Untraceable Electronic Cash with Digicash

Waleed Abrar
Uni-Konstanz

ABSTRACT

Digicash is an online payment method that has a very unique concept regarding the privacy of their clients, which is anonymity, David Chaum introduce a brilliant method to ensure anonymity by introducing blind signatures, this concept is the major milestone for ecommerce and other financial institutions.

This report tends to through light on some important concepts regarding DigiCash, how it works, how they insure anonymity, what's the price of anonymity and how they mimic paper currency properties pros and cons of DigiCash and what happened to the company in the end and current revival.

Keywords

Digicash, double spending, Blind-Signature, anonymity, properties of e-cash, online vs offline DigiCash.

1. INTRODUCTION

Digicash came into being in on 21 April 1990 after working on a project with a colleague, David Chaum decided to open his own company in the year 1993 he introduce electronic cash. His Idea was to mimic the properties of paper cash and produced them in ecash so that to remove the concerns of people regarding buying and selling online as much as possible. The main actors of Digicash are shown below. The concept will be explained later in the report.

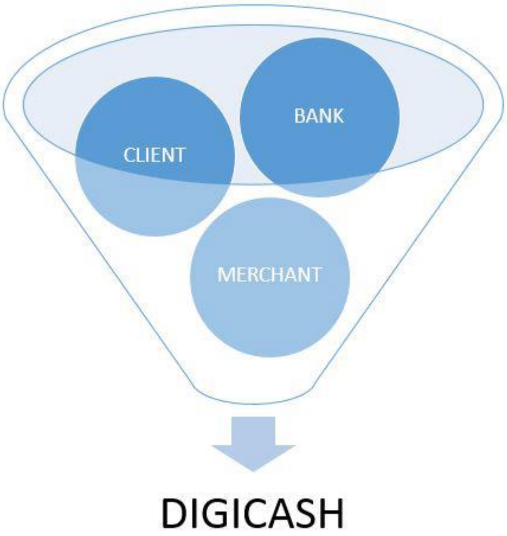

Fig.1: Three major building blocks of DigiCash

2 MOTIVATION:

The main motivation behind Digicash is that it ensures anonymity of the person as long as he didn't double spent and at that point payment with credit card is not secured as there are no standards for sending the data online because SSL are not introduced yet and credit card numbers can be intercepted. Some other factors are, online payment transaction charges are too much and people really avoid online transaction at that time so DigiCash targeted those flaws and became an instant hit in the beginning.

3 PROPERTIES OF ECASH AND DIGICASH:

E- Cash should hold following properties:

1) **Secure:**
E-cash should be secure so that the e-cash should not be forged.
2) **Anonymous:**
David Chaum argued in the paper that as people say the paper money is anonymous, it's not because of the number printed on it. DigiCash introduce anonymity by introducing blind signatures
3) **Portable**:
You can easily carry the e-cash with you anywhere this property also hold in Digicash as well.
4) **Two way:**
One can buy and sell with ecash just as normal cash this property also holds in Digicash as well.
5) **Off-line capable:**
One can perform transaction offline as well without active network connection. This property also holds with Digicash as well.
6) **Widely expectable**
The currency should be widely acceptable and globally recognizable. That's not the case with Digicash it's basically at a small scale level.
7) **User friendly**
E-cash spending should be easy just like paper cash and this property also holds for Digicash. (Birmingham, 2004)

4 HOW DOES IT WORK?

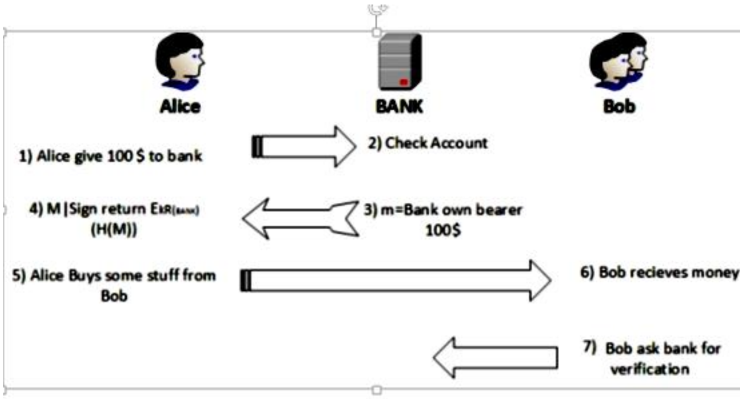
Alice
BANK
Bob
1) Alice give 100 $ to bank
2) Check Account
4) M |Sign return EkR(BANK) (H(M))
3) m=Bank own bearer 100$
5) Alice Buys some stuff from Bob
6) Bob recieves money
7) Bob ask bank for verification

Fig.2: General working of DigiCash

The initial requirement for Digicash to work is that the client and the merchants are sharing common bank which make it a centralized network. Alice deposit some money into her account and afterwards Alice can generate coins based on the money in her account those coins are signed by the bank Private key and returned back to Alice H (M) +Bk after the coins are signed they become currency and now be used to buy some stuff from Bob, Bob verifies the coins from the bank or give challenge to Alice in case of Offline (Friis, 2003). After verification goods can be shared and money will be transferred to his account.

5 BlIND SIGNATURES:-

The mechanism is very simple instead of bank generating the coin. Alice PC software generate the coin requests and hide it with the encryption scheme and send it to the bank to get them stamped .Bank honor the request put forth and sign it with its private key and return it back without having any knowledge about coin (Chaum).When coin is spent it's a valid coin as validated by the bank stamp, because the coin is hidden with the encryption scheme bank can't tell or link it back to the owner of the coin

6 Cut and choose method to avoid cheating:

As the Bank has no information about the coin and it has to trust Alice software to generate the correct sequence, it's probable that Alice generate a 10 $ coin and ask for 100 $ for bank to sign and since bank don't know about coin so its problematic, To avoid that situation, when Alice generate the message to bank for signature, instead of 1 message Alice generate let suppose 100 messages and bank check other messages and then randomly chooses any one message and sign it .The probability for Alice to cheat in this scenario depend upon the number of random messages generated by Alice .Since in our scenario its o.oo1 that Alice is able to cheat.

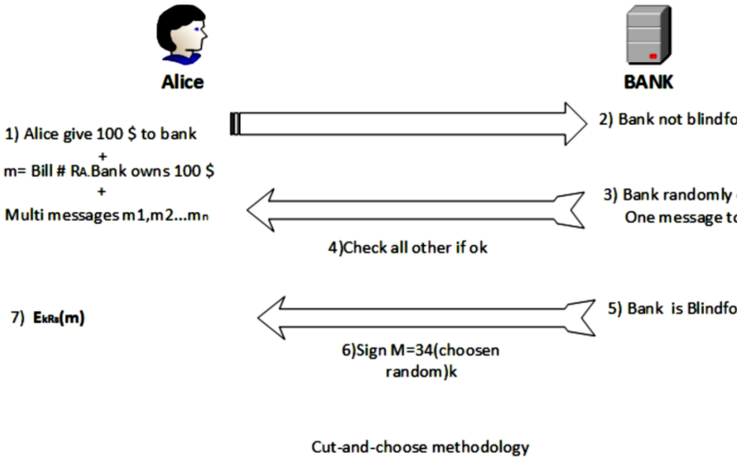
Alice
BANK
1) Alice give 100 $ to bank
+
m= Bill # RA.Bank owns 100 $
+
Multi messages m1,m2...mn
2) Bank not blindfo
3) Bank randomly
One message to
4)Check all other if ok
5) Bank is Blindfo
7) EkRa(m)
6)Sign M=34(choosen random)k
Cut-and-choose methodology

Fig.3: Working of cut and choose methodology 'n' message sent instead of 1

Since bank cant link the Coin origin to its source. One can try to spend the same coin twice , as the coin is digitally signed ,a mechanism should be created to not only detect double spending but get the culprit as well .So David Chaum introduce (David Chaum) a random number whenever the Bank sign a coin it maintain that number into its repository with the count of the number . Double spending is not a problem when working with online Digicash because the Bank check the random number with the message and if the random number exists it will not sign on the coin. But the problem occurs in offline Digicash, Offline Digicash is just like normal Digicash but it has additional hardware with the mechanism inserted to verify the identity of coin and that hardware is trusted by both bank and vendors.

6 AVOIDING DOUBLE SPENDING:-

So to avoid double spending the mechanism is very simple whenever Alice send coins to Bob. Bob give Alice a challenge and just like a Hang man game ask Alice to revel some part of identity and match it with some part that is attached to the Coin for example

ALICE A=1,L=2,I=3….
BOB randomly ask Alice to open 3rd Index and check with the part of identity already sent with Coin not the full identity. If I=3 than the Bob can ask about 1 which is A.
If the challenge is successful than the coin is legitimate and Bank update the account of Bob if Alice Try to double spend Say give the same coin to Lisa.
Lisa has let say ICE part attached with its coin which is 3rd, 4th and 5th index. Lisa challenge and now bank have the same random number and the other half of the Identity which is Anonymous until she double spend.
Now bank can XOR both part of Alice Identity with the padding that was inserted in case of double spending.

The mechanism is explained in below table where two transaction are monitored by bank by BOB and LISA and the bank Identify the Culprit ALICE. (Birmingham, 2004)

TR1	A	L	I	0	0	BOB
TR2	0	0	0	C	E	LISA
XOR	A	L	I	C	E	Gotya

Fig.4: Getting the identity if person do double spending.

7 Advantages and Disadvantages of Online vs Offline DigiCash.

At that time the connections are not very reliable and the merchants are too much focused on having an offline product as well, their advantages and disadvantages are explained below:-

A) **Online Advantages:-**

-Fully anonymous and untraceable unless double spend
-No dual spending problems (coins are checked in real time during the transaction).

-additional hardware is not required.

Online Disadvantages:-

-Communication problems in case of network breakup.

-Huge number of coin database to maintain and match when verifying the coin

-Coin are actually not reusable.

B) **Offline Advantages:-**

-User identity is hidden unless double spend

-Bank can detect double spender accurately.

-Banks don't need to synchronize database in each transaction.

-Reusable coins

Offline Disadvantages:-

-No prevention for double spending.

-Extra security and hardware needed so additional cost.

8 What happened to Digicash and why?

Digicash got bank corrupted in the year 1998 and as pointed out in the article (RH, 1999). It's Mostly because of lack of David Chaum managerial Skills. He is a very good mathematician but not a very good manager due to this they missed many opportunities to do good business with other companies and in the end the board of directors meet and said either you quit or we quiet so at that point he quite the company and short after his departure the company collapsed and all its patients are sold to other companies on very cheap rate.

9 Revival of Digicash:-

As I was going through some literature I found out that DigiCash is going to be reinitiate with a new concept a modern touch (DIGICASH, 2014) .They introduced QR code and software on smartphones which are doing the same stuff as introduced by David Chaum in his paper and they said that it ensures anonymity of user as well, but firstly you have to connect your bank account with it. A simple scenario is explained in diagram below:

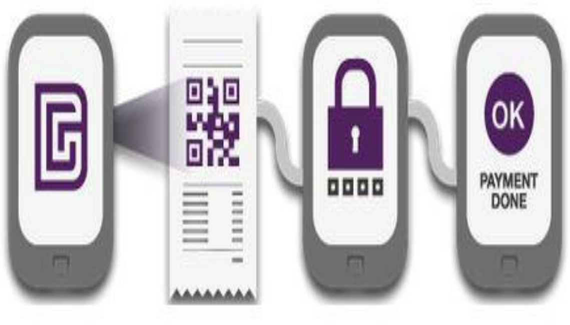

Fig.5: A scenario of a Bill payment with Digicash

Run the app on the smartphone secondly read the QR code on the bill by the camera, App ask to enter the security code and your payment is done.

10 Summary:-

Digicash was an example of an excellent idea went in vein due to some wrong managerial decisions while reading an article (RH, 1999) " Jan Kees Dunning is convinced that the business could have turned out differently to the fatal chain of events that seems to have happened. He estimates that DigiCash needed only another six months to secure a breakthrough. But the company fell during that time. Digicash gave an excellent alternate for paper cash but fell due to some clashes with credit card companies and some people fear that Digicash can be used in money laundering.

11 Lesson Learned:-

According to me Digicash is still very attractive as it has the catch of Anonymity as every end user want not to be followed and leave a transaction trail. But there are some proven attacks now on the security of the RSA which is the basic building block in Digicash for getting Signature. So I won't recommend using Digicash unless those security flaws are removed. Removing physical cash is possible only from the technological perspective but actually it not possible to let people believe that their money actually is in their USB Drive.

Works Cited

Birmingham, L. R. (2004, 02 21). *University of Birmingham Lecure Repository*. Retrieved from Digital Cash: https://www.cs.bham.ac.uk/~mdr/teaching/modules06/netsec/lectures/DigitalCash.html

Chaum, D. (n.d.). Blind Signature System. *US Patent #4759063*.

David Chaum, A. F. (n.d.). Untraceable Electronic Cash. *Advances in Cryptology - CRYPTO '88 Proceedings*.

DIGICASH. (2014). Retrieved from https://www.digicash.lu/fr/fonctionnement

Friis, J. B. (2003). Digicash implementation. *University of Aarhus*.

RH, I. (1999, 2 10). *How DigiCash Blew Everything*. Retrieved from Next! Magazine: http://cryptome.org/jya/digicrash.htm