Introduction to crypto-finance

By Alex Kampa (alex@kampa.com)

Text of an allocution made on 5th June 2015 at the conference
"Crypto-finance for the financial community"
Organised by Hiero a.s.b.l. and held at Lalux Assurances, Leudelange

Hiero a.s.b.l.
17, rue des Légionnaires
L-1926 Luxembourg

www.hiero.lu

Good morning,

[1]

Cryptography has been used in banking for many years now.

Online banking relies heavily on data encryption, and few of us can image a life without online banking any more.

The SWIFT network is the backbone of worldwide banking, and all messages sent via SWIFT are of course also encrypted.

So one could say that much of today's finance is already crypto-finance. However, that specific expression “crypto-finance” is now used in a different context, for which I will attempt to provide a meaningful example.

[2]

Let's take SWIFT. Although the expression “SWIFT payment” is often heard, in fact SWIFT is simply a very secure messaging system. No actual funds are transferred over SWIFT.

Many of you probably know how it works:

Bank A will send a SWIFT message to Bank B, for example requesting a transfer of funds to another bank

Bank B does the transfer (which may also involve SWIFT messages)

Bank B then sends a confirmation to Bank A, stating that the transfer was done

Bank A, although it has received confirmation, has not received proof of the transfer. It cannot be 100% sure that the transfer was actually done; there may have been a computer glitch or some other problem.

To overcome this limitation, we could of course create a world-wide central clearinghouse for banks. However, this is very unlikely to happen.

[3]

But it is also possible to use new concepts of crypto-finance, in particular the concept of distributed ledger, also called shared public ledger.

How could this work?

Suppose a group of banks set up a common network, with each bank representing one or more nodes. Each node maintains a ledger of all the positions and transactions of all the banks in the system. The nodes constantly communicate with each other, and the ledgers are synchronised across nodes in real time.

A transaction occurs through the exchange of messages a bit like SWIFT. For example, Bank A sends a message to Bank B: "transfer 1 million Euros from account ac1 to account ac2". If Bank B acknowledges and confirms the request, then that confirmation open a transaction in the system. This is followed by a consensus-building process across nodes, after which the transaction, if confirmed, becomes part of the ledger (i.e. of all the ledgers). The payment has been made.

Both Bank A and Bank B, as well as the account holders of the accounts that are being debited and credited, can see and verify the transaction in the ledger, they can see the payment.

One can simply say: "The message **is** the payment"

Such a system can be highly resilient. If a node goes down, the system continues to function. When that node then comes back online, it "catches up" with the other nodes and quickly becomes synchronised again. And of course, each bank may choose to have 2 nodes, or more, to avoid being down.

In addition to resiliency, you can imagine the cost efficiency of such a shared system. It eliminates the need to install and maintain complex IT systems at each individual bank, it reduces the need for software and hardware redundancy, it simplifies operations a great deal. There is also much less need for reconciliation.

[4]

I am not speaking of some distant future here. A few banks already use such technologies in a production environment.

And last Friday, exactly one week ago, The Commonwealth Bank of Australia (CBA) announced that it will be using Ripple technology to facilitate payments between subsidiaries.

http://www.coindesk.com/australia-commonwealth-bank-ripple-experiment/

CBA is a major player, it has over 44,000 employees and made a profit of over EUR 6 billion last year.

And Ripple is a leading payment protocol that is open source and is based on a shared, public ledger.

[5]

Let's go back to our example and look at confidentiality.

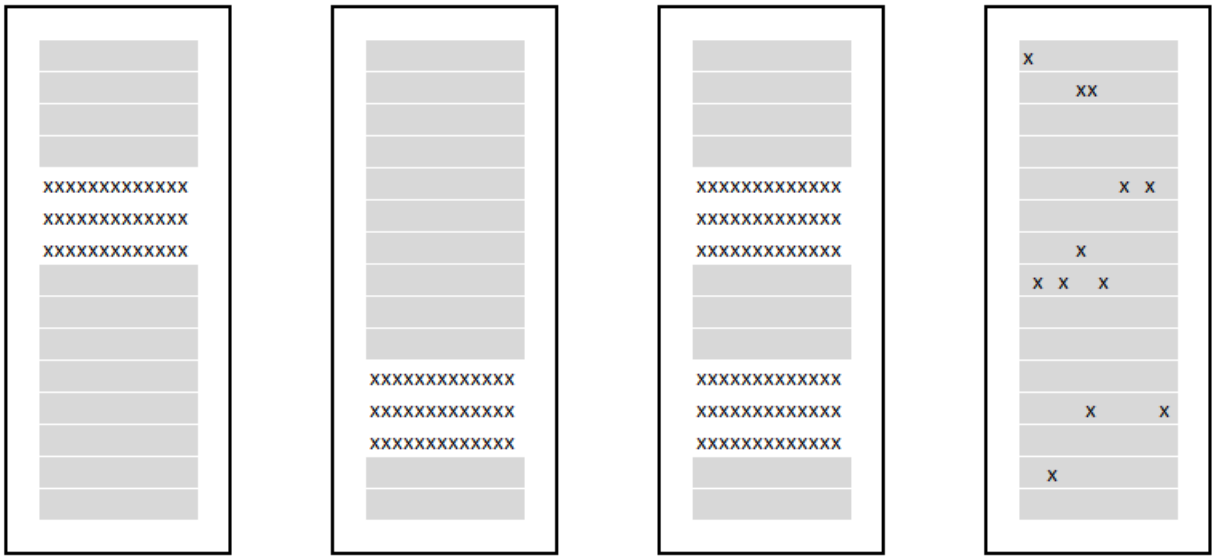
In a network of subsidiaries belonging to the same group, each bank does not necessarily need to hide its information from the other members.

However, if the banks are independent of each other, each bank in the network will clearly not want to show the other banks the details of its operations.

There is a solution: each bank should see only the details of its own customer accounts, and only as much about the system's transactions as is necessary. The rest is rendered opaque via encryption.

However, regulators can be given access to the data of specific banks that are under their supervision, or even just to a certain groups of clients across all banks, for example clients of a certain nationality.

So different actors will have different views of the ledger:



Banks will also require additional features such as KYC (know your customer), the ability to block accounts in case of fraud or theft of identity, and others.

Once these features are available, I believe we will be on the threshold of widespread acceptance of distributed ledger technologies in banking.

That is the coming crypto-finance revolution.

[6]

It so happens that the Ripple protocol mentioned before does not address all of the features that banks and regulators would require. However, Ripple is open source, and anyone can take the source code and build upon it. So there are companies who are developing solutions based on Ripple, that have these key features needed by banks.

One of them is Tembusu Systems, and I would now like to introduce its CEO, Andras Kristof, who has travelled all the way from Singapore to speak to us today.

■