Interledger

possible solution for path-finding & id-management

DRAFT

moneygrid.net

Version 0.1

21/10/15

by Lucas Huber
http://moneygrid.net
lh@codoo.io

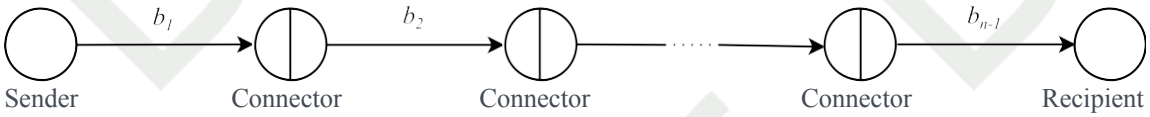
Content

1 Overview

The interledger[1] protocol (ILP) does provide a very promising path towards a universal standard to perform Realtime Clearing or transactions between ledgers of any type.

The solution with escrowed (atomic notaries) transactions allowing a high security standard and the universal mode with a minimum set of security is giving enough flexibility for many use cases. But what needs to be looked at is the ways how a transaction finds the way through a number of connector to catch the receiver of the payment and even more complex how the participants of this transaction gets information about each other (id-management).

If we look at this payment chain it is obvious that a lot of information to establish even a valid connection between Sender and Recipient are missing.



If you attach a global kind of ID server to the system at least the information who belongs to which ledger could be solved and distributed. But this is of course far from to be an ideal solution. Another challenge is that different types of ledgers have also very different solutions to keep track of the ID's of its participants. So maybe it would a good starting point how this different systems are handling this problem or what information they could provide to enable the connectors to find the correct path to the Recipient.

1.1 Classification of use cases

So a classification of use cases can give some information in which direction a good solution for interledger can be found.

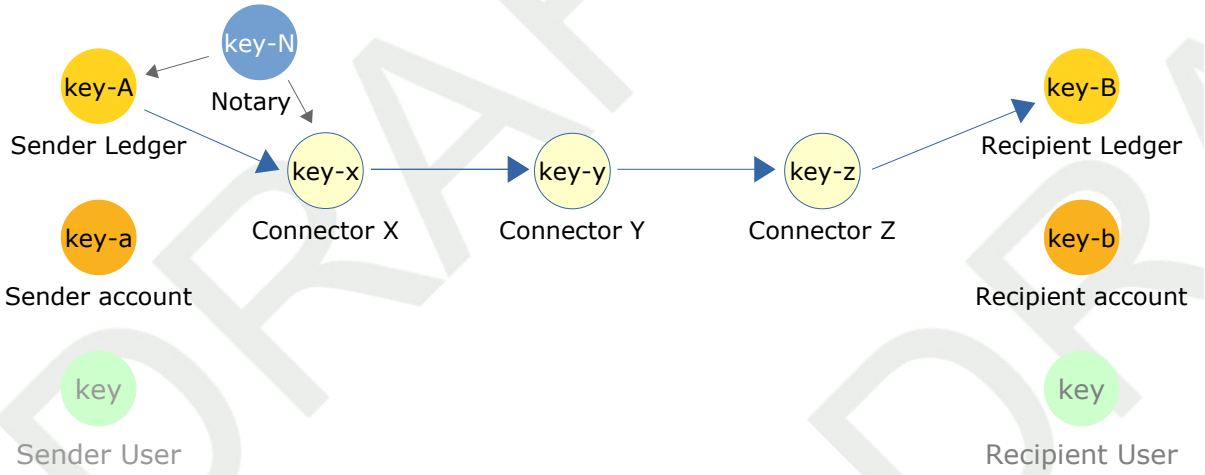
Use Case	Basic ID instance	ID inherited infos	Existent protocol	Remarks
Banking	IBAN[2] or other	ID of recipient Bank	ISO 20022	
CryptoCurrencies	Public key	none	none	
CommunityCurrencies	unknown	none	none	
Other	unknown	none	none	

Obvious it would be a bad solution to use a kind of IBAN system for all the other use cases. The system has to be as simple as possible. A Public Key or and URL ID system are both simple and universal. Of course use cases with other ID Systems as IBAN have to provide a Public Key or an URL if they would like to use interledger for their transactions.

1 Link to http://interledger.org
2 IBAN International Bank Account Number: https://en.wikipedia.org/wiki/International_Bank_Account_Number

1.2 Possible solution using keys

Lets suppose Public Key are used to define the identities of all the participant. That includes accounts, ledgers, connectors and ev. Users too.



The important question is how the connectors know to establish a path to the Recipient ledger (key-B) and what other actors are involved into the transaction. Furthermore they have to know the IP address and other stuff of each other.
A straightforward solution would be to use a permissoned distributed ID ledger between all the instances. If the sender does or must know the key of the Recipient ledger (key-B) then every information should be in place to start a transaction.

Maybe it is helpful to introduce here a new name for the participant? State-machine[3] would be appropriate. In this case sender and recipient ledgers plus ID are state-machines as well the connectors are. All transaction related process are correctly handled if in a certain timeframe all state-machine have the same state about a transaction. But not only about transaction but also on the information about ID's.
The distributed ID ledger should contain at least the following information:

Items	Type	keys	IP/port	Remarks/name	connection
Sender ledger (A)	exchange	key-A	234.011.002.121:?		key-x
Recipient ledger (B)	exchange	key-B	034.211.102.141:?		key-z
Connector X	conn	key-x	123.011.042.211:?		key-A,..y
Connector Y	conn	key-y	241.011.302.116:?		key-x,..z
Connector Z	conn	key-z	189.111.002.121:?		key-y,..B
Notary N	notary	key-N	?	For escrowed transactions	Key-A,..x
Regulator	regulator	key-R	?	Optional if needed	key-z

For each Connector also the information to which other Connector and Exchange he is directly connected to is important. That can be solved with a Many2many relationship between a field connection and the other entries.

3 Link to Wikipedia: https://en.wikipedia.org/wiki/Finite-state_machine

This solution has still a great risk that the relationship and ID's between the different actors or state-machines could be tracked and published or used for unwanted purpose. An additional cryptographic layer could help here to provide a maximum of privacy of the participants. It is worth ta take a look to Pavel Kravchenkos paper in which he introduces his concept of Proof of Identity (POI)[4]. A similar solution as POI could be used to encrypt most the users Public Keys in the ID ledger so that only the stake-machines that are involved in a transaction have the possibility to get the correct public keys.

1.3 Path-finding

Generally to different types of path-finding should be possible, depending on the use cases. Either the marketmaker approach, in which the connector(s) with the best rates does perform the transaction and a structured solution where it is predefined which path is to go. The second approach is absolutely a must for most of the community currency type transactions, because mostly CC's are per definition local, eg. intertrading them has to be done very carefully under very limited conditions.

TBD

4 Link to Google doc Tembusu Whitepaper: https://docs.google.com/document/d/1pqeAD7OhP9nEmwqEm6SucGaSGhJMW_GCf2Ggo0BXX5c

2 Closing thoughts

Of course this paper can only give some hints about a possible solution and hopefully introduces some basics for the further discussions.

Beside of the fundamental aspect of path-finding and ID management to ILP, there are other issues that are worth to have look at. For example, how to enrol and list the fees to the users. I can imagine that every user would like to know in human readable form where all the fees are coming from and why.