6.915 Computer and Network Security **Fall Term, 1995**

Lecture 18 : November 9

Lecturer: Ron Rivest *Scribe: Yael Gertner*

Outline:

In this lecture we will discuss the following topics:

- Digital Cash
- Micromint

1 Introduction

Prior to discussing digital cash, it is necessary to describe different payment schemes and the properties of cash.

As a good reference to this topic, the book Digital Cash by Peter Wagner (Academic Press, 1996) is recommended. It describes how cash has evolved over time. First, it lists different currencies such as black shells, gold, and tobacco leaves. Then, the book suggests that paper money evolved in the U.S because it helped defeat the English, since it had no value back in England. Some problems with the currencies were raised such as how to convert paper to gold, and the ability of forging by dying while shells black.

Properties of cash or money:

These are the properties we would like money to have, and that money has. They do not define money, since some contradict others. However, they help discuss money.

- Scarcity - the amount of money that we have around.
- Ability to make more - Can more money be easily prepared? Does the ability to make more enables forgery?

- Transferability - The notion of possession is intrinsic with money. Thus, can one own it and then pass these rights or possession to someone else.
  - physical
  - electronic
- Durability - A good currency should not loose value with time. Ice cubes are not a good currency.
- Recognizable - Verifiable digital signatures are easy to recognize. Money has to be recognizable in a way that is not destructive (tobacco leaves should not be smoked in order to verify)
- Measure its value - (intrinsic vs. extrinsic) gold can be weighed, but a person needs to be trained in order to measure the quality of a diamond. The measure should be universal. Intrinsic value is , for example, the property that tobacco leaves can always be smoked if cannot be used as money.
- Uniform size value
- Variable -value (scalability)
- Divisibility - It is convenient if the owner can split a ten dollar bill to 2 five dollar bills.
$$(10\$ \longrightarrow 2 \times 5\$)$$
- Universality - Accepted as medians of exchange. Examples: coupons, frequent flier miles.
- Portable - Could be taken along, in order to pay for a taxi for example.
- Anonymity - could be full-partial-conditional. For example serial numbers on cash are not followed but could provide some info.
- Untraceability
- Unlinkability - Coins should not be connected in a way that would link purchases made with different coins. For example, if a person buys something with one coin, then it should not be linked to his purchase with another coin.
- Privacy
- Utility

- Unstealable
- Liability - Who is responsible if money gets stolen? American express checks cannot be used until signed, and therefore they are replaced if stolen.
- Copiable - It would be helpful to have a back up electronic wallet, so if it is destroyed it can be restored.
- Cash can be defined as a currency that is always accepted without having to worry every time. Thus, what cash is depends on the context.
- Expiration Date
- Revocation - cannot be done with paper money.

2 Account based vs. token based money

In an account based system the broken maintains the account. The user has an account with a certain amount of money in it. He can deposit and withdraw money from the account held by the broker. It is easy to implement an account based system electronically. To have a token based system, electronically, the user can ask for signatures of certain sums from the broker For example, ($ 100 signature{bay bank}) This is verifiable, but easily duplicatable.

Duplication can be either prevented or detected.

- prevent - It is hard to prevent duplication. A way to do it is to use a smart cards that is supposedly tamper proof.
- detect duplication - After a person is detected he can be punished or prevented from doing it again.

For more security prevention and detection can be done.

Detection is complicated because:

1. It is not clear who should do the detecting.
2. Suppose the bank does the detecting, then how can it detect duplicated money that does not pass through it. Therefore, there is the presumption that the money either ends up in the bank by a certain time or expires. A way of making the money end in the bank is limiting the times it can be transfered.

Payword is a credit account system, in which a payword is a claim on an account. The broker maintains the account of the user and makes sure that the user does not over spend. Anonymity is hard to preserve because the internet asks for your address to deliver.

Each scheme has its drawbacks. If we use only account based system and get rid of all cash it would be hard to make simple transactions. On the other hand it is not convenient to have the user go back to the bank for every token spent in a store in order to exchange it. In general the time it takes to make a transaction should be small.

Another difference between the systems is in the way they are perceived. An account based system is similar to maintaining ownership over a particular account. A token, on the other hand, is transfered. Its ownership is exchanged.

Micromint

The desired properties for a token system is that not everyone can come up with a valid token. Only the holder of a secret key could produce a token that is recognizable for signature. A public key system could be used for this purpose. However, it is not efficient, especially for many tokens of small values. Therefore another method should be used that would produce tokens that are easy to recognize and hard to create.

Micromint uses collisions in hash functions to create tokens. Since it is hard to come up with collisions in hash functions, no one other then the bank will be able to create tokens. Furthermore, once a collision is found many more are likely to follow. Thus, we can get a system that produces many tokens that are easy to recognize and hard to forge.

How can a collision be found? Create a table of hash inputs and hashed values and search for duplicates. How long does it take to find a collision? According to the Birthday Paradox for random numbers collisions can be expected after about $\sqrt{number of hashes}$

After collisions are found a token is created by listing all inputs that lead to a collision. Thus, a token is easily verifiable by hashing, which is quick. In addition, a small party like an adversary will not be able to find collisions because it takes a long time to compute. If a party could compute collisions then it could be bank and make money legally that way instead of being an adversary.

The rate at which we see collisions is as follows. At first it takes time for collisions to appear but once they start appearing many of them are found. Thus, this scheme requires paying a lot of money up front, and getting results later. If a token is $(x_1, x_2, x_3, ...x_k)$ and N is the number of bits of Hash (x) Then we will see collisions in $N^{\frac{(k-1)}{k}}$, and after $cN^{\frac{(k-1)}{k}}$ hashes we start seeing c^k coins where $1 \leq c \leq N^{1/k}$.

In addition, the bank can make sure that the coins are not forged by hiding some secret in the x's of the coin, that only the bank knows. For example $lsb(x) = lsb(h(x))$. A forger on the other hand cannot tell if he is satisfying this property. If the forger figures out the secret, then the bank can change it quickly, and the forger will never be able to catch up with the bank. Suppose that some people get caught with forged coins then they lose. Therefore, the coins should return to the bank at the end of the day so that no one will lose vast amounts of money.

The bank then can produce, sell, verify and pass the tokens around. The bank cannot issue two different coins with the same hash value generate.

3 Handouts and Readings

Problem set 8 was handed out. A reading packet containing the chapter called Digital Cash by B. Schneier was handed out. Handouts