Generic Value Transfer

Joost Bambacht

May 4, 2021

1 Problem Description

People and businesses strive to become more digitally oriented and more in control of privacy-sensitive data about themselves. This may sound contradicting, but it does not necessarily has to be that way. Identities are already implemented digitally in some way, although, the implementation lacks privacy standards of the user. The required authorisation of third parties to connect your identity to their systems unnecessarily exposes a lot of information about these people. With the introduction of digital identities users should be much more in control of their own data and choose what attributes to share with these organisations and other individuals. Big-tech companies like Whatsapp do not care much about the privacy of their users and have a lot of valuable information that could sell to other companies. Online chats between peers should be privacy-oriented such that no-one else could take advantage of their conversations. Old-school cash transfer between you and your friends, without the intervenience of banks and authorities, can be replaced by the use of digital stablecoins. These coins represent a native currency digitally and can be bought or sold from/to the physical currency. These transfers would not appear on bank debits or any tax forms. The only thing that is visible to banks and authorities is when someone trades the digital currency for the native currency.

All three concepts has been researched before in the form of PeerChat, EuroToken, and SSI. The transfer between these concepts can be seen as value transfer from one identity to another identity or organization. The integration of these three concepts can be merged in order to create a connection and transfer of value between digital identities and other identities/organizations.

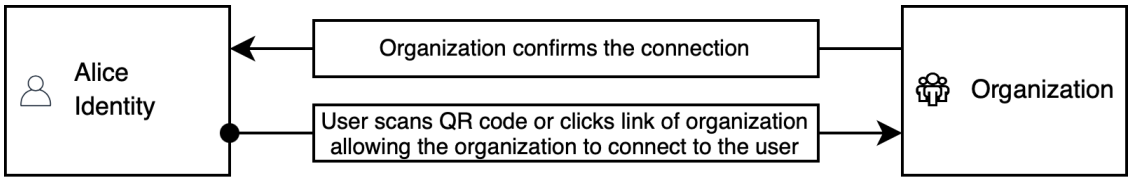
Especially organizations obtain a lot of information about individuals that they do not need. A person should be able to be in control of their information at all times. To sign a contract with an organization for example, the user should, of course, hand over some information about theirselves. It is difficult to know what the organization does with this information. Are they saving it locally to fetch it from their database when they need it? This is of course not very privacy friendly. A better method would be for example to request the information every time it needs it, but that requires a lot of more interaction between the user and organization.

The goal of this thesis is to create a platform that enables users to stay in control of their own digital identity, arrange the communication between users and organizations/users and enables the transfer of value between these parties. These values include personal information, digital cash, conversations, documents and contracts, and possibly other assets. These informations should be stored decentralised on the users personal chain and can only be accessed by the includes parties.

1.1 Transfer of value between an user and organization

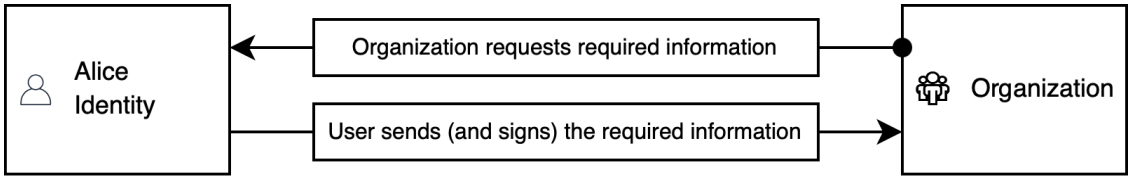
Users and organizations must be connected and share information in both directions to be able to deliver and use the service they aim to provide. This can for instance be a health care organization or telephone provider that requires confidential user information. Instead of obtaining this information by the use of DigiD, a digital identity can deliver only the required information. The user is always in control, meaning the user should initiate the connection to the organization in order to prevent spam and impersonating attacks by malicious organizations. After the user and organization are connected, the organization is able to request information, send information (like normal peers) to the users, propose a contract, or asking the user to sign a contract or document.

Connection and interaction between user and organization



Initiative must originate from the user to protect the privacy of an user. Even if the organization has the public key of the user it is not able to make a connection. Only after the user scanned or clicked the link it can connect. Possibly also allow the organization to connect to the user with its public key in combination with a 'secret' key.

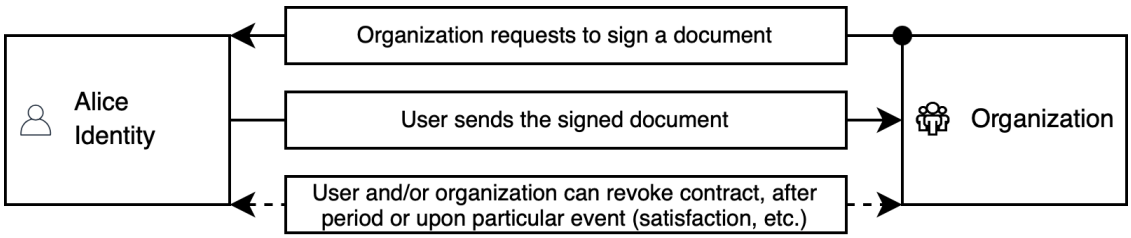
Information request from organization to user



Difficulty: when 'sending' this information to the organization the organization is able to save this data. How to control this? Revoke authorization of looking into this data? Possibly by creating a contract in case the users' data is mis-used the organization will get a penalty or the user will receive compensation?

Brainstorm: example application may be a health dossier of an user that possibly can be stored on the chain of the user?

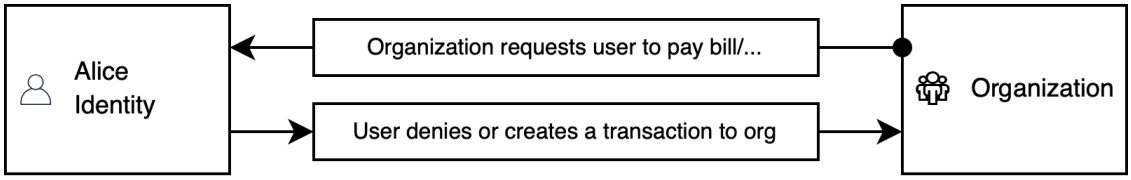
Organization requests user to sign a contract (or other document)



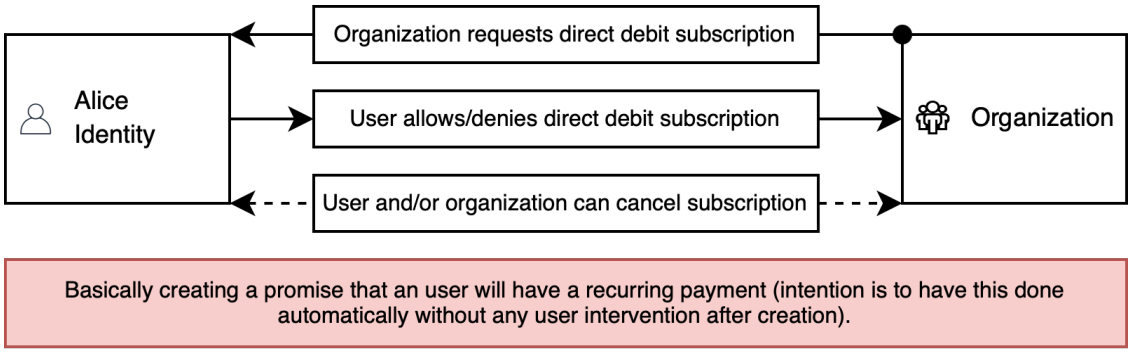
1.2 Money transfer between user and organization

An organization also requires payments for their services, in this case using the EuroToken protocol. This can be done by either sending a pay request or a direct debit request. These requests can only be sent (and received) after a connection is established between the user and organization.

Pay request from organization (using EuroToken)



Direct Debit Request (using EuroToken)

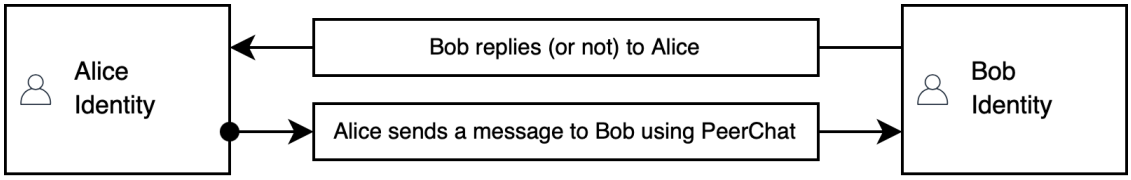


Basically creating a promise that an user will have a recurring payment (intention is to have this done automatically without any user intervention after creation).

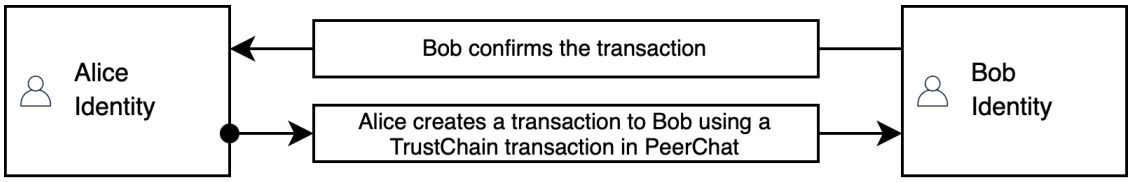
1.3 Value transfer between two individuals

Apart from the transfer of value between users and organizations it is also possible to have conversations between two identities. Messages are probably not directly seen as value transfer, but the transfer of digital cash is.

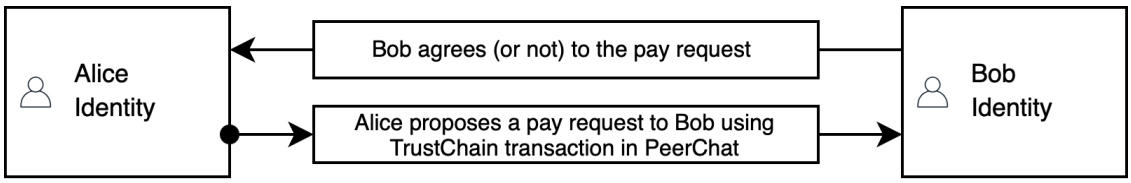
Send message (w/o payload) from peer to peer



Send money from peer to peer



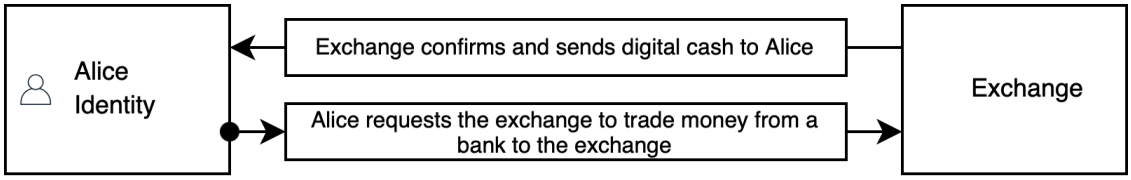
Send pay request from peer to peer



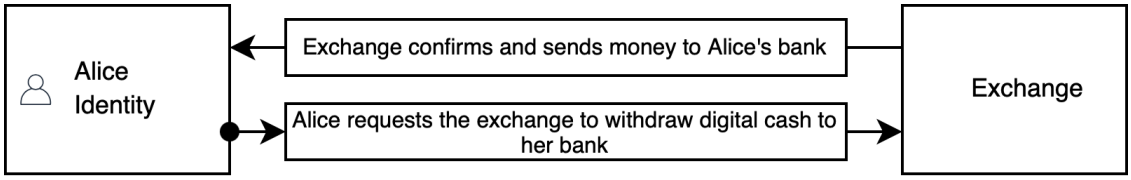
1.4 Value transfer from/to bank and exchange

In order to be able to send money to organizations or other users, it should be possible to top up the users' balance. This can be done by converting real money from a bank to digital cash in the form of EuroTokens. Since the EuroToken is a stable coin, the rate should have very small fluctuations around 1.00. It should likewise be possible to exchange the digital cash for real money and withdraw it to your bank.

Add balance to wallet



Withdraw digital cash to bank



1.5 Example App Sketch