Project no. 610349

D-CENT

Decentralised Citizens ENgagement Technologies

Specific Targeted Research Project

Collective Awareness Platforms

D5.5 Implementation of digital social currency infrastructure

Version Number: V1
Lead beneficiary: Dyne
Due Date: 30 Sept 2015
Author(s): Denis Roio, Marco Sachy
Editors and reviewers: Harry Halpin, Robert Bjarnason

Dissemination level:		
PU	Public	**X**
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

Approved by: Francesca Bria

Date: 30 September 2015

This report is currently awaiting approval from the EC and cannot be not considered to be a final version.

Contents

1 Introduction

This deliverable is led by DYNE.org and focuses on the implementation of a software toolkit useful to run community owned infrastructures for the digital social currency design schemes envisioned in D4.4 (Design of digital social currency). Work has been conducted in contact with partner Thoughtworks leading WP5 to share a common set of software technologies, expertise and understanding of the challenges ahead.

While progressing on this software implementation it is important to restate two problems we aim to solve:

- the vulnerability of centralised information systems, whose integrity can be jeopardised by compromising a few points of failure. This problem becomes particularly relevant in our case as we are dealing with systems for monetary credit, value transmission and validation of transaction flows.
- the weakness of validation processes that are operated between different organisations who may not share trust, but need to agree and verify the integrity of a transaction history, being able to recover such data even in absence of the other organisation.

To solve such problems in D-CENT we have decided to investigate on the potential lying beyond blockchain technologies, with less emphasis on purely technical qualities, but seeking an understanding for their functional value within the social practices we have previously analysed in D4.4. In that deliverable we have described in length what a peer-to-peer blockchain is: a distributed and authenticated ledger whose mode of operation is based on decentralized consensus. With this deliverable we aim at offering practical software solutions to implement the advantages offered by this technology in specific conditions.

The reader has to keep in mind that the decentralized technologies we are focusing on are still very experimental and not standardised, while some key implementations are undergoing a remarkable amount of development work by all sorts of interested players, from grass-root communities to major banks and corporations. Our implementation of a toolkit for social currency design is called Freecoin and should be still considered experimental and as such aims to establish a generic blockchain API as a minimum viable product that can allow interfacing with multiple blockchain backends.

API documentation and user-experience testing of Freecoin will happen throughout the project, along with regular releases of the open-source D-CENT code, via the D-CENT account on GitHub. As most other tools in D- CENT, Freecoin is a web-based platform and should work on any device with a web-browser, following a mobile first approach. Testing of the web-facing platform happens over a variety of devices including all major browsers as well as Android and Apple smartphones.

2 Overview of features

Freecoin in brief

FOR: Participatory and democratic organisations
WHO: want to incentivise participation
IS: a set of tools that lets people run a reward scheme that is transparent and auditable to other organisations
UNLIKE: centralised banking databases
IT IS: a social digital currency that is reliable, simple and resilient

2.1 Why a toolkit

While conducting our research on D-CENT pilot communities and projects we did realise that, especially when dealing with value transactions, the needs are very diverse and the software implementations that can satisfy them turn out to be very different from each other, especially on the level of human-machine interaction.

Therefore for our implementation task we aim at developing Freecoin as a toolkit that can deal with a common backend: distributed and authenticated ledgers, like cryptographic blockchains that can be easily adapted to draw interaction patterns that adhere to particular situations. It is important that those projects willing to adopt it are able to familiarize with the toolkit, install and control it directly. Freecoin does not configure itself as a final product, but as means to build final products that can satisfy the needs of specific deployements. It is free and open source.

Other than fostering the bottom-up appropriation and comprehension of technologies, another problem we are trying to address by developing a toolkit is that of the rapidly changing panorama for the backend we are adopting, that of blockchain technologies. The increasing development activities in this field, also previously described in D4.4, end up inhibiting developments and generating a techno-political instability around foundational choices advocated by different factions, with even spectacular clashes (for instance in case of the Bitcoin implementation) between developers, governmental and industrial interests.

Therefore a toolkit like Freecoin aims to be mostly a "middle-ware" placing itself between an ad-hoc customisable layer of interaction and a process of standardisation for backends that is still in-flux and should contemplate multiple options.

Freecoin as a middle-ware

Layer	*Component*	*Interfacing*
Upper	**Restful API**	Organizations & participants
↕	**Freecoin**	↕
Lower	**Blockchain abstraction**	Distributed authenticated ledgers

The top layer in such a middle-ware design is Freecoin's Restful API: organisations can tweak it easily with basic HTML knowledge and HTTP requests to integrate and build interfaces for the participants. The bottom layer is a "protocol" abstraction (a sort of abstract class) which aims to be the lowest common denominator between different blockchain backends and ways to operate them.

In short, the Freecoin toolkit is free and open source software that anyone can use to design an application using patterns for individual or collective access to distributed authenticated ledgers, recording value transactions within small or mid-sized groups of participants. Ledgers exist not only on databases, but also on peer to peer blockchains, with a sort of *peer-validation* of authenticated records that are tamper proof and exist beyond the actual Freecoin installation.

2.2 Basic workflow

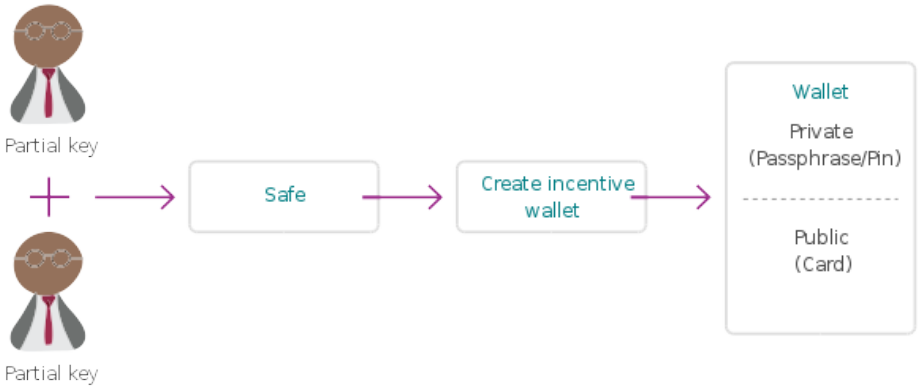
Here we illustrate the basic workflow that Freecoin allows for organisations and participants: generate and award incentive, check balance, exchange and transfer value units.

2.2.1 Create incentive by organization

Application of Social Proof-of-Work in the form of incentives tailor-made for each pilot and assign rewards through multi-signature controlled with commonly agreed upon procedures by pilot managers. This is the first step, and the most important one, where decentralized currency creation takes place.

For instance, each pilot will present its own incentive structure, here summarized by the related Social Proof-of-Work (see the scenarios in Section 3.1, 3.2 and 3.3 below for a qualitative user journey explanation of its potentials):

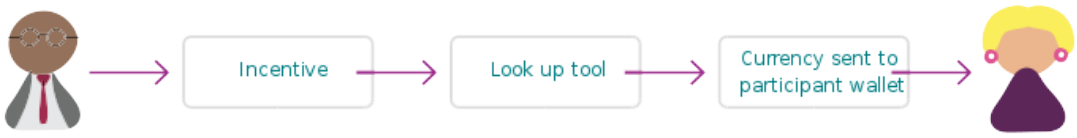
- Iceland: Social Proof-of-Work as Proof-of-Political-Participation
- Spain: Social Proof-of-Work as Proof-of-Business



- Finland/Italy: Social Proof-of-Work as Proof-of-Contribution

2.2.2 Award currency for incentive

Secondly, after the Social Proof-of-Work has been created in the form of incentive(s), i.e. rule(s) of the game, the currency and trust game can start, whereby participants will act in the system and will be rewarded or self-reward themselves according to the Social Proof-of-Work that they have decided to abide to:



Organisations incentivise behaviour by paying participants with rewards which contain an amount of currency set aside for that purpose.

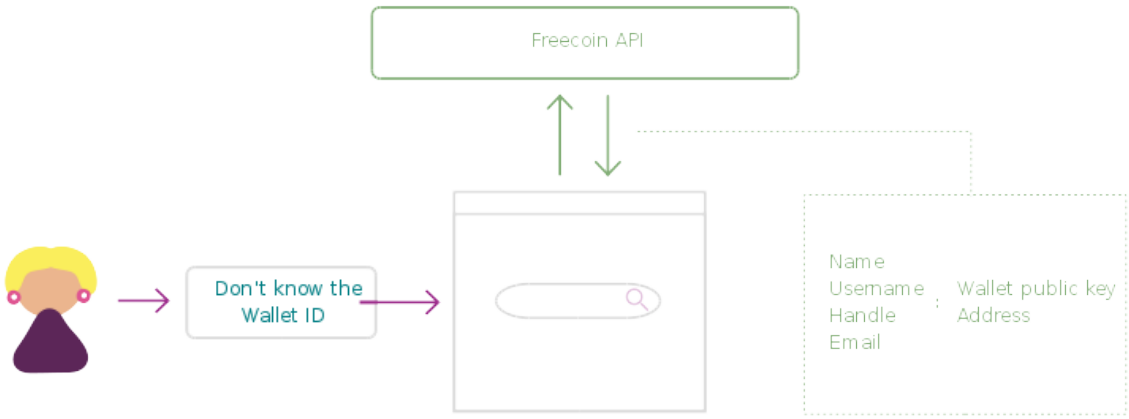
2.2.3 Check balance / audit

After receiving the reward, and as for every crypto-currency wallet, a participant can check the balance of her wallet / audit the Freecoin distributed authenticated ledger of the related pilot which she is taking part in. Here users will enjoy the embedded transparency of that the system allows for.

Participants are able to use a web form to check the amount of currency and history associated with their wallet.

2.2.4 Find other participants

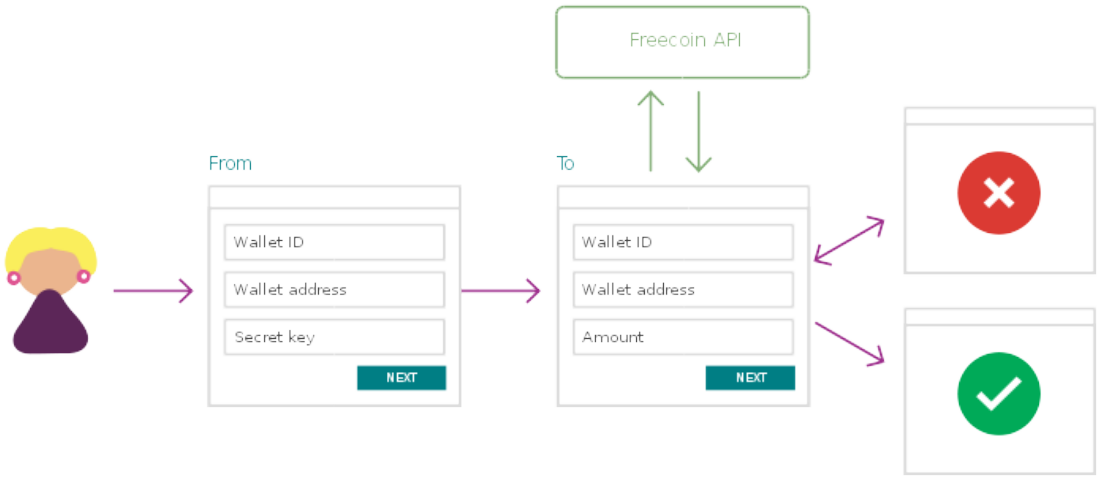
In order to provide efficient currency circulation, together with the instantiation of pilot-specific reciprocity chains, participants will be endowed with the possibility to look up the details of other participants in order to transfer currency / value to them in a bottom-up context.



Participants are able to look up the details of other participants in order to transfer value units to them.

2.2.5 Exchange value units

As a participant finds the data of another member of the same complementary currency community, she can exchange currency and manage her economic relations with others. Here, the Local Multiplier effect will increase in relation to the Velocity of Money that Social Proof-of-Work coupled with the reciprocal interactions in each pilot will allow for. In this step, participants will appreciate the extremely low transactions cost that Freecoin can allow for.



As a participant I want to exchange "freecoins" for other available units of value.

2.3 Web application

Freecoin is a web application since we need to rapidly deploy and operate it without the need of software installations on devices that have to be in the possession of participants. This approach seamlessly extends support for a wide range of computer and mobile platforms, but sacrifices some degrees of cryptographic security.

We need to carefully evaluate this trade-off in the long-term development perspective of Freecoin, but for the time being this is facilitating deployment and testing. The fact that a Rest API is central to the design of Freecoin will make it easier to extend later to ad-hoc mobile applications. To integrate clients capable of high-level "trustless" security (like for instance some Bitcoin wallets) Freecoin should be able to import transactions executed directly on blockchains, or provide a cross-platform native client that acts as the central point of operation between the Freecoin web application and the distributed authenticated ledger.

We consider it premature to implement such a client at this stage: while still researching on the direction that the process of standardisation for distributed authenticated ledger technologies is taking, we prefer experimenting on a platform that can almost seamlessly switch implementations on the server side, without requesting constant updates from participants.

Still, from a security standing point, we observe that this design choice opens a classic attack surface: that of server compromise and man-in-the-middle aimed at spoofing access keys by retaining them when interacting with a participant, because the secret-sharing key join operation is executed on the server side.

For the short and mid-term deployment cycles of Freecoin we intend to address this vulnerability by signing and hashing binary releases of the software, aiming also to implement reproducible builds that can demonstrate the software hasn't been tampered with. Since the software is run on a server, this would not defend a client per se against a server maliciously corrupting the source code. However, we will assume our root of trust is with a community-run server, and deploy standards (such as those from W3C) to defend the user from a server as it matures. If there are multiple non-colluding servers, a malicious server should in theory be detectable if the user notifies honest servers.

2.4 Facilitated integration

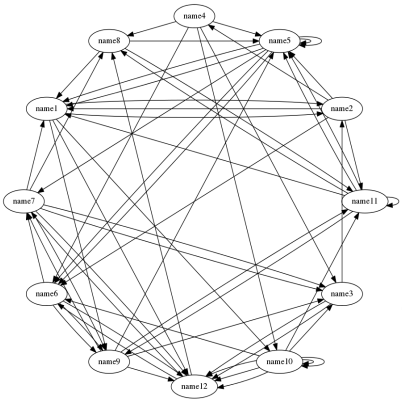
While implementing Freecoin we contemplate the case of existing software suites made to manage mutual credit and complementary currency accounts, to be able to adopt Freecoin as a handy component to issue currency, identify ownership and store transactions on a distributed ledger.

We aim to facilitate existing applications to the point they may simply include Freecoin inside an <*iframe*> html element and interact with it via its Rest API.

On the authentication side we have successfully experimented with OAuth2 support (for instance with Twitter integration) and we are progressing toward OpenID connect support for other D-CENT components as stonecutter and mooncake.

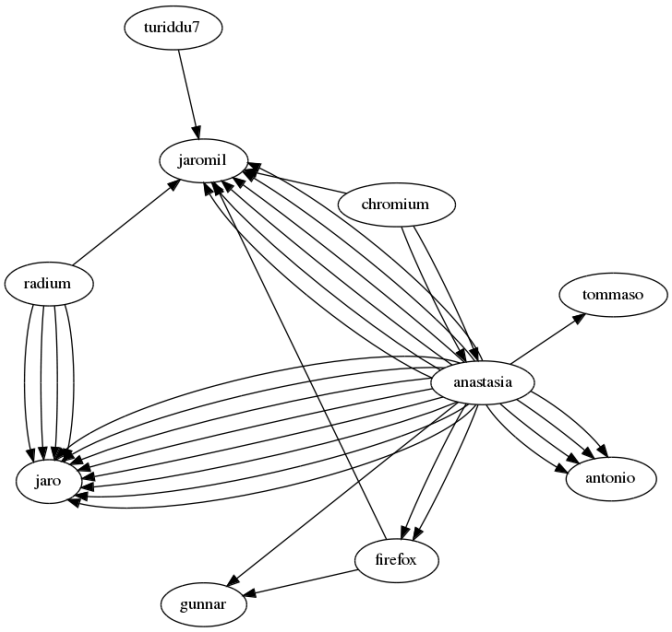
Work on integration will continue for deliverable D5.7.

2.5 Contextual transparency



Freecoin refrains from covering use cases in which anonymity is a requirement and mostly regards transactions as a common history of how resources are allocated and values are circulated. Our approach aims to leverage physical presence, community awareness and reputation, a requirement emerging from various pilots analysed.

The access right to watch how funds are circulated among participants does not need to be highly secure and in fact with blockchain technology the history of transactions is mostly public. Access to the Freecoin ledger and generated network graphs is protected by simple server based authentication, where most transactions are matched to a layer of metadata which is not inscribed to the blockchain.



By accessing the server with a participant account it is possible to visualiae transactions matched to participants' identifications, also browsing and navigating through transactions and visit cards. An external enquiry that has only access to the blockchain then would obtain a map and history of transactions, but still lack the metadata to associate them to actual participant accounts.

Both weighted and unweighted graphing approaches will be applied for visualisations aimed at giving context awareness using the volume and frequency of value transactions.

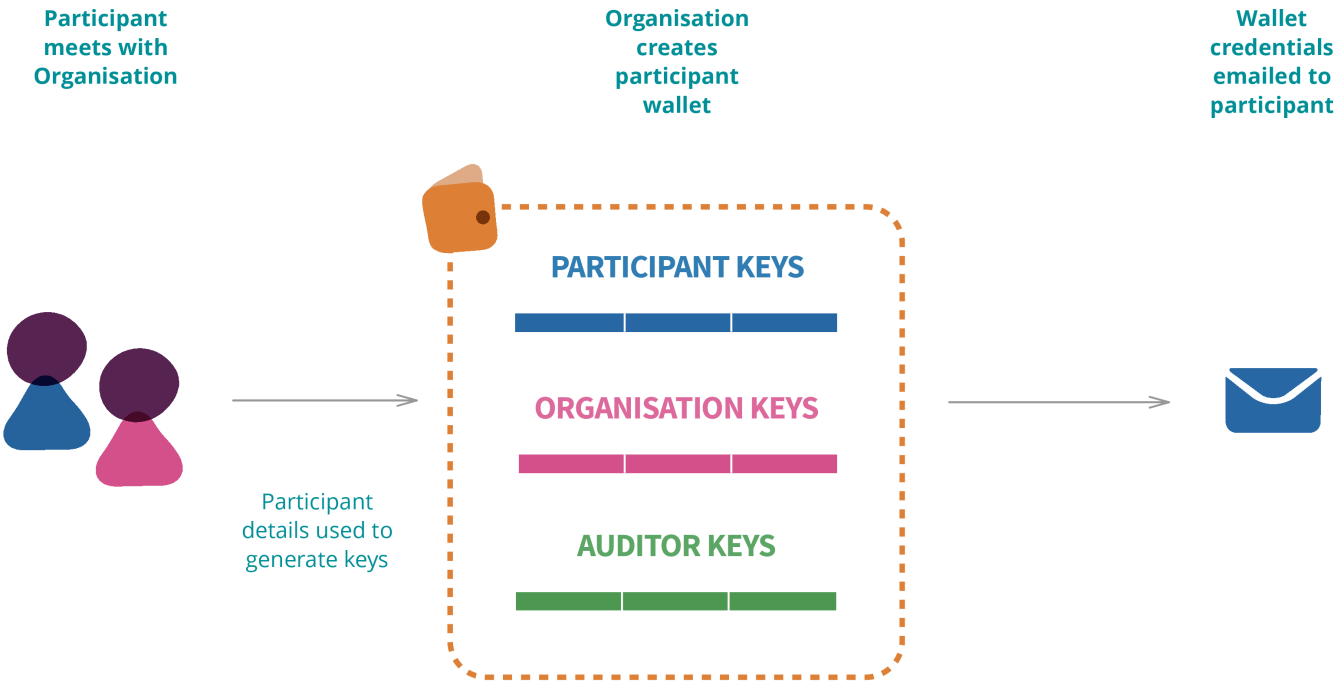
2.6 Shared secret authentication

Shared secret authentication is a core feature of Freecoin, allowing to adapt its security model to various situations. We will explain here the mode of usage and later on in section 6 how this is cryptographically implemented.

As previously mentioned in 2.5 the access to transaction history does not require critical security measures for the sort of use-cases Freecoin is focusing on, but still the actual possibility to make transactions and transfer values (wallet operations) must be well guarded.

We must be able to avoid the case in which a server may be compromised and with it the credentials of all participants, as well grant the fact that the access to a wallet requires keys that are not in unique possession of an organisation and/or a participant, but also an auditor which may require access to wallets with the consensus of at least another party.

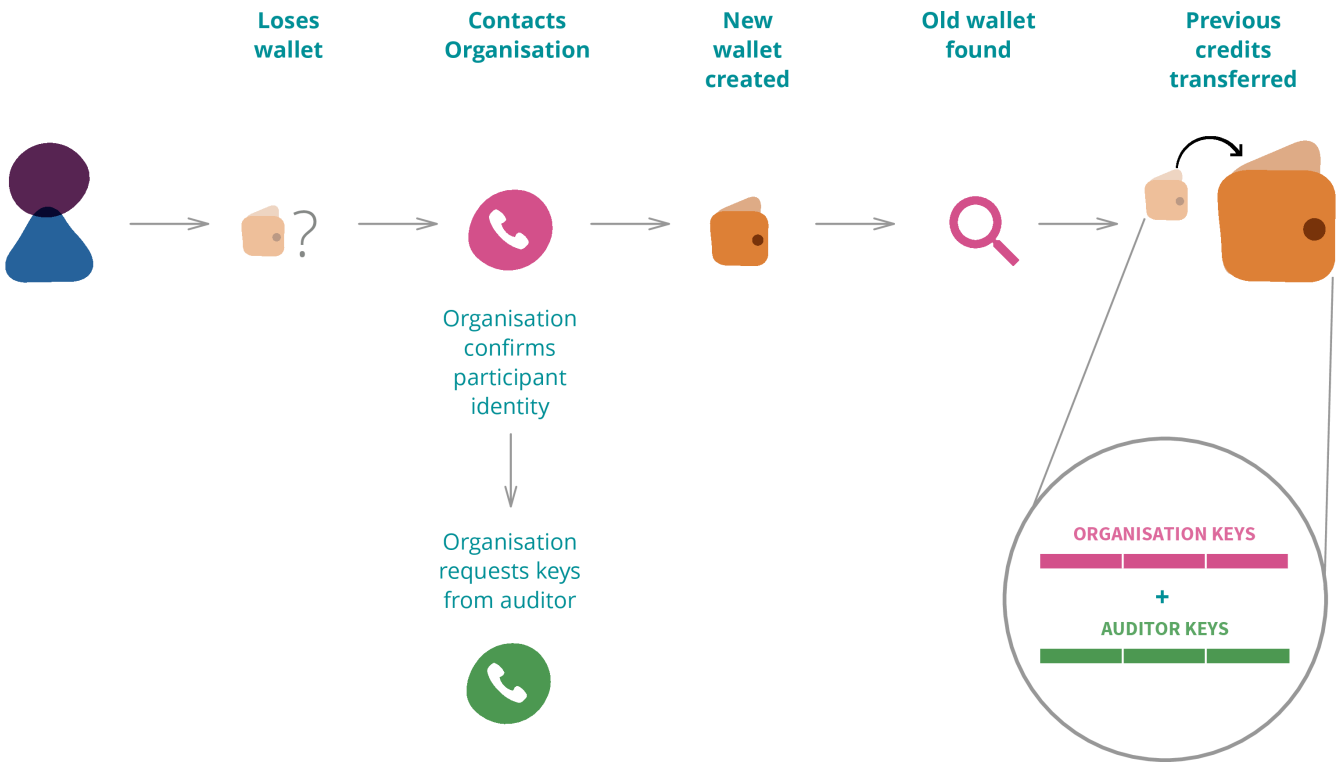
This is all necessary if we want to decentralize and avoid a single point of failure, but also if we want to avoid that when a minting organisation disappears all the value system created vanishes. While implementing such redundancy, we still want to be sure that the auditor organisation is not able to access the wallets of participants without their consent, or the consent of the minting organisation.



In Freecoin we implement a solution to this problem by using a cryptographic algorithm that breaks in 3 parts the key to access a wallet. Every time a wallet is created, the key to access it can be split in three different parts and at least two of these parts need to be joined in order to access a wallet. Therefore the participant may be able to access its wallet either by interacting with the organisation or with the auditor, as well an auditor is able to access wallets by either interacting with the participant or with the minting organisation.

This cryptographic scheme for keys satisfies an important requirement for the use-case of EUROCAT in Catalunya, a Commercial Credit Circuit project that expressed many difficulties in dealing with blockchain technologies when it cannot be possible for the minting organisation and an auditor to intervene on participants wallets, for instance in case of fraud or insolvency.

Finally, in case a participant loses the keys to the wallet nothing is lost, but the organisation will need to contact the auditor in order to access the old wallet and transfer its funds to a new one.



The organisation will then need to identify the participant (it may well happen in person, as required by a specific context and with the main goal of avoiding impersonation), create a new wallet, ask the auditor's keys to access the old wallet and then transfer the funds to the new wallet. This is done so because there is no way to retrieve keys that are lost: we then rely on the fact that different pieces of the key are in custody at different places. Similarly a participant may have access to the wallet by contacting the auditor, even if the organisation loses its key database.

2.7 Off-line transactions

In most existing complementary currency and credit circuits that we observed most of the value circulation activity is operated off-line. With its growing complexity digital technologies can even play a counter-productive role for the wide adoption of an economic circuit, especially when raising the requirements on devices to be owned, like smartphones or personal computers. For these reasons we pay particular attention to the possibility to create off-line transactions: vouchers that can be printed from Freecoin and contain cryptographically authenticated units of value which can be then also redeemed via Freecoin. Using QRcodes, a sort of advanced bar-code system to store information, one can spend funds into printed vouchers that are transferred by physical possession and can be redeemed with the simple use of a webcam or a smartphone.

2.9 Free software licensing

The license adopted in Freecoin is the Affero GNU General Public License version 3 and any later version, while some of its dependencies are licensed the same as Clojure: Eclipse Public *License* 1.0.

The AGPLv3+ licensing scheme that we adopt allows any use, be it commercial or non-commercial, of this software, with the only condition of providing its sourcecode in any case, be it modified or not. We are confident this model can protect this work from being appropriated, while keeping it free and open to exploitation also in business cases.

The motivation in releasing this software as free is primarily ethical: we believe that this is the way we can really contribute value back into the public, as a result of a public funded research. We also believe that the particular conditions contemplated by the AGPLv3+ are well fit to create the sort of commons economy even among commercial initiatives adopting this software entirely or in part.

The Dyne.org foundation, main partner responsible for this deliverable, has strong commitment in maintaining Freecoin beyond the time span of the D-CENT project and will maintain and integrate valid contributions to its sourcecode. Here below we report the explanation of this license given by its authors at the GNU Project:

The GNU Affero General Public License is a free, copyleft license for software and other kinds of works, specifically designed to ensure cooperation with the community in the case of network server software.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, our General Public Licenses are intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

Developers that use General Public Licenses protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License which gives you legal permission to copy, distribute and/or modify the software.

A secondary benefit of defending all users' freedom is that improvements made in alternate versions of the program, if they receive widespread use and become available for other developers to incorporate. Many developers of free software are heartened and encouraged by the resulting cooperation. However, in the case of software used on network servers, this result may fail to come about. The GNU General Public License permits making a modified version and letting the public access it on a server without ever releasing its source code to the public.

The GNU Affero General Public License is designed specifically to ensure that, in such cases, the modified source code becomes available to the community. It requires the operator of a network server to provide the source code of the modified version running there to the users of that server. Therefore, public use of a modified version, on a publicly accessible server, gives the public access to the source code of the modified version.

An older license, called the Affero General Public License and published by Affero, was designed to accomplish similar goals. This is a different license, not a version of the Affero GPL, but Affero has released a new version of the Affero GPL which permits relicensing under this license.

The precise terms and conditions for copying, distribution and modification are found on their website http://www.gnu.org/licenses/agpl-3.0.html .

3. User research

As for what happens in the Direct Democracy track of the D-CENT project, the full Freecoin prototype will be a backend codebase that will allow to distribute, in a decentralized fashion, the collection and storage of the append-only log of democratic decisions, i.e. the economic "collective memory". This will be one of the first bottom-up examples of trust management as an open-source social service that will defend communities from the drawbacks of centralised solutions: single point of trust and single point of failure. Our belief is that can be best done with participatory design and by virtue of free and open software ethics.

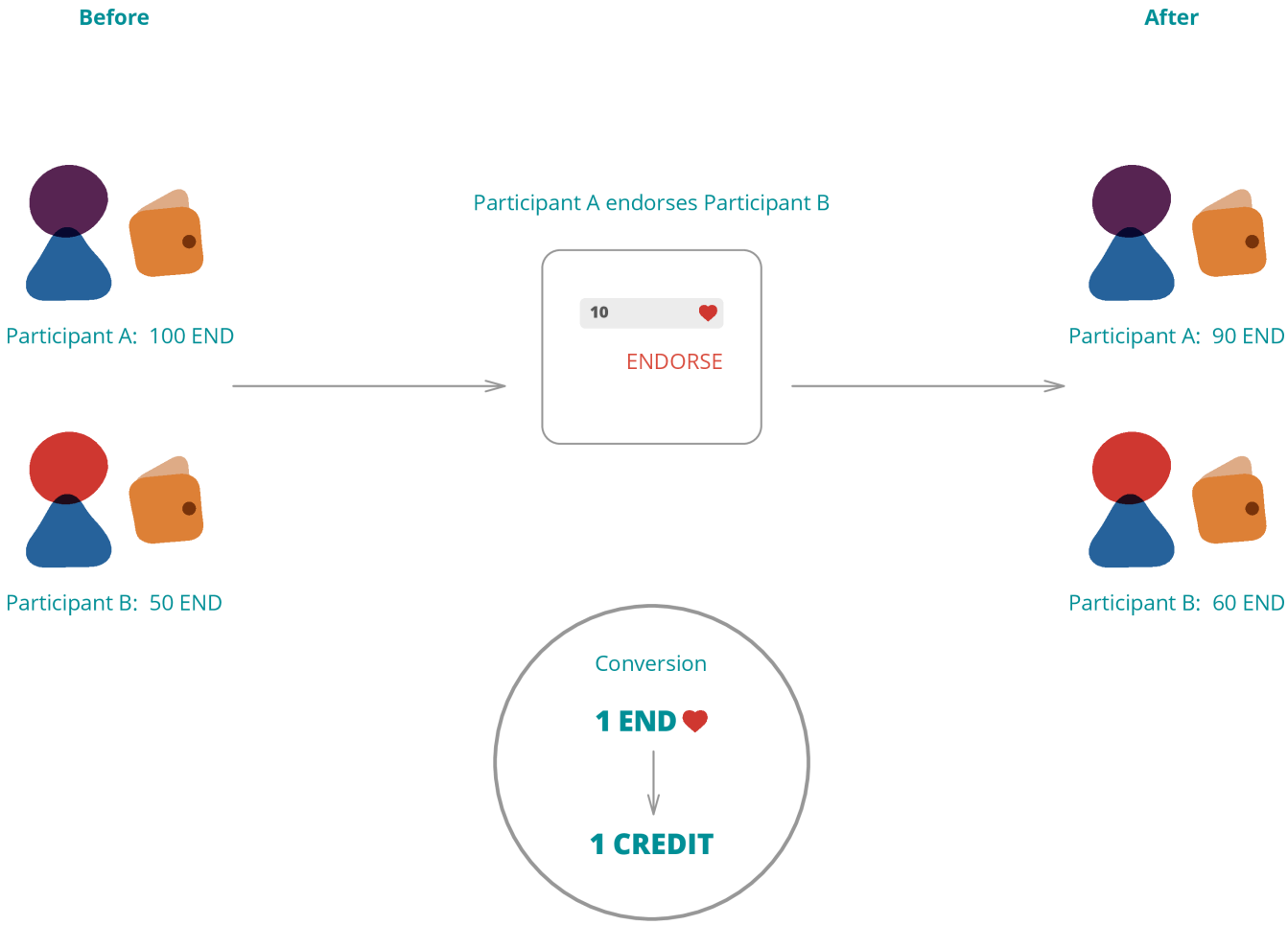
Moreover, within the dynamics of the D-CENT Digital Social Currency pilots, the deconstructed versions of the blockchian technologies that the flexible design patterns of Freecoin allow for will be tested in order to ascertain whether and to what extent communities can autonomously run and participate into those decentralized complementary currency schemes that have been designed and detailed in D4.4/Annex I: a political-participation reward system for Iceland (Social Kronas); the storage of a data commons for a regional complementary currency in Spain (Eurocat); and an innovative social remuneration mechanism for Finland (Helsinki Urban-Cooperative Farm) and Italy (Macao).

During autumn 2015, the D-CENT consortium will organise specifically targeted technical Freecoin Workshop to organise prototype testing and roll out the pilots in concrete. The general rationale for each Freecoin workshop is to select a Pilot Management Team for each D-CENT digital social currency implementation, whose function will be to interact with relevant stakeholders and make decisions about role subdivision in terms of initial participants' number, organisations' managers and auditors of the pilot systems with the respective facilities to store Freecoin keys.

Another important part of the Freecoin worshops will be to provide technical training and information on the systems while monitoring progress toward the finalised minimum viable product. In particular, alongside organisations managers of this systems, each relevant D-CENT Consortium partner needs to offer technical personnel to have some overview and synergy with technical personnel of the various organizations involved in the pilots on the field in Iceland, Spain, Finland and the use case in Italy. Accordingly, Dyne will remain the main facilitator of the process, Dyne will be ready to collect feedback and motivated to continue development of Freecoin and port it to more hardware platforms and support other FXC protocol implementations.

Finally, the workshop will provide documentation and guidelines needed to kickstart the systems: by invitation (or creation), pilot participants are going to be involved to start prototype testing, i.e. creating a wallet from the web service on their browser and start interactions with other participants and the distributed trust management system as a whole as it is addressed to organizations who want to incentivize members participation in an open and transparent socio-economic framework.

In both Iceland (section 3.1) and Spain (section 3.2) the Freecoin will allow to bootstrap and test prototypes that follow a common scheme, as for the figure below:



In effect, in both cases participants will be able to give and receive trust, i.e. endorse or be endorsed, on a common platform shared by other participants. On the one side of the coin, Spanish small and medium sized enterprises will be able to initiate a distributed web of trust potentially covering the region of Catalunya to increase commercial liquidity through a form of social control of credit, i.e. the micro-endorsement and mutual credit Eurocat system. On the other, subscribers of the Your Priority software will be able to take part to the participatory budgeting event at the City of Reykjavik, vote best ideas proposed by peers, who will gain social credits representing their reputations. These social credits representing participants' reputation will in turn become social kronas, a currency that they will be able to spend in the socio-economy of the Icelandic municipality. In both cases, trust management will take place in a decentralized fashion and value will circulate on a distributed ledger giving to these communities more built-in transparency and resilience to count on.

Hence, in the following two sections we present user journeys resulting from an educated approach to how implementation may result in these two pilots at the light of the design effort made in WP3 and WP4 and the codebase prototype developed in WP5.

3.1 Iceland – Freecoin Pilot Implementation

Magnus Reifnir is a young member of the Your Priorities platform. He works in the fish industry, spending a good part of each day sailing on the trawler. Every day, his lunch break includes the reading of Your Priorities RSS feed in order to see what are the latest news from the movement. While working in the high sea with his sailor mates, conversations usually rank between the last news in sports and the next political controversy affecting the national and international landscapes. In case the sailing day brings about a political issue, Magnus likes to discuss with his mates and captain about the ping pong politics among left and right, trying to let them understand how a majority guided by the Icelandic Pirate Party - the second political force as for March 2015 - could indeed represent a game changer moment for the life of the nation. When faced with the sarcastic comments of the white-beard captain, Mr. Gottschalk, about the impossibility to have an ordered democracy "if everybody had a voice in the political arena of the nation", while stacking yet another box of fish just decked from the net, Magnus stubbornly replies that it is only a question of time when we will reach a transparent direct democracy in which each voice will have a weight in the policymaking process.

Magnus is also a member of Betri Reykjavik and takes part in the participatory budgeting annual event as it is one of the rare occasions when he feels "really empowered and free to decide", to have a voice at the executive level of the political system. During the days of participatory budgeting, Magnus proposes a few ideas for the betterment of his neighborhood and the city as a whole: in 2015 he proposed to fix a metal ladder that allows access the beach nearby the dock where he banks everyday coming back from work. He got two thousand Your Priorities members voting in favor, i.e. allocating city budget resources for fixing the metal ladder. Today, it is indeed easy to see kids playing on the beach or people jogging or walking their dogs as it is now easier to access the sands. Those two thousand votes are then used to rate Magnus reputation on Your Priorities platform. On Your Priorities, members call them, 'social credits': the more the good ideas, the more one gets voted, thus increasing one's reputation based on the betterment of the common good of Reykjavik civil society. Magnus is very glad about his two thousand social credits, and he likes to recall them when he speaks with peers about the next proposals for the participatory budgeting event, while drinking a beer after work.

Also that day, it is again time for a break in the middle of the work shift. Magnus takes his backpack and picks up his smartphone, and his lunch box. It is the end of March 2016, the day is fresh and there is a briskly breeze, and also some sun. Magnus seats to rest for 20 mins as usual after his lunch for reading the Your Priorities RSS feed, while drinking a black coffee. There is the announcement of the next participatory budgeting event and Magnus is ready with a few proposals for this year. He will upload them from his PC at home that very night in order to increase the chances to be voted by Your Priorities members who may like them. Scrolling down, the next message of the Your Priorities RSS feed makes Magnus almost jumping on his seat with the risk to spill the coffee on his smartphone screen. The message object reads: "Social Kronas - When Your Priorities reputation becomes real money".

Magnus reads and quickly understands that Your Priorities will launch a new scheme on the platform where a member's reputation will be converted in Kronas (10 social credits for 1 krona) and it will be possible to enjoy some categories of goods and services around the city and within the larger metropolitan area administered by Reykjavik City Hall. The scheme will pilot initially with a digital

wallet embedded into the very widespread app (he also uses it) of the Municipal Bus Company (http://www.straeto.is/app). Magnus reads again, but he thinks there are no mistakes: his good idea about fixing the metal ladder transformed in the possibility to have free rides on the local bus network. For Magnus, this means free transportation for the value of 200 kronas (as he got 2000 votes from peers last year) that will expire in one year, until the next participatory budgeting event.

Magnus is thrilled by the idea that bettering the common good of Reykjavik could mean free transportation in his very city and homeland. However, he knows that he had earned the ride with the time that he spent actively participating on Your Priorities, time dedicated to the common good. The bell announces that the break is over. Magnus goes back to work fantasising about the new proposals for the participatory budgeting event in 2016 and the possible economic advantages that he would get thanks to an increase in his political reputation. Back to the fish boxes, Magnus starts to narrate to Mr.Gottschalk about the new service provided by Your Priorities. At the end of the tale, Mr. Gottschalk ask Magnus how to take part to the next participatory budgeting event and start earning Social Kronas, as also Mr. Gottschalk has one idea or two for the betterment of Reykjavik's roads, parks and pools.

3.2 Spain – Freecoin Pilot Implementation

In a general scenario case, to access credit, Company X (or just 'X') must fulfil the following prerequisites:

a) having a fiscal address in Catalunya

b) accessing with digital signage (the government's)

c) having a positive turnover the previous year registered in the mercantile Registry.

d) having received the first endorsement

EMC audits Company X, a medium sized Catalan retail company, and fixes its credit ceiling at 30% of its previous year turnover, i.e. c). In practice, if the turnover of Company X is 100k EUR, then the company can give to and receive UT from other companies for a maximum of 35k EUC. After the audit, company X gets into the Eurocat mutual credit game and receives a percentage of the figure in c), for example 35k but not in Eurocats (EUC).The trust that endorsements entail will be measured in UT (which are not good to spend, only to endorse). Then, for each END (UT both received and given), X gets a EUC in his Eurocat Trust Capital account. The END would be just a public notice that everyone can see, and that a complementary currency payment system would need to copy for the concrete issuance and circulation of EUC. In other words, Freecoin will focus on the trust management aspect of the Eurocat system, i.e. on the management of UT and END. While EUC will be managed with a traditional software for mutual credit systems, either Integral CES or Drupal 8.

It is worth noticing here that on the one hand, the credit ceiling is the maximum credit limit that a company can petition for in the Eurocat network in order to receive endorsements from other member companies.Therefore, the credit ceiling is the maximum level of debt that a company can demand the system (other companies) to bear by receiving correlative and equivalent endorsements. On the other hand, the credit ceiling is the maximum trust that a company can give to endorse other companies. '35% of a company's annual turnover' (35kT) is the parameter that defines the upper limit/benchmark for endorsements (and max overdraft). 35kT is the credit ceiling for each company in the network. The credit limit is the lesser among: (1) Endorsements received; (2) Endorsement provided; (3) Company's credit ceiling.

In particular, it is after the audit by the Eurocat Management Committee and a cross-check with the Mercantile Registry database that Company X can bid for receiving endorsements from other member companies, for example Companies S and T, wholesalers of electronics and machinery. Once S and T decide to trust X, i.e. to endorse X for 20k EUC and 5k EUC, respectively, UT exchanged will be mirrored by a correspondent amount of EUC in both Company X and S & T accounts (END). EUC thus issued for productive purposes within the regional construction sector will allow all three companies to inter-trade among themselves and other member companies within the regional economy of Catalunya.

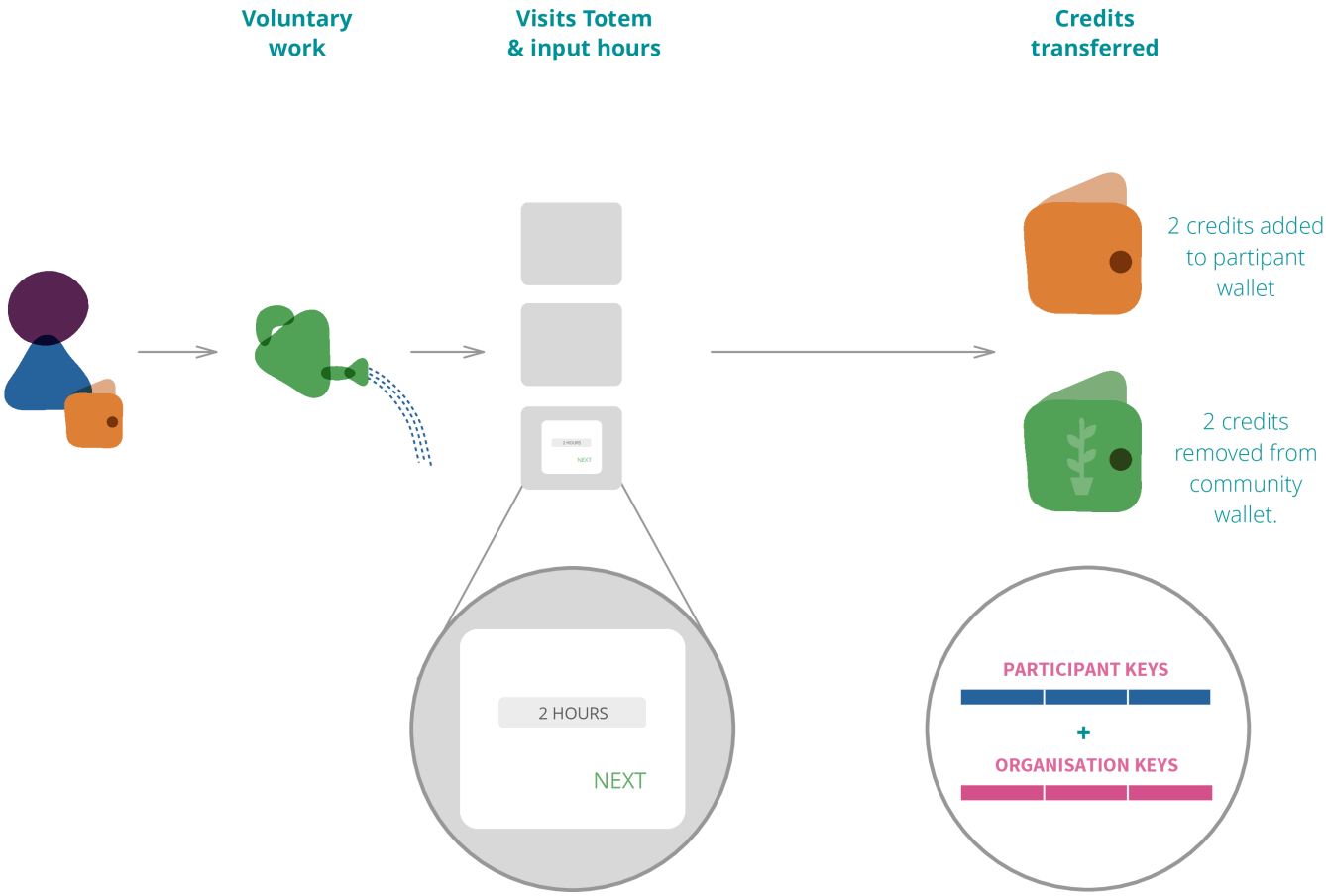
The fundamental point here is the following: when S is being assigned UT by the Eurocat Management Committee, S is really empowered to decide to give (or refuse) trust in the form of endorsements to X, creating the ENDs that will become EUC. UT are not currency per se (that is, EUC) at this stage: S is dealing with trust, is empowered to exchange trust creating the pairs of endorsements.(END), which can be counted in EUC as Company S decides to tolerate risk and exposes to X for 20k EUC. In this view, endorsements can be thought of as the collateral backing the Eurocat currency. All three companies will see their web of trust on a transparent and decentralized public ledger, where trust as a common good will be represented in terms of economic relations among members.

Endorsements (exchanged units of trust) become currency (a means of payment backed by trust) after END are in Company X's trust capital account and then converted as EUC on the system that manages the complementary currency. Conversely, X can endorse, for example Company Z, only after Z bids to X for receiving UT, that is X will exchange UT according to its own credit limits and, however, respecting the ceiling. Indeed, the system managing END will only be the source of the money supply in the descending complementary currency system. In effect, central banks power money by vertical fiat while Eurocat members do so with horizontal trust. The important point here is that the act of issuance, the act subsequent to the acceptance to provide endorsement (pushing a button on a screen or keyboard), to tolerate risk, is the equivalent of the signature on a paper mortgage contract one asks for a loan to buy a house. The mechanism is the same, while the architecture is flat in case and vertical in the other. In brief, in the context of the Catalan SME sector, Company X is producing goods and services for the market already and receives endorsements according to its turnover. When this company gives and receives endorsements to and from other companies, it gets the EUC.

As we saw above, UT can be withdrawn (END undone) and the system must reflect the new balance in the EUC accounts of both companies. In practice, endorsing means that both trustor and trustee receive EUC, but in case the trustor withdrew the endorsement (for example, toward the end of the quarter), this would reflect a loss on both sides EUC accounts. That is, when a company withdraws endorsements, the corresponding EUC disappear, for both companies, but the company who withdrew the endorsements, e.g. if Company S withdraws UT from Company X, S gets UT back while X loses them. If Company S gives the UT in endorsements again, then both get the EUC again. The other Company X is free to receive UT in endorsements from a different company and if this happens Company X would also get the EUC again (if nothing else changes).

3.3 Finland – Freecoin Pilot Implementation

In the case of Finland and Macao the basic implementation scheme is different than the one for Iceland and Spain. The following figure presents the basic scheme grounding implementation in the Finnish Pilot and the use-case in Milan:



In this case, experimentation regards the study of trust management dynamics within a community that allows its participants to self-remunerate themselves. Indeed, members of Helsinki Urban Cooperative Farm (or Macao's cultural workers) perform voluntary work. After a working session, they can remunerate their own work by interacting with a Freecoin 'Totem installation': a terminal that will handle transactions from the 'community wallet' to participants' ones, thus dis-intermediating administrative tasks and simultaneously testing trust and distrust relationships between the participants and the community together with the common reserve of digital currency to which everybody can have access to. It is worth noticing here that every participant will have a backup copy of the community wallet, which is therefore not a mere central point from which acquiring remuneration.

Scenario

Rikka is an interior designer that is waiting for a new contract to start as her former company will finish the merger procedures with American and Japanese counterparts. Riika is also a new young member of Helsinki Urban Co-operative Farm. Rikka is quite proud of her socially sustainable lifestyle. She discovered the community supported agriculture project as on a Saturday morning last December she saw a point of sale of harvested products at Helsinki Public Library. It is the end of April and she is finally able to take part to the various field activities of the cooperative, esp. cultivating various vegetables in the common allotment.

As the summer advances Rikka likes to spend more and more time at the allotment, where she sees the work in the field also as an open air fitness activity waiting for the harvest and the hard season. She enjoys distributing flyers around Helsinki bars and to the concerts she attends in town (and in other Finnish cities). Further, she sometimes manages the cooperative's selling point at the Helsinki Public Library, usually for 6 hours twice a month. She is very interested in the overall message that the Helsinki Urban Co-operative Farm shares with members and allows them to experience a new sense of community in their neighborhood. Rikka is in fact enthusiastic about the 'currency' application that Helsinki Urban Co-operative Farm website offers.

Since she puts a lot of work and dedication into the common interest of building a good community supported agriculture in the city, she likes that the organiaers proposed a system for tracking members contributions (in hours of time, thus rather intuitively). She is sure that all the value that she puts will be mirrored in her cooperative's wallet where she receives digital tokens from a 'common account', as everybody refers to the Helsinki Urban Co-operative Farm Escrow Wallet. Therefore, Rikka finds it very empowering to be part of this social experimentation in trust building, measurement and translation into currency.

However, she finds very engaging and sometimes conceptually demanding a second aspect of the social currency that members at Helsinki Urban Co-operative Farm use to pay each other for goods and services based on time. This second aspect is the one that Rikka sometimes, especially when she is involved into transactions with euros, finds more unnerving: the fact that all members at the cooperative have in their wallets a backup of the total amount of the tokens parked in the 'common account', the one from which everybody is paid. While thinking about her job as interior designer or as she speaks with her husband about his business issues, she considers how the economy would be if everybody could carry the entire current account of a nation state in a digital wallet on everyone's smartphone, laptop or similar device.

Rikka knows that the currency at Helsinki Urban Co-operative Farm works because everybody trusts everybody else (for everybody knows each other). Moreover, everybody can access the full transaction history of the network and analyse it, thus spotting free-riders who credit their wallets unduly, thus breaching the honesty rule. In effect, up till now, nobody abused the Helsinki Urban Co-operative Farm Escrow Wallet, and nobody signaled unusual changes in the balance of the wallet that everybody has backed up on one's personal member wallet. But tools are there to explore the transaction history in order to spot irregularities in a transparent and public way. Who pays his wallet from the cooperative's Common Escrow Wallet - the Freecoin Totem - an amount that exceeds one's real contribution will see his wallet banned by the totem with an almost irreparable loss of reputation (who would tolerate risk to have business with somebody that abused the Escrow Wallet?). Apart from a joke by two youngsters who transferred from their mother's device (the password was their first names) a few million tokens for a bill of just 5 mins of work and restituted

them in 15 mins, from April to September no abuses were registered on the public transaction history of the Multapakku system for Helsinki Urban Co-operative Farm.

Rikka will start working again in just a month. She will continue to participate actively into Helsinki Urban Co-operative Farm, since she wants to gain more Multapakku and spend them inside the marketplace of the cooperative where members post offers and wants. She would like that the currency be successful for six months consecutively, i.e. that no abuses on the Helsinki Urban Co-operative Farm Escrow Wallet happen by users who self-pay their contributions to the cooperative. This would help say much about trust among humans. And it is funny to think about that as Rikka often recalls the Multapakku slogan: "You work; you pay yourself for the work done from a common pot of money that everybody carries around. And if you steal, you literally steal from everybody's wallet."

4. Overview of APIs

Design of the API is sharing flows and standardization ambitions with the UETP initiative by Focafet and struggling to establish a pattern language for interacting with blockchains, taking as a first development target NXT (second genaration blockchain).

4.1 Public API (Restful)

The REST API of Freecoin is designed to provide interaction to external applications, facilitating read/write operations on the blockchains supported.

The API is being designed to provide both programmatic endpoints (JSON) and a simple web application interface to facilitate a quick integration via <iframe> into bigger applications.

Freecoin's API is still being developed and may be subject to changes as we progress our testing on pilots, here is presented a basic outline of its most important endpoints.
Balance

- Participants
- GET /participants
- GET /participants/all
- GET /participants/find?
- GET /participants/:name
- GET /participants/:name/qrcode

- Sending
- GET /send/:participant/:amount
- POST /send

- Vouchers
- GET /voucher/create/:amount
- POST /voucher/create
- GET /voucher/claim/:voucher-id
- POST /voucher/claim

In addition to the Freecoin API it is also provided an "application protocol bridge" mapping one to one the API of supported blockchains. For instance it is possible to call the underlying NXT API using /nxt/* endpoints, which can also be selectively enabled. Also thanks to Clojure's simplicity and performance when serving concurrent calls, Freecoin's code is extremely malleable for such uses.

4.2 Internal blockchain abstraction

An important outcome of the research behind Freecoin is the abstraction of a generic blockchain API, a sort of lowest common denominator for the interaction with most blockchains. The blockchain abstraction is a sort of polymorphic class (implemented as a protocol in Clojure) that declares the methods to be implemented by any blockchain support built in Freecoin.

```
(defprotocol Blockchain
  ;; account
  (import-account [account-id secret])
  (create-account [account-id])

  (get-address [account-id])
  (get-balance [account-id])

  ;; transactions
  (list-transactions [account-id])
  (get-transaction   [account-id txid])
  (make-transaction  [account-id amount recipient secret])

  ;; vouchers
  (create-voucher [account-id amount expiration secret])
  (redeem-voucher [account-id voucher])
  )
```

The main implementation present in Freecoin is NXT, as that provides a stable API for the "monetary system" function that easily allows one to issue a new crypto-currency. While the support for implementations are planned in future (mostly to use Bitcoin based alt-coins, but also sidechains and smart contracts) this abstract approach to the blockchain API will allow Freecoin to leave all the layer of user-interaction untouched while switching the blockchain backend.

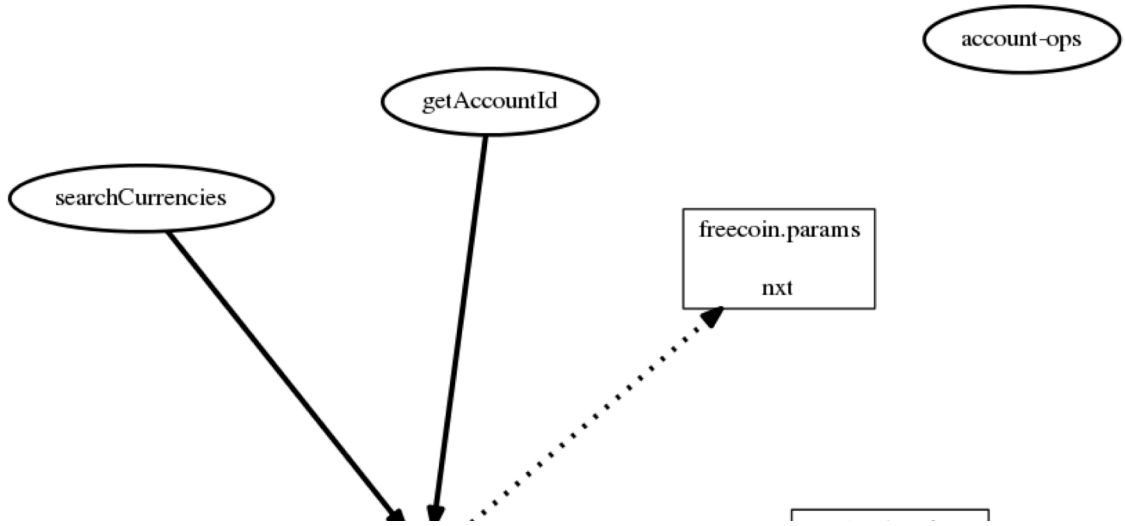


Figure 1: Function call graph for the current NXT API bridge

4.3 Internal transaction and wallet API

The wallet data structure contains:

- simple fields as a unique id, name and email.
- a low-security public/private key pair for off-the-blockchain asymmetric encryption operations, which may be useful to operate on the server and between participants.
- an array of blockchains known to this wallet, indexing clojure protocol implementations
- an array of blockchain secrets, basically consisting of the known secret-sharing splices

```
{:_id ""            ;; unique id for internal use
 :name  name        ;; identifier, case insensitive, space counts
 :email email       ;; verified email account
 :info  nil         ;; misc information text on the account
 :creation-date nil ;; date on which the wallet was created
 :last-login    nil ;; last time this participant logged in succesfully
 :last-login-ip nil ;; connection ip address of the last succesful login
 :public-key    nil ;; public asymmetric key for off-the-blockchain encryption
 :private-key   nil ;; private asymmetric key for off-the-blockchain encryption
 :blockchains {}        ;; list of blockchains and public account ids
 :blockchain-keys {}}) ;; list of keys for private blockchain operations
```

The presence of last-login information hints about methods we apply as connection throttling, to avoid brute-forcing of access codes. This internal wallet structure may be subject to small changes in future.

Voucher

Vouchers are transactions that can be printed and authenticated back and forth between the physical and digital domain. As such vouchers do not require any authentication to be spent, but they are rather anonymous and to be transferred is enough to transfer their possession and eventually redeem them.

```
(defrecord voucher
  [_id
   expiration
   sender
   amount
   blockchain
   currency])
```

The creation of vouchers in Freecoin serves various purposes, the most obvious and bound to currency use is that in which one can carry value without any device, knowing that at the other end is enough to scan the QRcode or BARcode on the voucher to redeem it and have the value transferred on the recipient account.

The less obvious, yet very functional use is that of releasing vouchers from a particular account that is not bound to a person, but to an event. This way the voucher can function as a voting certificate, for instance, in a ballot in which the number of voters is established beforehand and in which the identity of voters can be kept confidential and in any case established off-line in ad-hoc ways by humans upon presentation of the voucher.

Another use of vouchers can be that of entrance tickets for events, where the verification can be simply operated using a PC connected webcam or a smartphone scanning the voucher and redeeming it: the correct reception of a unit of currency can confirm the validity of the ticket.

Vouchers are seen as a basic functionality in Freecoin, while their implementation is still being studied in relation to various types of blockchain that may or may not be adopted as backends. In considering Freecoin as a toolkit we expect to be able to adapt and customise Freecoin to fit particular needs as the scenarios described above and even beyond the mere application of issuing currency, but that of issuing authentication tokens that are bound to the carrier rather than to a registered identity into the system.

Transaction

Transactions are defined in a minimal way and will be also implemented as activitystreams events to be emitted as they occur and consumed by the Mooncake project. In Freecoin transactions are stored as server-based metadata (easy to export to csv, json and other formats) as well in configured blockchains (our LEAN experiment phase is focusing on the NXT MS for now).

Here a sketch of the internal data representation for a transaction emission unit:

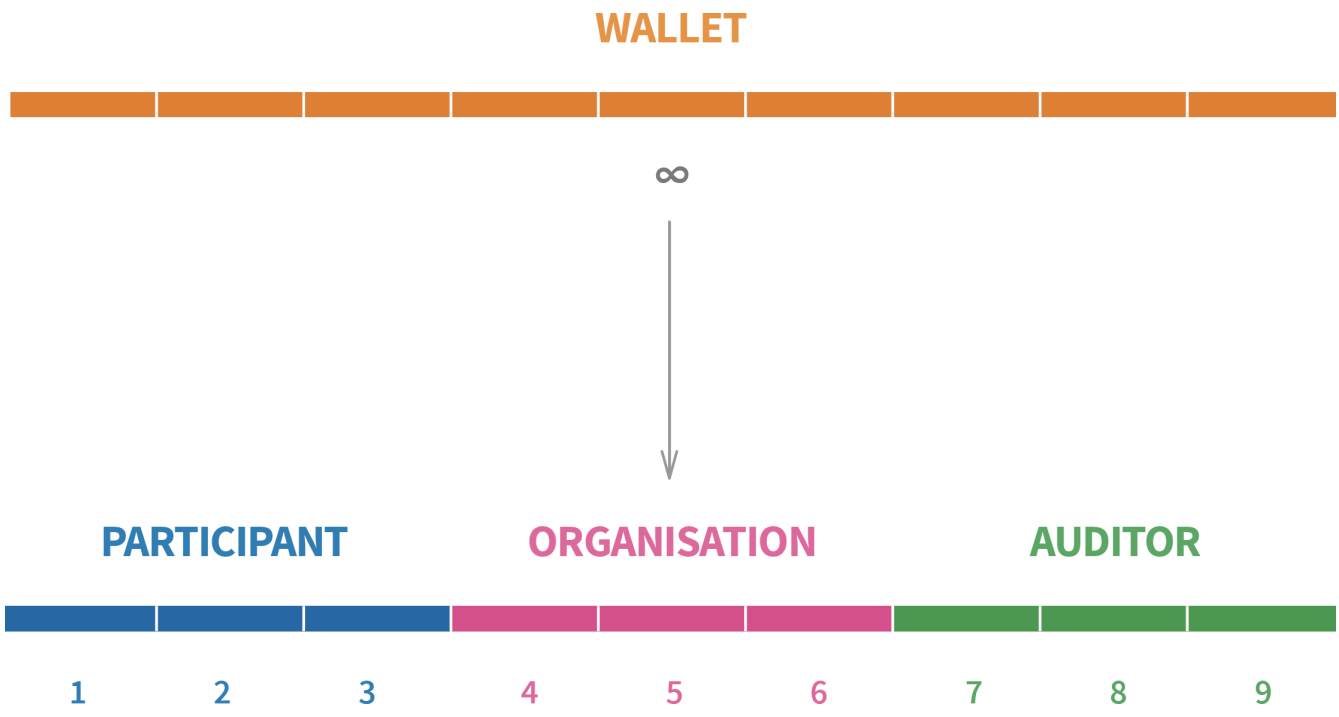
```
(defrecord transaction
  [_id
   emission
   broadcast
   signed
   sender
   amount
   recipient
   blockchain
   currency])
```

This is the part of Freecoin which should see most of the future development as it has to grow to implement a rich description of value transactions as relationships which are way more complex than what we call here a transaction. We write more about this horizon in the conclusions of this document.

5. The FXC secret sharing crypto protocol

The FXC protocol aims at marshalling fairly large integer numbers into strings that humans can easily note down on paper and communicate in voice. The encryption scheme still requires a machine to run software and with Freecoin we struggle to make such software free and open source, well readable and easy to re-implement. All libraries used for Freecoin's implementation of the FXC encryption protocol are F/OSS licensed and different peer-reviewed implementations are available in various languages, prominently C and Java.

As mentioned in the previous section on secret-sharing, Freecoin's approach to protect the access to blockchain operation is that of splitting the wallet key in 3 parts distributed among participants, the minting organization and an auditor.



More in detail, each part is constituted of three splices for a total of 9 different splices, consisting in numeric sequences of integers generated by processing the wallet key through a "Shamir secret sharing" (SSS) algorithm1. The SSS takes a secret integer number and splits it in 9 new integer numbers of which only 5 are needed to "unlock" and retrieve the secret. In our case the secret wallet key is composed by two numbers, to increase the cryptographic strength with larger number sequences. These two numbers are marshalled into the FXC protocol. Here we present version 1.

1 For more information see https://en.wikipedia.org/wiki/Shamir%27s_Secret_Sharing

Slices form a 2x9 array of SSSS keys are vertically associated.

P = Participant (passcard keys)
O = Organization (online portal)
B = Auditor (secondary online portal and/or cold storage)

```
    :HI       :LO
FXC1_random_FXC_random_1 - P     } participant's web cookie

FXC1_random_FXC_random_2 - P     } participant's passcard
FXC1_random_FXC_random_3 - P     } participant's passcard

FXC1_random_FXC_random_4 - O & P } organization & participant's passcard
FXC1_random_FXC_random_5 - O     } organization
FXC1_random_FXC_random_6 - O     } organization

FXC1_random_FXC_random_7 - O & B } organization & auditor
FXC1_random_FXC_random_8 - B     } auditor
FXC1_random_FXC_random_9 - B     } auditor
```

This cryptographic scheme allows the organisation to serve access to blockchain operations accepting a single FXC slice stored in the participant's web browser cookie that was set upon authentication. The participant has also a QRCode and/or SIMcard and/or USB key where other slices of the key are stored and can be combined with those of the auditor for blockchain access. Of course also the organisation can grant access to participants via the use of a physical key.

The random is a long integer created from a cryptographically strong random source (/dev/random) while the presence of an entropy gathering daemon as *haveged* is recommended on the running server. Regarding the dimension of the random numbers, ideal usability can be reached by making them 8 integer ciphers long, such as numbers can be easily communicated without ambiguity in any language and can be easily concealed by participants as phone contacts. Yet a total of 16 ciphers would not provide sufficient protection against brute-forcing: considering this is a base10 sequence of integers there should be 24 ciphers at the very least, which is the current default in Freecoin. Our code also contains a switch to measure the entropy of generated numbers, so far tests have been made using a Shannon filter to measure entropy, managing to harvest an average index of 3.1 on an Intel machine installed with GNU/Linux.

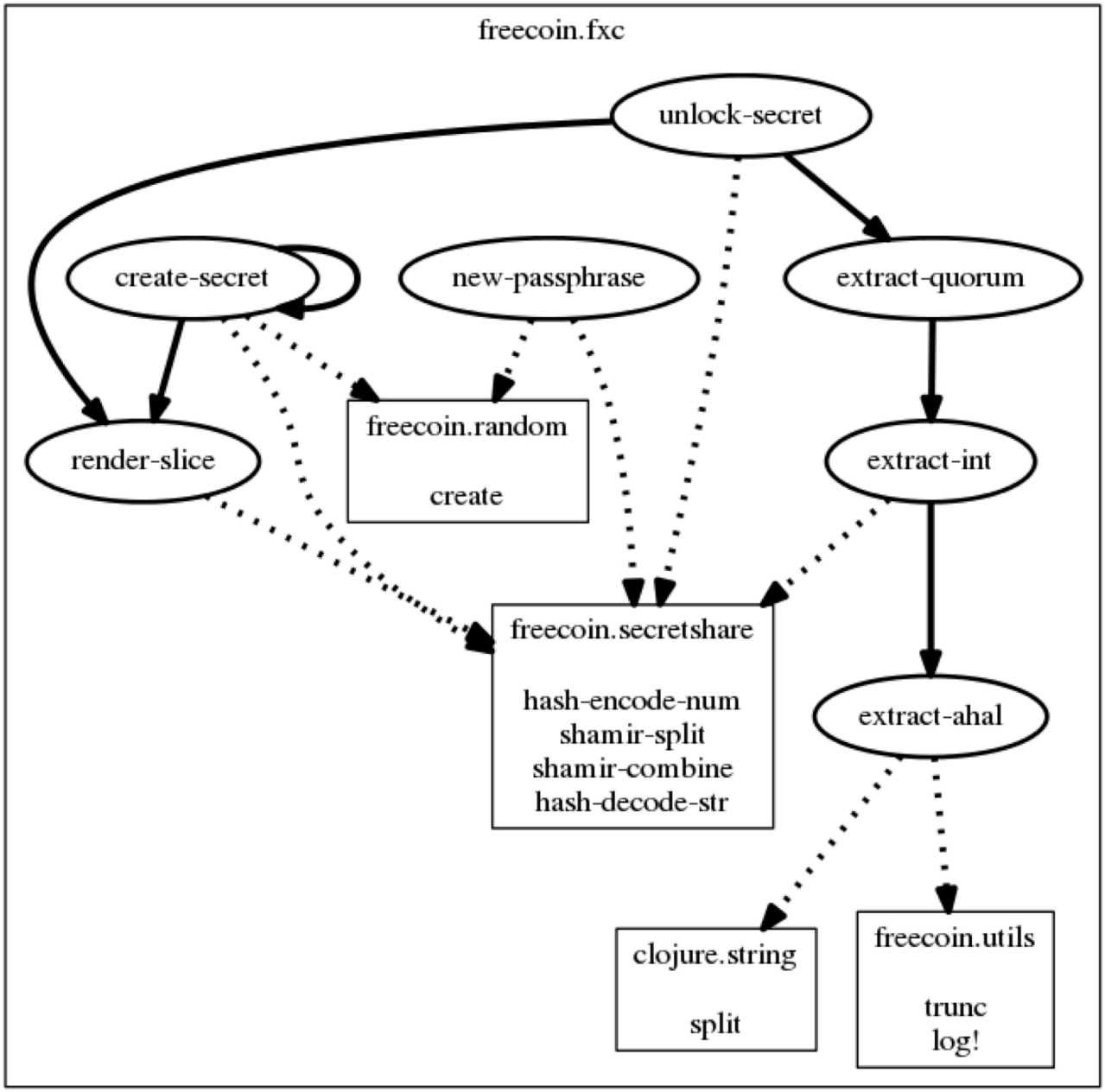


Figure 2: Function call graph for the FXC implementation in Freecoin

Please note this approach may or may not grant long term security for the passphrases generated, since brute forcing can happen directly on the blockchain, bypassing Freecoin and typical throttling measures for server access. At the time of writing we still consider our key creation and sharing methods as experimental and invite researchers to prove it breakable. An example of this sort of attacks for blockchain based accounts is well represented by the directory.io repository of private blockchain keys: the vulnerability of any accounts to this attack directly depends on the way wallets create the secret access keys, an issue common to all blockchains we know so far. Therefore we are

emphasising this aspect of technical development and is our ambition to propose the FXC protocol as an approach to create strong keys that can be easily shared, confident in its scalability as columns can be increased without influencing the plans on key redistribution. For example, there are attacks based on malicious parties seizing control of large amounts of blockchain (i.e. the "Eclipse" attack, but these are structural to the blockchain and not Freecoin itself, and mitigations are under active development by the academic community. See here for details: **http://cs-people.bu.edu/heilman/eclipse/)**

At this stage of development we are refraining from taking further decisions based on technical assumptions and we look forward to field testing into specific applications in order to realise what can be the best format to allow also a safety backup on paper that can be easily kept in custody and eventually communicated between humans. Ultimately relying on social measures for security complements technical measures.

Here below an example of wallet key generation in FXC shows how keys are basically strings with a prefix, an infix and a suffix containing information on the version of the protocol, the name of the blockchain and the positioning of the slice, since the Shamir's secret sharing algorithm requires all slices to be placed in the same order as they were created.

```
FXC1_STUB_837685160169_FXC_641128068918_0
```

The sequence above is the secret key to grant access to the blockchain, which is then split in 9 slices with quorum 5 using a factorization based on a large prime number:

```
{
 :description "Freecoin",
 :quorum 5,
 :prime prime4096,
 :type "STUB",
 :prefix "FXC1",
 :total 9,
 :length 12,
 :entropy 3.1,
 :version 1},
:slices
["FXC1_STUB_2242358125519_FXC_2285708168403_1"
 "FXC1_STUB_14374647279005_FXC_14241997681154_2"
 "FXC1_STUB_61982961124341_FXC_57694744128243_3"
 "FXC1_STUB_186088494123289_FXC_166646182785894_4"
 "FXC1_STUB_443985226695659_FXC_387916036685483_5"
 "FXC1_STUB_909239925219309_FXC_781141516613538_6"
 "FXC1_STUB_1671692142030145_FXC_1418777321111739_7"
 "FXC1_STUB_2837454215422121_FXC_2386095636476918_8"
 "FXC1_STUB_4528911269647239_FXC_3781186136761059_9"]
}
```

This process has full test unit coverage and is replicable via the continuous integration infrastructure setup to verify builds on TravisCI.

6. Conclusion and future roadmap

This deliverable documents an ambitious development, which goes beyond the immediate perception of innovative technologies. We have worked to understand the vision of how humans relate with the notions of currency for the commons, digital social currency and social proof of work explored in D3.4 and D4.4. Our implementation, Freecoin, aims to be a readable and interoperable implementation for a basic system of value transactions that can serve such notions.

We decided to share the same technical framework adopted by our partners Thoughtworks for other D-CENT software components as Objective8 and Stonecutter, as we clearly realise the power of Freecoin software can reside in its level of specialization, integration and overall simplicity.

The attention on the disruptive innovation of blockchain technology dominates the research panorama for the field we have chosen, often with reference to large scale financial technology and scenarios in which anonymity is desirable and trust is absent. The most engaging architectural task we faced has been that to find a way to relate complementary currency communities and commercial credit systems (C3) to the sometimes confusing information or biased interpretation of what are cryptographic blockchains and what they can be used for. The solution we propose for the use-cases we have observed is to overcome the total isolation of subjects on the blockchain with a device that can work along the notion of a Social Digital Currency, can integrate itself with collectively administered identity management services and decision making platforms and can provide a level of resilience for sharing mutual access to a wallet.

Much of the complexity added by the development of the FXC protocol is justified by a clear need shown in our most advanced use-case: EUROCAT. EUROCAT as a democratic organisation administering a credit circuit needs to be able to recuperate funds from the wallets of single participants, at certain conditions, for instance in presence of an auditor. This basic need makes the integration with blockchain technologies not desirable, as organizations remit all their possibility to access individual participants' wallets, even in the evidence of a lost password, a most frequent situation.

Such a requirement may seem fundamentally opposite to all what blockchains provide in terms of innovation, but we don't think so. From the social research being made so far we can only evince that the possibility for a community to help each other recovering a password, to hide secret codes into a classic pen and paper address book, to share consciousness about fraud is far more important than isolating assets in digital vaults, letting them travel anonymously across the world.

Blockchain recorded transactions still have a useful role in providing neutral ground for external validation of ledgers. In Freecoin we argue that blockchain ledgers, being transparent and distributed globally, break the sort of contextual integrity we all require for a reasonable level of privacy and for a reasonable fulfilment of the digital right to be forgotten. Therefore we do not intend to save all data on a blockchain, but just commit the basic volume of information that may be interesting for external apparatus to analyse and for which the access is radically open, but not total.

Far more important to the future of Freecoin is the quality of human interaction, adopting basic transaction gestures that are familiar to users. Not only QRcodes, but also PIN protected smartcards (just like bankomat) can be easily implemented as methods of signing a transaction. The availability of USB card readers on the consumer market at approximately 10€ makes it possible for

anyone with a reason and reasonable technical skills to build a small access point for transactions, a POS or a simple totem for CSA participants to mark down their working hours.

For transactions, the basic units of activity, timing is relevant in a concentric sense, meaning that closer to the circles of participants in which the activity is most intense, transactions should travel faster. As we approach the distance from a centre of activity, across the server-side information to reach the end of an outer blockchain, it is convenient to save transactions and commit them in bundles. This is an optimisation since transactions on blockchain are expensive, metaphorically speaking, as fees to miners and an increasing micro-transaction traffic may quickly turn out to be costly. Such an optimisation is already familiar to banks and we believe has to be implemented for software dealing with blockchain based Digital Social Currencies.

At last, more functions could extend the notion of transactions in Freecoin or even constitute the reason to develop a new complementary codebase that extends a model of information management that is context-sensible. In full serendipity and thanks to the Webpayments group process lead by D-CENT partner W3C we crossed the paths of our research with the UETP protocol, an initiative promoted by the Focafet foundation in Amsterdam. UETP is a protocol specification nurtured by strong commitment to free and open source standards and excellent knowledge of established industrial practices for value transactions. Considering UETP an ideal literature of reference in these matters, we conclude using their scope graph as a map of what a basic transaction system like Freecoin may need to facilitate. UETP lays the way for adaptable scenarios that seamlessly integrate C3 models, FIAT currency institutions and the outer blockchain based space. In such scenarios the financial game of speculation is no more at the center of the equation, shifting the focus on a human scale of consciousness for flow of transactions comprising business agreements and physical delivery of goods with a context-aware information scheme.

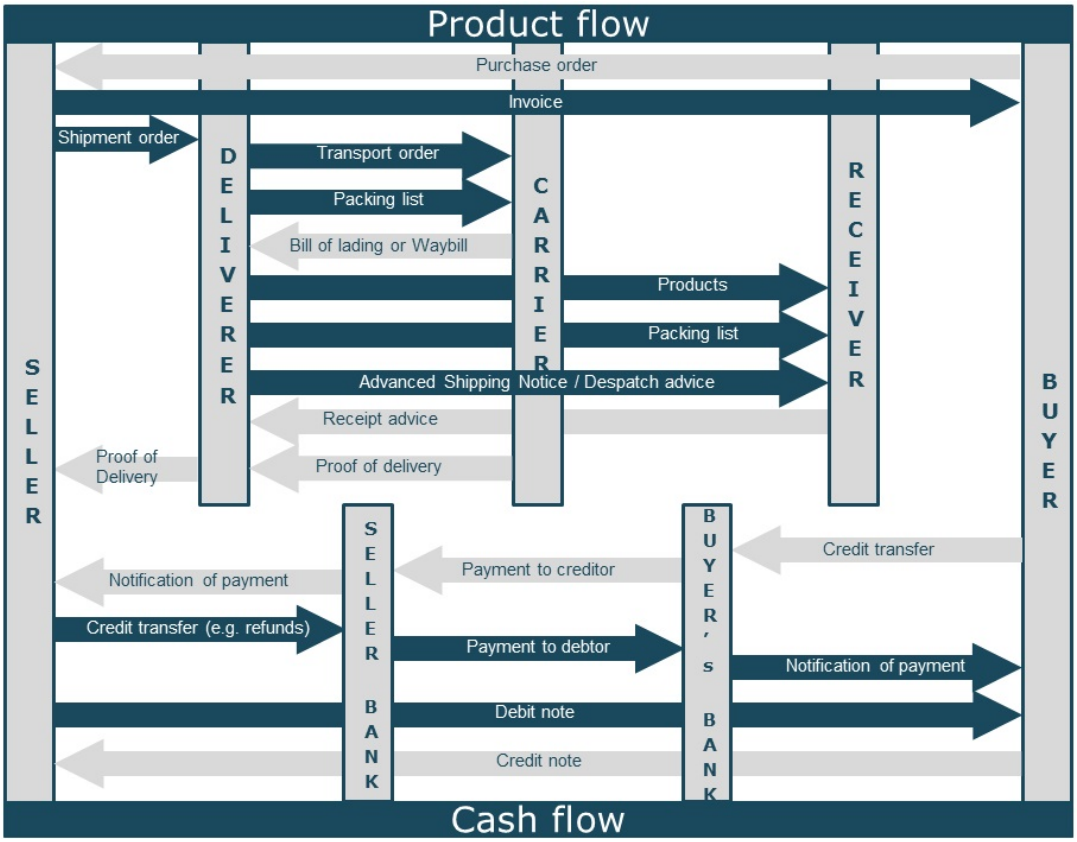


Figure 3: Product Flow