TRANSFER OF GENERIC VALUE BETWEEN SELF-SOVEREIGN IDENTITIES

Joost Bambacht

June 2, 2021

1 Introduction

-

2 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 digitally oriented and available, although, current implementations do not respect users' privacy standards. The required authorisation of third parties during the connection of identities to their systems unnecessarily exposes a lot of information about these individuals. With the introduction of digital identities users should be much more in control of their own personal information, also called self sovereignty. Current social media platforms enables users to create identities with fake user information, something that shouldn't be possible with legitimate digital identities.

In general, most big-tech companies like WhatsApp and Facebook do not respect the privacy of their users. Valuable information of users is being sold to other companies, for example for personal advertising. The content of online chats between peers should be secret to others besides the participants. These companies are leading in the market and therefore have power over its users. Privacy-related changes in their terms and conditions will still result in nearly everyone agreeing with it, even people that actually read the changes in the policies. The main reason is that people are depending and/or addicted to their service. It is clear that these companies benefit from their position and that centralization, at least in this case, is not a good thing. Organisations 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 organisation for example, the user should, of course, hand over some information about theirselves. It is difficult to know what the organisation 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 organisation.

It's no secret that offline money transfers in the form of banknotes and coins will eventually disappear. Currently, cash is still the second most preferred payment method, with in the Netherlands in 2020 worth for one-fifth of all transactions and two-fifth of all person-to-person transactions[1]. The Netherlands is one of the countries in Europe that is further digitally developed than average, indicating that cash payments are far more important in less developed countries. Unfortunately, there are costs attached to the transfer of money, both online and offline. The costs of the use of an ATM or in-store debit-card transactions range from about €0,05 to €0,20[2] per transaction, uncorrelated to the transaction value. Online payment services like iDEAL, the leading online payment method, even asks significantly more, depending on the contract the webshop has. The transactions costs that are charged between the buyer and seller are unnecessarily high, and (almost) neglectable in blockchain-based applications. It is important to offer the option for online/offline cash-like money transfer in the future, mainly to retain peoples' privacy and stop government agencies from lurking over peoples' transactions. Cash transfers between people, without the intervention of banks and authorities, can be replaced by the transfer by the use of Central Bank Digital Currencies (CBDC). These coins transfer almost instantly without fees, making it a serious contender for current online payment services.

The concepts of the mentioned problems has been researched before and resulted in the standalone implementations of PeerChat, EuroToken, and SSI within TrustChain[3]. TrustChain is a so-called Super App that (in this case) provides the framework to include many small apps. It is possible to share user identity and information over all apps.

The goal of this thesis is to design and implement a platform that enables users to stay in control of their own digital identity, while communicating with other users or organisations enabling the transfer of sort of value between the participants. These values include personal information, digital cash, conversations, documents and contracts, and possibly other assets. User information should be stored decentralized on the users personal chain and can only be read by the included parties and never by anyone else. No information can be inferred from the chain without authorization.

3 State of the Art

In this section the principles of various researches, concepts, protocols or implementations of subproblems that are used in this thesis are discussed.

3.1 Network structures

For a long time most infrastructures of services, systems and networks were designed such that a central authority is responsible for everything: availability of the service, storage of data, updates and security fixes. At first sight this centralized structure [1] sounds very convenient for the end-user since they do not have to care about anything apart from using the service. There are however major drawbacks from this structure: (1) controlled by

[1] `https://factsheet.betaalvereniging.nl/en/`

[2] `https://pindirect.nl/kennisbank/uw-eigen-pinautomaat/wat-kost-een-pintransactie/`

[3] `https://github.com/Tribler/trustchain-superapp`

one (or more) parties that is able control the service without user involvement, (2) single point of failure, (3) storage of users' data on their servers. Especially the last argument received a lot of attention lately due to ignoring users' privacy standards. Other structures are nowadays often used in networks and blockchains, mainly due to the mentioned issues. In a decentralized structure a single central authority is replaced by numerous nodes to divide the responsibilities while each of the nodes is in full control. It obviously reduces the delays for its users and is less vulnerable for attacks, but still contains some (small) form of centralization. A distributed structure is a deviation that completely eliminates centralization by dividing the service across various hardware systems. This way the ownership of the data, therefore solving the single point of failure issue, decreasing security and privacy concerns, and improving performance. In contrast, in a centralized structure every client is directly connected to the central server while in a distributed setting clients are linked to multiple other clients, providing a lot more reliability. Anyone with a system with the required specifications is able to run its own node, therefore contributing to the peer-to-peer (P2P) network. In essence, a P2P network is a distributed network in which their nodes, or peers, are able to directly contact with each other. Blockchains (in general) make use of distributed networks that is completely decentralized and there is no dependency on single systems. In fig. 1 an overview of the discussed structures can be seen.

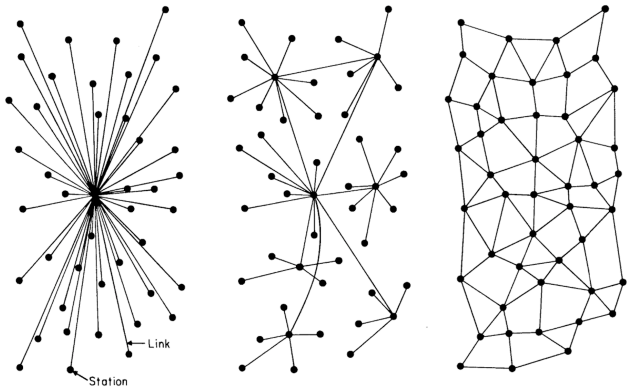


Figure 1: centralized, decentralized, distributed network structures [1]

3.2 Public Key Cryptography

Secure communication is a very important aspect of privacy, and plays a major part in this research as well. Since the blockchain is readable for basically anyone, (message) security by means of encryption is definitely required. Securing the communication between two parties by encryption using a shared secret key is not feasible, due to the exchange of a secret key between two participants. There does not always exists a secure channel for distribution of this key, both on- and offline. Diffie and Hellman [2] designed a system that doesn't require a common secret key that is known by both participants. Instead, every party has a public key E and private key D that are cryptographically entangled. Alice is able to send a private message to Bob by encrypting the message using the public key E_B of Bob. The message can only be decrypted using the private key D_B of Bob. Figure 2 shows the

encryption/decryption process between two participants. The public key can be publicly known by anyone, but in case of on-line exchange a secure channel must be used to avoid for instance man-in-the-middle attacks.

Figure 2: Public key encryption and decryption

Another great benefit of public key cryptography is that it is possible to create and verify signatures, signed by the creator of the message, to prove that the message is written by the sender and has not been tampered with. Alice can create, complementary to encrypting the message, a signature by signing the message with her private key. Bob can, after decrypting the message, verify the Alice's signature using the public key of Alice. Figure 3 shows the process of digital signing and verifying signatures.

Figure 3: Public key digital signatures

3.2.1 Private-public key generation

The TrustChain app creates a private-public key pair on first launch. The private key is a random string with length of 32 bytes. The public key can be derived using elliptic-curve cryptography, specifically Curve25519, by taking the generator point of the curve of the private key and multiply it. This process cannot be reversed, therefore providing the private key of a wallet often resembles sufficient prove of the wallet's ownership, and the public key is not required since it can be derived. The public key has a length of 148 bytes, therefore a bit difficult to handle manually. A member ID can be derived from the public key using SHA-1 to derive a hash of 40 bytes.

3.2.2 Public Key Infrastructure (PKI)

A thrust-worthy public key infrastructure (PKI) is required to realise this system. A government body is appointed as the root identity provider initially, and controls and manages the distribution of identities. Although this sounds like a centralised structure, the government is, and should, still remain the legal entity that is in charge of issue-ing new identities. Without their control there will be a market for fake identities which will destroy the ecosystem. The government, or a sub-body, also takes the roll of verifier, that will check the legitimacy of identities. In the future other institutions can fulfil the same role.

3.3 Decentralized social communication

Companies like Facebook and WhatsApp provide an easy way to create a social network for its users. By joining their services, the user has to agree that their company owns your data. Centralised structures like these are far from privacy friendly and many people do not realise what they are actually agreeing with. There is need for decentralized services in which the user controls, manages, and own their personal data. Research conducted by Skála [3] provides an overlay for the IPv8 framework[4] that serves as a communication application between two peers on the TrustChain. Peers are able to communicate text, digital money, and attachments after both added the public key of the other.

3.4 Central Bank Digital Currency (CBDC)

A CBDC represents a native currency digitally and should, in most cases, have the exact same value as is physical counterpart. An exchange makes it possible to buy and sell from/to the physical currency. These transfers would not and don't have to appear on bank debits or any tax forms as it has been before cash was digitised. The only thing that will, and should, be visible to banks and authorities is the exchange of a digital currency to the native currency and vice versa. The change in the identity infrastructure provides a lot of opportunities to the privacy to users. Blokzijl [4] researched and implemented a digital payment system for the Euro currency, including offline payment capability.

3.5 Self-Sovereign Identity (SSI)

A self sovereign identity (SSI) makes sure that its owner is control of the identity, and no other party (even the government) is able to manage it. The government is, of course, the institution that issues and distributes the a users' initial identity, after which it is not able to control it. The identity owner choose what attributes to share with third parties like organisations and other individuals. In previous research Chotkan [5] created a digital identity that enables attesting of attributes of an identity without revealing the actual value but instead proving it using a zero-knowledge proof.

An individual will have a standard self-sovereign identity while an organisation will receive a digital business identity (DBI). Using this identity the organisation should be able to perform various actions like composing contracts with individual identities. The core idea of this connection between SSI's and DBI's is that the user stays in control. This also means that the initial initiative is with the individual. This limits the possibility of spamming and phishing by fake businesses to obtain information or value from individuals.

4 Functionalities

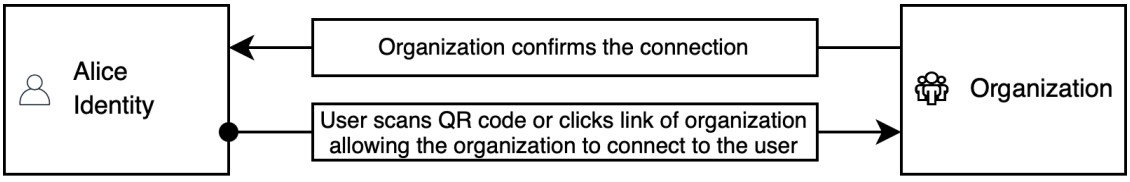
4.1 Transfer of value between an user and organisation

Users and organisations 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

[4] `https://github.com/Tribler/kotlin-ipv8`

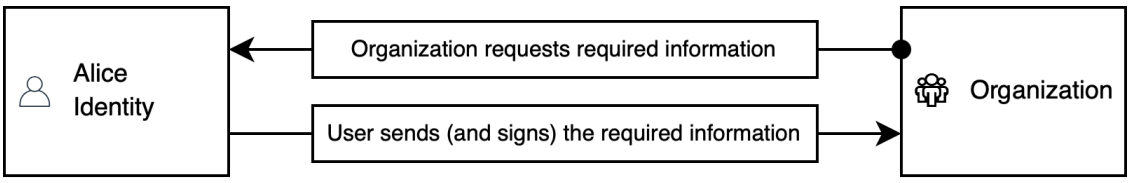
health care organisation or telephone provider that requires confidential user information. Instead of obtaining this information by the use of DigiD, a digital identity can deliver only the required information. The user is always in control, meaning the user should initiate the connection to the organisation in order to prevent spam and impersonating attacks by malicious organisations. After the user and organisation are connected, the organisation 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 organisation



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.

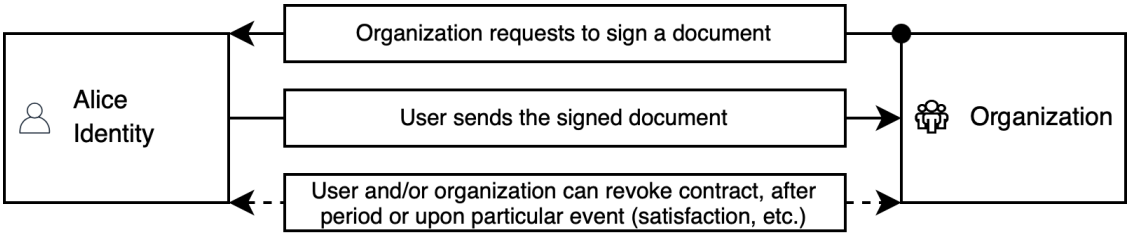
Information request from organisation to user



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?

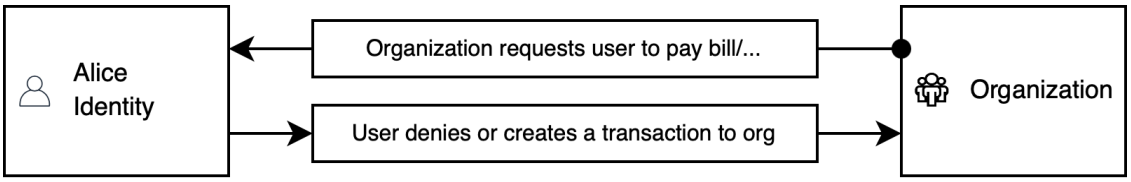
Organisation requests user to sign a contract (or other document)



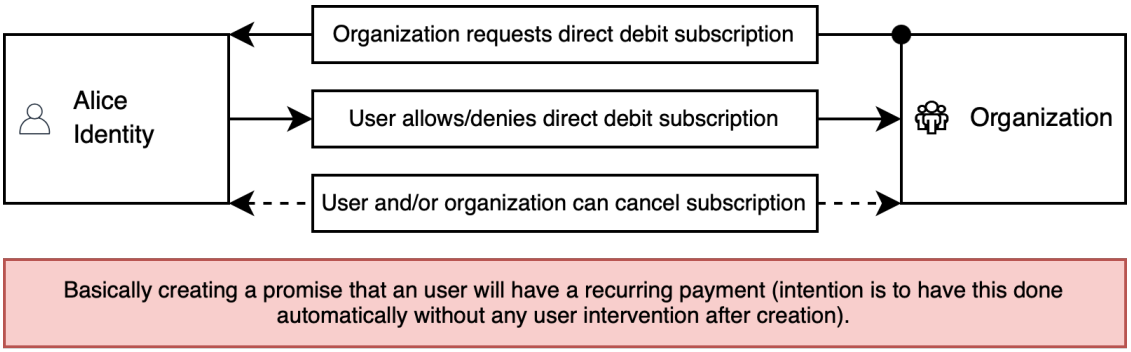
4.2 Money transfer between user and organisation

An organisation 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 organisation.

Pay request from organisation (using EuroToken)



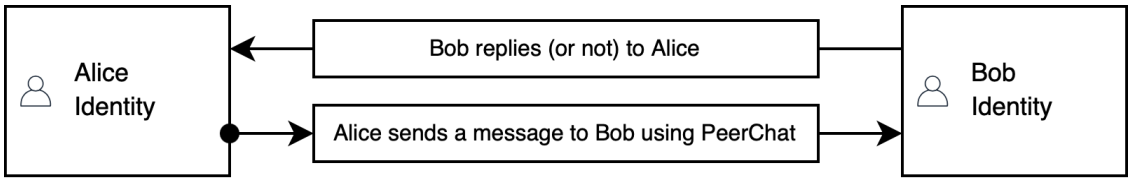
Direct Debit Request (using EuroToken)



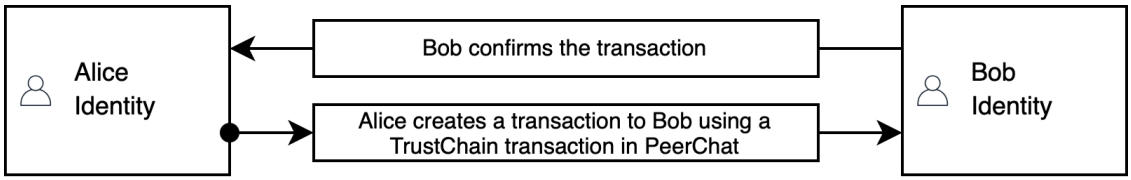
4.3 Value transfer between two individuals

Apart from the transfer of value between users and organisations 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.

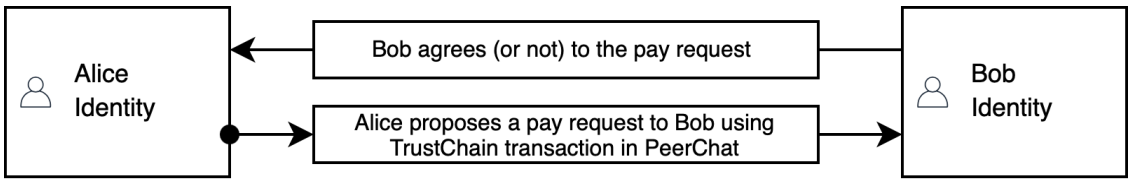
Send message (w/o payload) from peer to peer



Send money from peer to peer



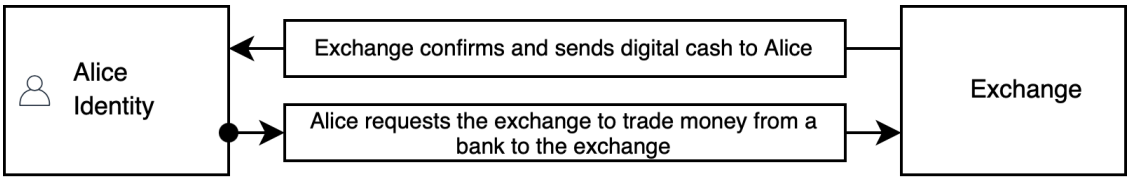
Send pay request from peer to peer



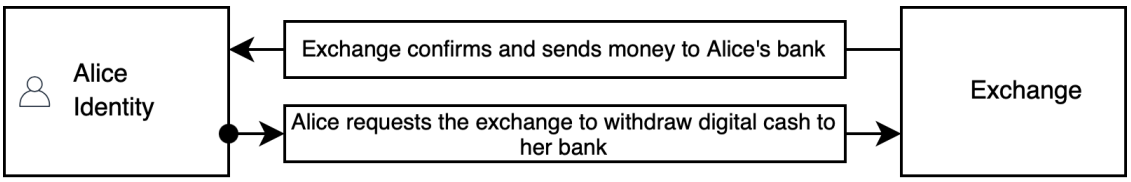
4.4 Value transfer from/to bank and exchange

In order to be able to send money to organisations 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.

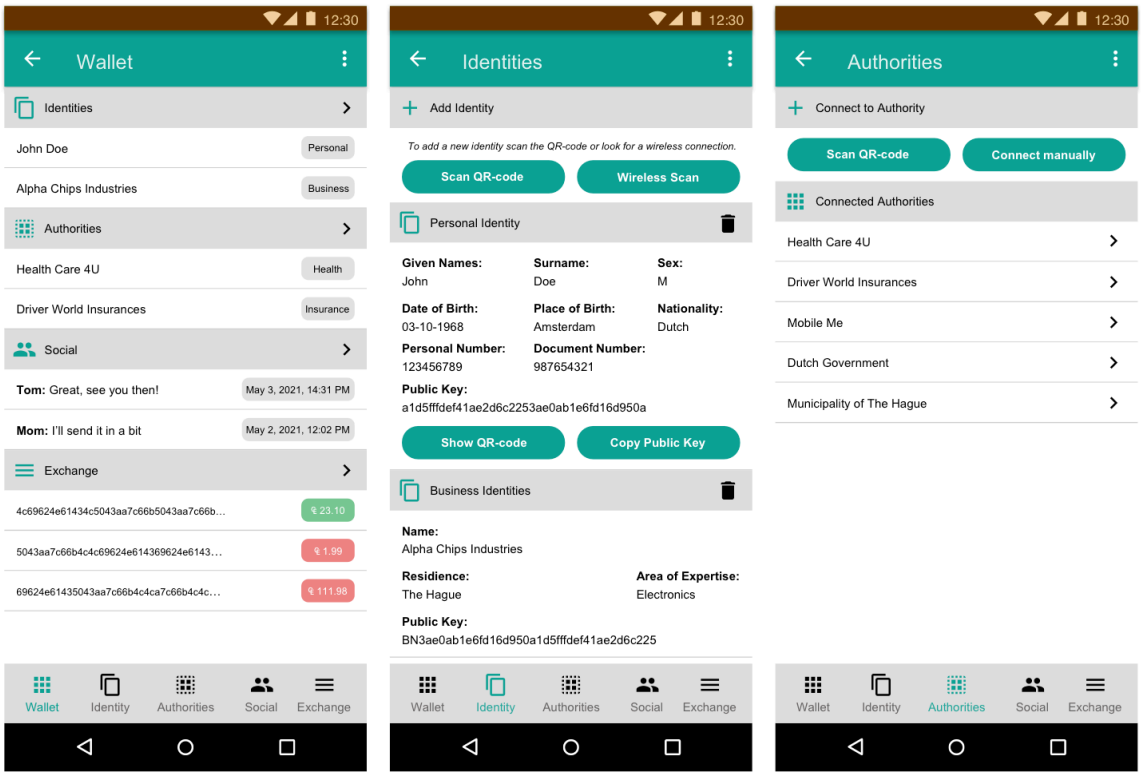
Add balance to wallet



Withdraw digital cash to bank



4.5 Example App Sketch



References

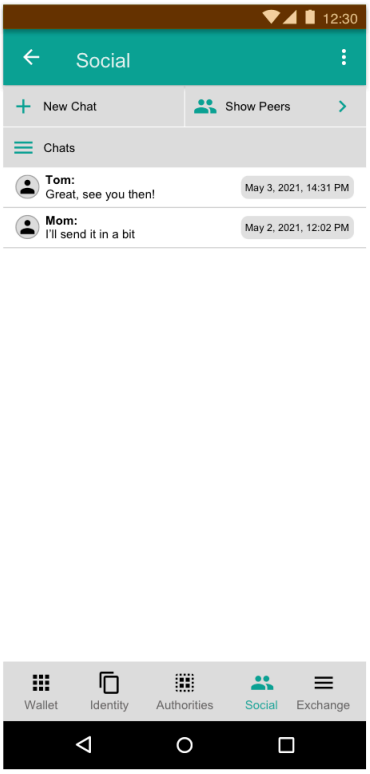
[1] P. Baran. *On Distributed Communications, Memorandum RM-3420-PR*, volume Introduction to distributed communication networks. 1964.

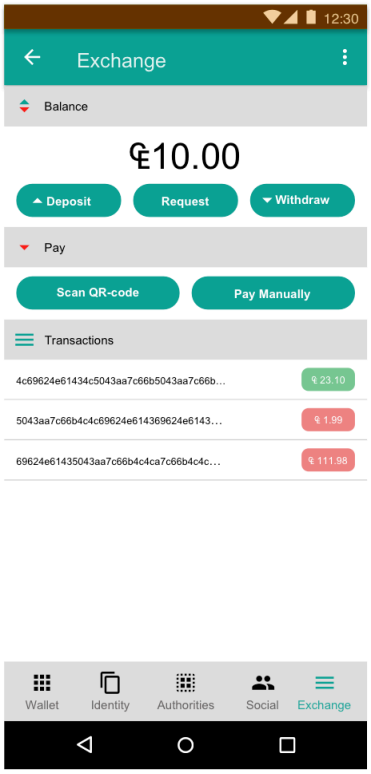
[2] W. Diffie and M. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, 1976. doi: 10.1109/TIT.1976.1055638.

[3] M. Skála. Technology stack for decentralized mobile services. Master's thesis, Delft University of Technology, 2020.

[4] R.W. Blokzijl. A central bank digital currency (cbdc) with offline transfers. Master's thesis, Delft University of Technology, 2021.

[5] R. Chotkan. Industry-grade self-sovereign identity. Master's thesis, Delft University of Technology, 2021.


12:30
Social
New Chat
Show Peers
Chats
Tom:
Great, see you then!
May 3, 2021, 14:31 PM
Mom:
I'll send it in a bit
May 2, 2021, 12:02 PM
Wallet
Identity
Authorities
Social
Exchange


12:30
Exchange
Balance
₲10.00
Deposit
Request
Withdraw
Pay
Scan QR-code
Pay Manually
Transactions
4c69624e61434c5043aa7c66b5043aa7c66b…
₲ 23.10
5043aa7c66b4c4c69624e614369624e6143…
₲ 1.99
69624e61435043aa7c66b4c4ca7c66b4c4c…
₲ 111.98
Wallet
Identity
Authorities
Social
Exchange