Hiero a.s.b.l.

Introduction to crypto-finance

Alex Kampa
alex.kampa@riskengine.com
+352 691 46 85 81

June 2015

Hiero a.s.b.l.

Cryptography

Cryptography is already widely used in banking:

+ online banking

+ SWIFT

+ etc.

Hiero a.s.b.l.

Example: SWIFT

SWIFT (Society for Worldwide Interbank Financial Telecommunication) messages:

- Bank A sends 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

The confirmation is not proof of transfer !

How can we solve that problem ?

Hiero a.s.b.l.

Distributed ledger

Also called shared public ledger.

Scenario:

- Network of banks
- Each bank has 1 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

Hiero a.s.b.l.

Transactions

A transaction occurs through the exchange of messages:

- Bank A sends a message to Bank B requesting a transfer
- Bank B acknowledges and confirms the request
- A transaction is opened in the system.
- After a consensus-building process across nodes, the transaction, if confirmed, becomes part of the ledger (i.e. of all the ledgers).

Result: 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.

The message **is** the payment

Hiero a.s.b.l.

It’s happening now

Australia's Commonwealth Bank Latest to Experiment With Ripple

Jon Southurst (@southtopia) | Published on May 29, 2015 at 09:53 BST

NEWS

521 131 10 20 24

The Commonwealth Bank of Australia (CBA) announced this week it will use Ripple technology to facilitate payments between its subsidiaries, describing distributed protocols as "the way of the future".

Last May, Germany's Fidor became the first bank to integrate Ripple's protocol into its payments infrastructure, with two US banks, CBW Bank and Cross River Bank, following suit four months later.

Hiero a.s.b.l.

Confidentiality

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

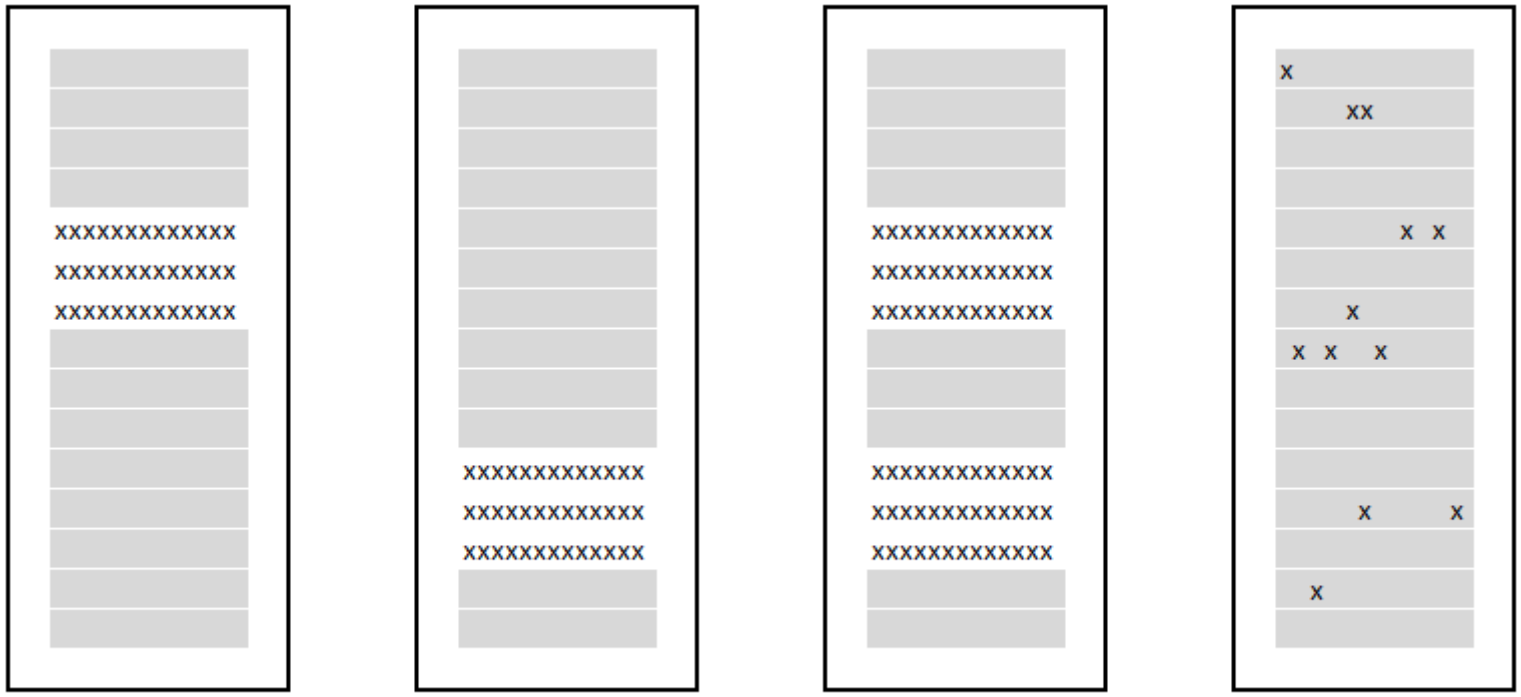
However, if the banks are independent of each other, confidentiality is required.

The 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.

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.

Hiero a.s.b.l.

Different views of the ledger



Hiero a.s.b.l.

The crypto-finance revolution

Distributed ledger technology

+

Features required by banks and regulators

=

Widespread acceptance in the foreseeable future