protocol in which these steps replace the payment step. There is the possibility of either party duplicating the coin, but this possibility existed before. The transaction can be aborted before step 2, which is the commitment step. If the coin is found to be faulty in step 2 then the original protocol will presumably take the proper action.

There is an apparent extra mode of failure. The seller can send a faulty R or fail to send any R at all. These cases correspond in the original protocol for the sending of the coin to be half done or incomplete at the receiver. Thus the original protocol should be able to cope.

Thus we can make the slightly exaggerated assertion that no new modes of failure have been introduced. However, their probabilities will have been altered. But when the new steps are introduced into the protocol, the optimisation and checking of the design will need to be done again, so coping with the altered probabilities will be part of that design process.

Alternative protocols

There are many variations of the given protocol. For example, the buyer could send the coin only if necessary. In the delightful protocol given for Micromint by Ron Rivest and Adi Shamir [1] we can arrange to send 3/4 of a coin which is sufficient to verify it but not cash it, and complete the protocol by sending the last quarter of the coin if it is necessary after the "dice" is examined.

A simpler alternative is to assume auditing will cause the seller to be honest. This was implied in the toll payment system given in the introduction. The steps become

1) The buyer sends the coin number.
2) The seller sends the result of the random discrimination to the buyer.
3) One party nullifies the coin.

Protocol Extension

The method illustrated above will allow protocol extensions. Using the Micromint example, instead of buying 37 pages by 37 one cent coins or 37 one hundredth separate chances of a dollar, we can now pay for them all by a single betting transaction using a dollar coin.

A further possibility exists that we could now arrange for a page to be charged at 1.1 cents with almost no increase in the costs of the transactions. In fact the need for multiple coins in a transaction could almost be eliminated. If a buyer does not care about the fluctuations in the average, he might prefer a larger coin. The use of 100 dollar coins would almost eliminate the need for multiple coin transactions, and allow the costs of the transactions to be kept very low, although the fraud precautions may have to be increased.

Conclusions

Zero average loss betting can often improve small cash transactions by reducing the costs. As one component of a protocol design it will require different optimisations to the basic design, but is likely to give improvements. This is true for both physical and electronic coins.

References

1) Micromint, Ronald L. Rivest and Adi Shamir, This Volume.
2) "Heads I win, tails you lose", Economist June 13 1992 p84.

This article was processed using the LaTeX macro package with LLNCS style