Project no. 610349

D-CENT

Decentralised Citizens ENgagement Technologies

Specific Targeted Research Project
Collective Awareness Platforms

# D4.4 Design of Social Digital Currency

Version Number: 2
Lead beneficiary: Dyne
Due Date: 31 March 2015
Author(s): Denis Roio, Marco Sachy, Stefano Lucarelli, Bernard Lietaer, Francesca Bria
Editors and reviewers: Kelly Armstrong

| 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: 1 June 2015**

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

# Contents

# List of Abbreviations

BTC Bitcoin cryptographic blockchain protocol

DSC Digital Social Currency

EMC Eurocat Management Committee

EUC Eurocat as currency unit

END endorsement as a currency of denomination for trust in the Eurocat system

EUR Euro FX

FXC The Freecoin Toolchain for the transfer of value(s)

MCS Micro Endorsement System

POW Proof-of-Work

UT Units of Trust in the Eurocat Micro-Endorsement System

XBT Bitcoin currency unit

XBN BitNation crypto-equity unit

# Executive Summary

D-CENT aims at developing large-scale collective platforms to support citizen empowerment. As shown by the preliminary considerations from the first round of interviews with alternative and complementary system managers in Spain, Finland and Iceland (D1.2 and D3.4), decentralised and privacy aware digital infrastructures are needed to allow institutions to integrate social feedback from the citizens, leveraging the potential of the extended society and social experts to improve democracy and many aspects of our society.

In turn, the experimentation on the Digital Social Currency Pilots in D-CENT can be conceived as an **open-source approach to decentralized complementary currency design**, which becomes ever more relevant where pilot communities are already actively designing tools for collective engagement and decision making on monetary economic matters affecting their communities.

The general trends that inform the design of the Digital Social Currency outlined in this report at the light of the findings emerged from field research conducted in 2014 (D1.2 and D3.4) are, respectively:

1. **Iceland:** a blockchain enabled municipal currency inspired by the case studies from Libra Circuit, the SoNantes (France), and coupled with use-cases like the HullCoin (United Kingdom). Iceland is offering the best suitable social environment for a Lean UX development of the currency software toolkit in D-CENT. We aim to facilitate the usage of cryptographic blockchain technologies by co-designing a reward system for political participation integrated in Betri Reykjavik in collaboration with the Municipality of Reykjavik.
2. **Spain:** the Eurocat complementary currency has already been launched in Barcelona on April 2014. We conducted an in-depth research on the status of the project, acknowledging that Eurocat needs a digital decentralization strategy to secure its resiliency and the reliability of its digital commons. We intend to envision and facilitate the evolution of its existing technical architecture to foster stewardship of shared data among participants. The aim is to decentralise the storage and distribute the responsibility of service hosting and data custody.
3. **Finland and Italy (Milan):** a decentralised social remuneration system that can reward the contributions that members of Helsinki Urban-Cooperative Farm perform to the common interest of the cooperative. This model will be also piloted in Milan, at Macao, an HUB for cultural workers of the city.

The focus in T4.4 will be on the technical and design elements that shape Digital Social Currency as a way to legitimise the bottom-up process by means of auditable cryptographic blockchain technologies, respectively: decentralized storage, ubiquitous wallets and ad-hoc social remuneration systems. Our focus is on complementary currency design in the hope that the distributed allocation of credit created among engaged members supports a reputation management in terms of tolerance of risk. This technical design will be the reference

framework for the Freecoin Toolchain implementation and experimentation across the different pilots here described (D5.5).

We also propose a first set of indicators to assess the success of the DCENT currency pilots, and their social impact. We define "social impact" here as the social and cultural consequences for pilots populations of the introduction of Freecoin. Social impacts, in this field, involve the ways in which people relate to one another by means of Freecoin tools, organize to meet their needs, and generally cope as members of the community, as well as changes to the norms, values, and beliefs of individuals that guide and rationalize the political process of deliberation. This first set of indicators will inform the future work on sustainability models and impact (D 1.3) and the framework for implementing digital social currencies (D3.5).

Finally, the common characteristic of the different pilots and use-case here described is the need to strengthen the democratic debate necessary to consolidate and preserve the management of economic transactions, especially those with a social orientation, inside the local monetary circuit.

This work shows the strategic importance to connect the D-CENT democracy pilots with the social currency pilots. Only through a democratic and participatory deliberation system, citizens can collectively define bottom-up their social needs, and inform the choices made on resource allocation and investment in social objectives and ethical criteria. This concerns the notion of **"social sustainability": without participation and real democracy, local monetary circuits run the risk to remain too little, too dependent on the local political cycles, too far from the real demand that may be expressed by the local economic system.**

# 1. Introduction[1]

All our Modern social organizations have either been created during the industrial age, or have been optimized for that environment. That is the case for production, distribution, housing, transport, education, healthcare, governance and political decision making, etc., The industrial age was also a golden age for "experts", people who know what has worked in the past thanks to specialized training in very specific fields. Almost all organizations took the form of pyramids, in which information would flow from the field through experts to the top where the most important decisions would be made. Good organizations were those that managed the necessary information flows in such a structure, and were effective in having the decisions made at the top implemented down the pyramid back into the field.

However, the industrial age has died with the 20th century. China becoming the "world's factory" was certainly not at the origin of this process, but has accelerated its implications, and is ensuring that the changes are irreversible.

It has thereby become a cliché that we have entered the information age. Interestingly, the way information technology itself has evolved has also shifted from what used to be expected. For instance, in Stanley Kubric's classic "2001: A Space Odyssey" (1968), computers were supposed to become giant centralized machines that control everything. Of course, what happened instead is the Internet: a network of millions of machines interacting in a distributed architecture. Mobile phone technology is guaranteeing that this networked approach is decentralizing further all the way to the individual citizen, and for the first time is taking place simultaneously on a global scale. This explains why mobile phone technology makes it possible for what used to be called "developing countries" to make a quantum jump in communications, to the point that it starts erasing the distinction with "developed" ones. Decentralized mobile payment systems are now more advanced in Kenya or Indonesia than in the US or Western Europe. Precisely because the information age is making our major social systems obsolete, all countries should be considering themselves as "developing". Some still happen to be in denial of that fact...

The shift from the industrial to the information age requires structural change by definition. In turn, structural change requires structural innovation, which is typically not the terrain of "experts" who have been trained to understand what worked in the past. There is risk that the old pyramidal decision structures and the established experts become obstacles to the necessary change.

One of the reasons for failures is that the traditional structures are simply too slow to be able to adapt to the speed of change in the field. By the time that the relevant information has been distilled upwards in the pyramid, and the implementation of the decision has percolated back down to the field, the reality may have changed enough to make even a correct decision obsolete.

[1] by Bernard Lietaer

It is only in such a broader context that the relevance and importance of a project like D-CENT becomes visible. It starts with the premise that democratic governance will have to adapt in the 21st century by smart use of the information technologies that have become available. It welcomes that civil society in general, and activist communities in particular, can become an important source of social innovations. What are the tools now available for a community to make decisions, and to organize and coordinate its actions? For they have the potential to implement the decisions made by the communities and for the communities in a shorter loop than the legacy governance systems. The currency designs that are described in this section aim at providing tools that fit those requirements.

# 1.1 Digital social currency experiments to foster direct democracy across Europe

The research and development approach proposed follows up on the definition of Freecoin: back in 2011 researchers at Dyne.org had announced their intention to "fork" Bitcoin and develop "Freecoin" with the aim to realize a software toolkit to build and deploy custom cryptographic blockchains. Having foreseen the success and importance of the Bitcoin project and its underlying cryptographic blockchain technology, the Freecoin initiative doesn't aim to be a currency in itself, but to be a base for field experimentation and Lean currency design practices based on such technologies. Freecoin is not a currency, but a suite to create P2P currencies, in order to scale bottom up cooperation for the social good Freecoin is thought of as a toolchain: a backend suite of interoperable tools to run free and open source, ad-hoc blockchain systems. The ultimate ambition of the Freecoin Toolchain is, even beyond the span of the D-CENT project, to reach GNU software quality standards to create and operate blockchain systems. In our previous research work (D3.4), we sketched out different kinds of local monetary circuitsand those systems that complement the conventional banking system by implementing currencies that perform countercyclical and social purposes.

On the one hand, we argued that a well-designed complementary currency is able to sustain businesses and finance local welfare services alongside with the national currency (Swiss WIR, French SoNantes, Italian Sardex, English Bristol Pound, German Chiemgauer). Both the case studies we presented and the users' interviews gathered in the pilot contexts showed that top-down projects do not work. For instance, SoNantes is perceived as a project without real participation and distributed democracy especially in the definition of social needs that characterize the community sector. At the time of writing the Sonantes launch has been announced for the spring 2015, after more than four years of "alpha-testing stage". In this period the launch has been announced three different times.

On the other hand, the Sol Violette case (Toulouse, France), a voucher allocated by the public sector to specific target groups, presupposes the collaboration with many actors following a bottom-up decision making process. It requires both increasing the diversity of businesses of social economy for widening the range of available commodities and the provision of funds, but the Sol Violette governance model seems to be a best practice: the organization running the scheme is divided into 5 advisory groups and each group sends representatives to a main decision making body, consisting of 17 vice presidents. Everyone who is part of the Sol Violette Association has a say in all matters affecting the currency, and all major decisions are taken by consensus.

This concerns the notion of **"social sustainability": without participation and real democracy, local monetary circuits run the risk to remain too little, too dependent on the local political cycles, too far from the real demand that may be expressed by the local economic system.**

In fact, all currency systems should ideally be managed as a commons. Indeed, if any currency loses the trust of its users, it simply stops being accepted as money. This is the case even for official money, as is demonstrated whenever there is a currency crisis. Contrary to the overly simplified idea of the "tragedy of the commons", communities all over the world have developed and used effective rules that make management of a commons successful. This has been well documented by Elinor Ostrom, in a life-long work for which she received a Nobel in Economics. (Ostrom, 1990, 1994, 2003). As stated in section 3.3, one of the most important of these rules is hyperdemocracy: most of the people affected by the system should have the capacity to influence and modify the rules, if and when needed. We are obviously very far from such an environment in the case of the official national currencies. However, for the management of social purpose currencies input from the users will be critical for the sustainability of such systems.[2]

By considering the peculiarities among D-CENT pilots, the definition of the social needs that characterize the communities and civil society sector represents not only a prerequisite to improve democratic participation of citizens, but moreover an important tool to well design and disseminate knowledge and best practices around digital social currencies. As we argued in D3.4, the ways through which people "enter" a complementary currency system - be the service providers or users who share certain social and economic issues - can be different. In any case, the local monetary circuit should provide liquidity to finance not only the local businesses, but also the collective services and the activities that correspond to the social objectives and ethical criteria as defined bottom-up by the community.

A ***Demurrage*** **mechanism** (a negative interest applicable to a currency) provides an incentive for the currency to circulate. At the extreme, credits that aren't spent by a certain date are automatically transferred to another account, as a donation or as a fee for the social services provided by local welfare system. The charities that receive the credits may then spend them to purchase goods and services from the firms. In this way the communities have to also discuss the possibilities to fund other social innovations programs.

[2]The seven rules for sustainably managing a commons by Elinor Ostrom are:

- Clearly defined boundaries
- Congruence with local conditions
- Hyper-democratic: Most individuals affected can participate in modifying the operational rules.
- Monitoring: Monitors are accountable to Users or are Users.
- Conflict-resolution mechanisms: rapid access to low-cost local arenas to resolve conflicts
- Graduated sanctions: Users who violate operational rules are assessed graduated sanctions by other Users, by officials accountable to these Users, or by both.
- Minimal recognition of rights to organize: No contradictions with State of Federal Laws

**The rules to issue the currency depend on the decision-making processes (i.e. direct democracy) that characterize different pilots**. For instance, also the *demurrage* mechanism should be decided bottom-up by considering the form of direct democracy that communities adopt and according to the principle of Isigoria, i.e. the notion about the citizen in Ancient Greece that enjoyed not only free speech but also equal say in the final formulation of policy, independently of whether he was rich, comfortably off, or indeed a pauper eking a modest existence out of manual labour. Aristotle's definition of democracy is still significant in this regard. A constitution in which the freeborn and the poor control the government; being at the same time a majority (Varoufakis, 2014).

In order to start Digital Social Currency design from desirable theoretical pinpoints, the suggestion in the concluding remarks of D3.4 was to endorse the insights from Lietaer et al (2001; 2010 and 2012), i.e. to design structurally sustainable money systems via the creation of a digital ecosystem of complementary currencies to use in parallel with conventional ones ( a "Monetary Ecology"). Indeed, alongside orthodox monetary economics, a polidoxy (Arnspenger, 2008) in the monetary field would mean the legitimacy of currency diversity that becomes the new norm for systemic resilience purposes.

Starting from these premises, the proposal in this deliverable is to design decentralised tools to manage trust relations among participants of multi-currency systems (Eurocat and Euro; Social Credits and Icelandic Kronas, etc.) by means derived from an interoperable backend software component that facilitates the usage and integration of cryptographic blockchain technologies for achieving social sustainability. In this way it is possible to have not only a structurally sustainable money system, but also a structurally integral one. In brief, sustainability is not enough; we also need built-in integrity for a 'stable' system to endure (Schumacher, 1989 and Illiceto, 2008), while preserving the path dependence that characterizes the different pilots.

Pilot presents different cultural norms and goals, consequently the technologies must consider some degrees of freedom in the social system: the way in which money is issued and distributed, the way in which the complementarity between business and collective social needs is ruled, the time when hoarding may be accepted, the possibility to remunerate specific work in complementary currency, or the opportunity to use them to pay local taxes to local governments represent just the most important parameters of the system that may vary depending on democratic decision-making process. Notwithstanding, technologies may be extremely useful for all D-CENT pilots to support the trust in the local virtual currency, to facilitate both monetary and informative exchanges in the community, to historically monitor the monetary flows and stocks at local level in a decentralized, democratic and transparent fashion.

In turn, the Freecoin Toolchain should respect the normative dimension of the monetary circuit. **Money is a social relation more than it is a pure technical instrument** (Ingham 1996, 2013). As such, it reflects social relations which function as providers of rules for games played by social and economic agents. The technologies and algorithms we will propose must be conceived as technical tools influenced by social variables and aimed to solve problems of social and economic coordination. Social purpose complementary currencies are monetary solutions for effectively reframing the structure of the communities and social economies participating to D-CENT pilotexperiments.

Following these lines of thought, an important aim is that the Freecoin Toolchain can increase the local multiplier effect by linking local unused resources with correspondent unmet needs and, consequently, foster local aggregate demand. This may take place within the dynamics of the Eurocat regional currency in Catalunya whose main purpose is to allow for collective social control of credit. Secondly, the local multiplier could increase in Iceland thanks to a municipal currency scheme allowing for the circulation of social credits within the network of participating local partners from both the public and the private sectors. In other cases in Finland and Italy, the digital social currency may result from an experimentation around the capability of the blockchain to process collective decision-making operations for the management of the communities, i.e. to increase of the local multiplier effect by virtue of increased efficiency gained from distributed computing.

Cooperative relationships will hence be reconsidered in a new way. Furthermore, the reduction in the cost of working capital financing coupled to increased demand - which in this scheme can potentially meet the new needs from the world of solidarity economy - could allow companies and public administrations to increase the long-term investments in EUR; funding availability and the expectations of increasing returns may actually be part of this scenario. The viability of a monetary circuit, depends not only on simple matters of social engineering or management. The trust dimension among participants is perhaps even more crucial.

Hence, in the following, **we propose design elements for a toolkit - the Freecoin Toolchain - to build blockchains for the social good aimed to improve decentralized trust management dynamics manifesting in the D-CENT digital social currencies pilot communities.**

# 2. Why Bitcoin?

This chapter will illustrate the present state of cryptographic blockchain technologies in relation to the aims of the D-CENT project. We will describe the design traits of cryptographic blockchain technologies (to which we will simply refer as "blockchain" in a rather abstract way), by deconstructing the features of this invention that we believe to have a massive innovative impact in the fields of information sciences and digital systems.

Our enquiry starts from the most mediatic and influential project: **Bitcoin.** We need to distinguish between two different uses of this name: the bitcoin as an Information Technology Protocol and its implementation as a Bitcoin Currency. They were both originally published by Satoshi Nakamoto and nowadays maintained by an active group of international developers. We will then take in exam some relevant first and second-generation blockchain implementations that have accompanied and followed the Bitcoin popularization and worldwide adoption. Further, we will present a critique of Bitcoin at economic and political level and we will conclude with a discussion of blockchain technologies developed for managing the social good in a decentralized way.

## 2.1 Cryptographic blockchain technologies in Bitcoin

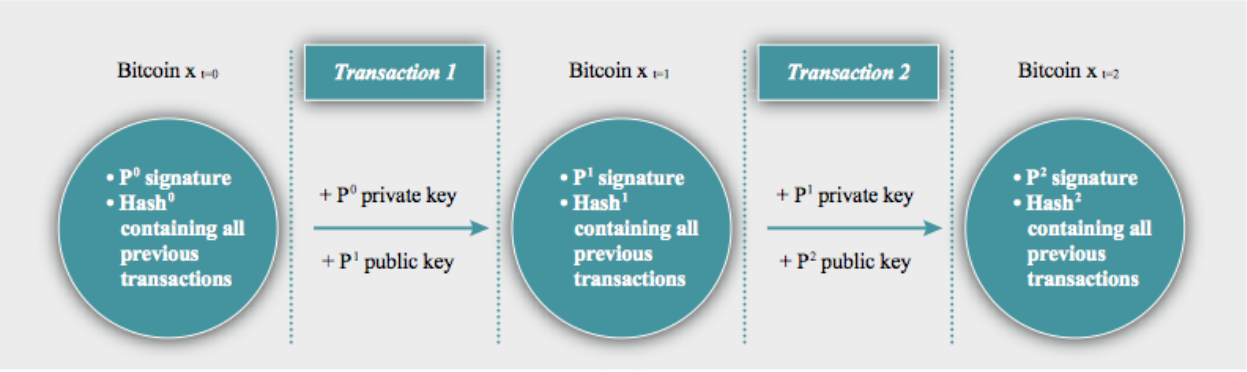
**Cryptographic blockchain technologies (blockchain), made famous by the Bitcoin project, are emerging as an interdisciplinary area of software development for decentralized data commons, value exchange and management of trust.According to the primary author of the Bitcoin Core implementation, Satoshi Nakamoto:**"Bitcoin is a decentralized electronic cash system that uses peer-to-peer networking, digital signatures and cryptographic proof so as to enable users to conduct irreversible transactions without relying on trust. Nodes broadcast transactions to the network, which records them in a public history, called the blockchain, after validating them with a proof-of-work system. Users make transactions with bitcoins, an alternative, digital currency that the network issues according to predetermined rules. Bitcoins do not have the backing of and do not represent any government-issued currency" (Nakamoto, 2008).

In other words, a blockchain is a timestamped ledger shared by all nodes participating in a system based on the Bitcoin protocol. The blockchain allows for a new architecture in payment system design: every device participating to the network - and the people using them - share the same transaction history by abiding to the 'longest chain rule': the blockchain is a tree-like structure that consists of all valid blocks whose entire ancestry is known, up to the genesis block. This common understanding creates a shared agreement within the whole Bitcoin community about the reliability of using the decentralized currency. Since there is no central point of single failure, and since it is available to everybody, a blockchain is structurally more resilient and transparent than the conventional monetary system, which has proven prone to collapse and very difficult to effectively audit by statute.

**A transaction on the Bitcoin blockchain** can be described as follows:

"A transaction is a *data structure* that encodes a transfer of value from a source of funds, called an *input*, to a destination, called an *output*. One should think of them as bitcoin amounts - chunks of bitcoin - being locked with a specific secret that only the owner or person who owns the secret can unlock. The fundamental building block of a bitcoin transaction is an *unspent transaction output*, or UTXO. UTXOs are indivisible chunks of bitcoin currency locked to a specific owner, recorded on the blockchain, and recognized as currency units by the entire network. The bitcoin network tracks all available (unspent) UTXO currently numbering in the millions. Whenever a user receives a bitcoin, that amount is recorded within the blockchain as a UTXO. [There] is no such thing as a stored balance of a bitcoin address or account; there are only scattered UTXO, locked to specific owners. The concept of a user's bitcoin balance is a derived construct created by the wallet xapplication. The wallet calculates the user's balance by scanning the blockchain and aggregating all UTXO to that user (Antonopoulos, 2014)."

Starting from the first, or genesis block, a chain of bitcoin transactions ignites a process of validation *via* **a distributed consensus algorithm** run by all those who participate into the activity of issuance of new currency, or miners. A chain of bitcoin transactions may be represented as follows:




Source: ECB.

**Figure 1: representation of a chain of bitcoin transactions.**

More than 5 years after its inception, Bitcoin Core is still the reference implementation of the Bitcoin protocol, its code is distributed under the free and open source software MIT license and maintained by a rather compact group of developers handling a significant load of daily contributions.


**Figure 2: bitcoin contributions per month**

Its code is cross-platform (binaries are provided for MS/Win, Apple/OSX and GNU/Linux operating systems) and written in C++, requires a reasonable amount of library dependencies and interfaces with users via a command line, a remote procedure call API (JSON RPC) and a QT graphical interface.

Here follows a brief list of library dependencies of the Bitcoin Core daemon binary (excluding GUI code) at the time of writing (version series 0.10):

- libgmp GNU MP Bignum
- libboost_system Boost C++ extensions
- libboost_filesystem Boost C++ extensions
- libboost_program_options Boost C++ extensions
- libboost_thread Boost C++ extensions
- libdb_cxx Berkeley DB version 5.1
- libssl Openssl 1.0
- libcrypto Openssl 1.0
- libminiupnpc Mini UPNP library
- libpthread.so.0 Posix 1.b Threads

In recent times the contributions on Bitcoin Core have increased significantly, something that makes our work more complex and definitely leaves behind most alt-coin forks.


Figure 3: bitcoin commits per month

However it must be said that the contributions go in good directions for the future of this codebase, also modularizing its code, removing unneeded parts and integrating a proper test mechanism.

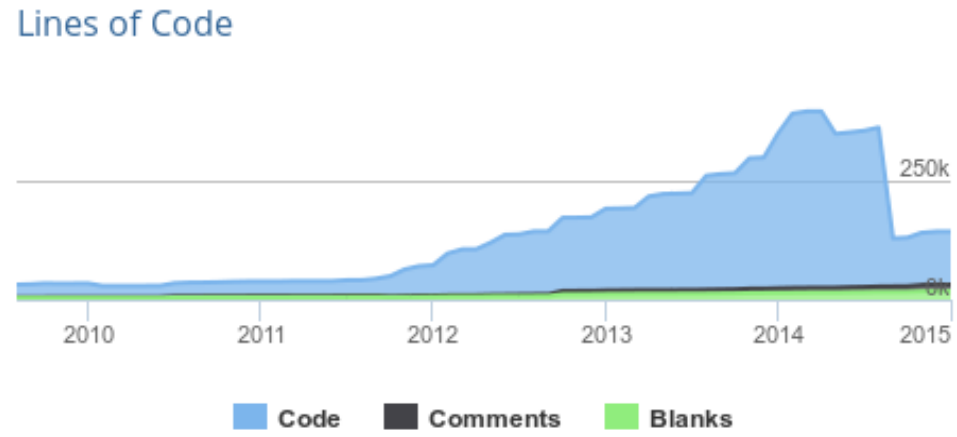



Figure 4: bitcoin lines of code

Most blockchain re-implementations share the same algorithmic scheme: one or more hashing algorithms (at least one to produce human readable addresses, usually RIPEMD-160) and an elliptic curve (EC) for signatures. In Bitcoin Core are used two rounds of SHA256 to calculate and verify "Merkle roots" (binary hash trees) as block identifiers and the EC DSA Koblitz to perform signatures (secp256k1). There has been a lot of speculation on the possibility of cryptographic attacks on this choice of cryptographic primitives. However for the way Bitcoin is engineered the compromission of one primitive would not carry over in other parts of the system. It must be anyway noted that the theoretical future popularization of quantum computing may open a relevant attack surface for this system architecture.

By now is clear that the general direction of blockchain technologies is that of making information systems more distributed and resilient: a general improvement that not only implies

having a distributed database, but also a timestamping mechanism for data operations and an authentication system that is decentralized and provides incentives for involved peers. Nevertheless these improvements come at a cost which is higher in these early phases, that of usability and malleability:

1) **Usability**: most blockchain based systems willing to bridge over the usability gap are giving up on decentralization and derived advantages to deliver a managed web environment for the users. Such solutions become less interesting as they come closer to what is already provided by more mature technologies as cloud distributed databases.

2) **Malleability**: adapting blockchain technology to specific needs turns out to be an extremely complex and dangerous operation which risks to introduce flaws that may also appear later in time when the deployment of the implementation has already grown in importance.

Second generation blockchain technologies mostly have struggled to improve malleability, for instance implementing touring-complete languages that can fit scripts between bytes padding some transactions and, in doing so, relying on the techno-political negotiation of the Bitcoin protocol Take for instance the debacle about the 80 bytes of OP_RETURN[3], an harshly contested ground for quite some time now among different design views at stake, something that several new implementations rely upon for their own existence. It is often the case that the implementation of such blockchain scripts is marketed as a multiplication of possible functions for the blockchain, yet the price of augmenting such complexity is not considered.

Meanwhile, as of today, there isn't a clear path marked for blockchain technologies to become less complex and more malleable: the complexity of implementations is growing directly proportional to the possibilities of adaptation in various contexts. We identify this as one of the biggest flaws in the current development of blockchain technologies, which we can only consider to be still far from adulthood. The still growing complexity of blockchain technologies undermines their long-term usage in mission-critical situations, making it difficult to deploy them for socially sound applications that can then be only understood and governed by a small elite of highly specialized engineers.

For these reasons we believe that the major weaknesses in blockchain technologies are not to be identified in the domain of cryptographic analysis and technical implementations, where steady progress is being made on top of a technically innovative design that offers qualitative advantages over what has preceded it. The major weaknesses lie into the possibility to appropriate and audit such technologies by a larger portion of the population affected by their use. As a solution to this, progressing on blockchain development for the social good, we propose to further deconstruct and simplify blockchain technologies.

3 On OP_RETURN see: https://github.com/bitcoin/bitcoin/pull/3737 https://github.com/bitcoin/bitcoin/pull/5286 http://www.economist.com/news/finance-and-economics/21599054-how-crypto-currency-could-become-internet-money-hidden-flipside

# 2.2 Features of the blockchain

At the time of writing this chapter (Jan 2015), we can count an existing amount of 585 alt-coin implementations, the majority of which are forked from Bitcoin Core at different versions mostly between its 0.7 and its 0.9 release, with a few exceptions of full-rewrites and/or complete replacement of the blockchain protocol. In the past 5 years about 70 "Bitcoin improvement proposals" (BIPs) have been processed and the Bitcoin Core has been updated and patched for problems encountered along the way, updates to which the alt-coin forks can barely catch up due to complexity and lack of modular design in code components.

On top of this scenario, it is difficult to ignore that the quantification of the Bitcoin market cap in financial terms today amounts to a total of approximately 5.5 billions US Dollars of which 4.7$ billions are stored in Bitcoin and almost 1$ billion in alt-coins, which should give us an idea of the peer pressure and interests present in debating technological enhancements and changes to the Bitcoin Core reference implementation.

To proceed explaining the design features of cryptographic blockchain technologies, let's deconstruct its core function into 3 main parts:

- **Proof of Work**
- **Authentication**
- **Decentralization**

## Proof of Work

The proof of work (POW) is the algorithm that needs to be solved in order to obtain a block as reward: it is what "Bitcoin miners" try to solve and what becomes progressively harder to solve at every new block rewarded. In Bitcoin mining is the act of creating bitcoins by running the proof of work algorithm, which produces network neutral proofs of the fact the algorithmic "work" has been done. The metaphor is that of finding this "algorithmical mineral" and minting it into usable tokens, which is adequate considering cryptographic currencies are digital assets, rather than coins in the most literal sense. The process of mining is remunerative for those who challenge it by running the mining software on their computers which transforms electricity into Bitcoins. By mining, computers look for numbers that are not yet discovered and, once they found them, these numbers can be relayed as coins within the network.

Miners generate a wealth they can put it in circulation at their own discretion. As absurd this may sound, the value of digital assets produced this way is purely relational and it is important to understand that the POW algorithm is really the seal of neutrality for such a system that will reward the same way any participant to the network.

As the design of Freecoin will show, the POW is also the main point for customization of the Bitcoin Core implementation. The forks of Bitcoin Core have created parallel blockchains just by using a new "genesis code" and a new POW, hence reusing most of the original source code. The substitution of the POW with different algorithms can have far consequences, for instance the most popular alt-coin called Litecoin has adopted the Scrypt hashing algorithm which is

memory intensive, rather than CPU intensive, to couple the mining process to that of Bitcoin, so that miners can mine both blockchains on the same machines. Adopting Scrypt for Litecoin has also meant to set a lower bar for new miners: the hardware race to ASIC and FPGA boards built with hard-coded SHA256 hashing is something that made mining extremely competitive for Bitcoin and less interesting for new arrivals. But Litecoin has disabled Bitcoin miners on its blockchain and, while growing, has raised industrial interest to offer new Scrypt miners on the market.

The approach to obstruct hardware mining and avoid the take-over by big specialized players has been adopted by various Bitcoin forks and re-implementations: so called "hybrid" and "CPU alternate" POW algorithms whose approach is often that of mixing multiple cryptographic algorithms, very different among each other, which are difficult to be implemented in a compact hardware setup, be it FPGA or ASIC. The diversity of algorithms is mostly implemented by chaining them and the increasing difficulty in mining is also claimed to be a warranty of long term security: it is the case for Quark (QRK) for instance adopting 9 rounds of hashing from 6 hashing functions (Blake, Bmw, Grøstl, JH, Keccak, Skein) plus 3 rounds of a random hashing function among those, or SecureCoin (SRC) chaining Grøstl, Skein, Blake, Blue Midnight Wish, JH and SHA-3.

The POW is also the computation that demands most power and generates most entropy (as heat) for the process of creating new blocks and processing transactions. The nature of this computation is entirely arbitrary and in most cases produces results that have no use outside of the blockchain itself. But for those using the blockchain it is not pure waste, since the work done increases the strength of authenticity in the blockchain - a critical role especially at the very beginning of a new blockchain.

It is important to note that the inutility of POW results outside of the blockchain has also been addressed by alt-coin projects, first and foremost by Primecoin, which has adopted as POW the search of new prime numbers. Thanks to the incentive of its financial value on the Bitcoin market, just during the first months of existence this project has been able to gather enough participants to find several new kinds of primes in the Cunningham series, a de-facto contribution to mathematical research that is still on-going. This may be an indicator of the fact that the POW of a blockchain can really be a relevant contribution to research if related to computations useful also outside of the blockchain, hence diminishing the entropy it creates.

### Authentication

Another core feature of cryptographic blockchains is that of authenticating data inscribed inside them, be them transactions of blocks or, in more advanced scenarios, any other sort of metadata inscribed or linked into such transactions.

The authentication (through distributed validation) works by the principles of triple-signed accounting already well described by Ian Grigg's article "Triple Entry Accounting", basically consisting in a peer to peer based network of witnesses that are offered incentives to sign the existence of contracts at a certain point in the blockchain, which also means at a certain point in time. Timestamping is in fact an important part of this feature that really makes it useful for the sort of contracts and notarile acts that are nowadays still authenticated by a centralized network of authorized subjects.

It is also important to note that within the digital domain the characteristic of unicity can only exist so far in a blockchain system: still everything that is digital can be copied, yet by virtue of signed contracts a digital asset can be publicly transacted and every participant to the blockchain can verify that and even sign it as a witness. The blockchain will timestamp and store the whole history of transactions for each asset. This feature of authentication becomes very close to the etymology of the word itself: composed by αὐτὸς and ἐντὸς the noun refers to the assessment of truth, reality and unicity within a system. It is not a coincidence that notarile acts are said to be "authenticated". Authentication is an important feature of blockchain technologies that stays unvaried across all forks and re-implementations. Here we dare to say that the core innovation of blockchain is really that of giving a group of participants the potential to assess what is true for its peers and to track and store the genealogy of such a truth.

### Decentralization

The third salient feature of blockchain systems is that of decentralizing the storage of all the data contained in it, by distributing it among the whole set of participating peers. In Bitcoin Core anyone who has the software running, even those who are not mining, will have a "wallet" and the full copy of the blockchain, storing the full history of the network. Such private nodes do not depend from any cloud or centralized service of sorts: the only thing they need to function are other peers of the same kind. Every peer stores the complete blockchain.

Due to the increasing size of the blockchain, this way to function is being changed in many Bitcoin re-implementations at the risk of losing an important feature: a very resilient way to store the history of contracts taking place inside the blockchain - and possibly also more attached data.

Obviously this is a feature that is very important for the D-CENT project and we are looking forward to keep it around in any implementation we use. It should also be noted that nodes storing the whole blockchain can be small hubs connecting multiple users, hence the load in running one can be shared - or should we say federated - among multiple local communities. Decentralized and resilient storage also makes available to anyone the possibility to run data analysis and tracking of transactions across the whole network, something we see as desirable in most use-cases dealing with credit circuits and accountability for public funding.

The aforementioned **ubiquitous wallet** feature we intend to deploy in pilots is heavily relying on such decentralization traits: so called brain wallets or paper wallets are basically storing all their contents on the blockchain and providing access to them from anywhere with the only requirement of a secret (be it a passphrase or qrcode). We believe this goes even beyond the concept of mobile clients in opening up new opportunities for public shared interfaces and technology independent access to participation.

## 2.3 Overview of blockchain codebases

From the Bitcoin popularization and until today a variety of blockchain implementations have appeared, most of them emphasizing on the decentralization aspects introduced by the technology, coupling them with more features contextual to different areas of application.
To simplify this overview we will distinguish between three generations of codebases, briefly describing their origin.This section does not aim to be comprehensive, rather than sketch a generic distinction that is useful for the analysis being conducted on pilots.

## First generation codebases

We ascribe to the first generation of code-bases all those implementations based on "Proof-of-Work" schemes that combined cryptographic hashing algorithms in different ways, but all substantially adopting a determined subset of results from such algorithms as the finite total amount of a certain "digital asset": for instance in Bitcoin that is all values that when hashed lead to a result that has a number of leading zeroes, while other "crypto-currencies" have adopted different arbitrary sequences here.
This is the cryptographic trade-off at the base of Bitcoin's mathematical architecture and all first generation code-bases: the difficulty to find values increases exponentially as more of them are found, but verifying their authenticity is easily done just running the hashing algorithm. The vast majority of "alt-coin" implementations are forks of the Bitcoin Core code-base from its published version 0.6 to 0.8 and are based on this principle, mostly applying variations on the hashing algorithm and in some cases on the P2P stack.

To operate in various ways on the "main" Bitcoin blockchain, more implementations have been undertaken by different developers and in different languages, opening up the possibilities to have an incredible proliferation of first generation blockchain applications bearing different features. One of the first and foremost features to be developed was that of storing the blockchain on a server that can communicate with lightweight clients in order to overcome the need to have the full blockchain downloaded, a feature very useful for mobile clients. For instance the "Stratum" protocol was then developed to allow the Electrum client (written in Python) to operate in communication with a blockchain server, such a protocol became a de-facto standard also for mining software, but its status has not yet been formalized into a BIP (Bitcoin Improvement Proposal) for standardization.

A mature re-implementation of Bitcoin's protocol we find particularly interesting, because of its versatility in handling such client-server scenarios, is Libbitcoin: written in the earliest period of Bitcoin popularization with a clean approach to a modular C++11 code-base, Libbitcoin expressly aims at being a modular component (a library) to be used by and included into larger architectures. Libbitcoin also managed to provide a very fast ad-hoc database filesystem for blockchain operations and an API that can be exported to different languages, first of all Python.

In the domain of what we call "first generation" much more development has taken place and it is beyond the scope of this document to map all of it, it is however worth mentioning the BitcoinJ implementation, among the first implementing the "lightweight simplified payment verification" (SPV) mode to verify transactions by downloading only limited segments of the blockchain.

We consider such first-generation blockchain technologies viable for further development, but they all bear the cost of an algorithmic POW which is energy intensive and mostly grants a huge advantage in minting to all those in possession of specialized hardware. Our research and development should not ignore the future of Bitcoin's blockchain, the biggest working protocol of a decentralized blockchain ledger being maintained today. However we individuate in the second-generation codebases interesting opportunities to implement lightweight systems that are well usable and adaptable as prototypes for our user-centered design approach.

## Second generation codebases

We define "second generation" codebases all those implementations that have developed their own blockchain protocol, not compatible with Bitcoin's protocol.

The first and foremost implementation of this kind is NXT which has also generated a family of forks and adaptations. Implemented in Java, NXT has also substituted the "Proof-of-Work" in Bitcoin with a "Proof-of-Stake" (PoS). In the PoS architecture there is no reward for miners, whose sole incentive is that of gaining transaction fees: this way also the rush to energy consumption is tamed down to reasonable levels. The trust in PoS systems is not based on the quantity of present calculations a miner can do, but on the quantity of accumulated wealth a participant to the network has, presuming that such big stakeholders won't even reach the 51% of the market cap nor will act against the interest of the network itself.

NXT has recently implemented a feature that is very interesting for us, called "Monetary System", facilitating the creation of new currencies circulated via the NXT blockchain and even allowing the tweaking of their characteristics following some generic guidelines. NXT also offers an API to interact with all its functionalities and it is distributed as a platform that can be operated both locally from a desktop and remotely on a server.

Another important improvement that NXT has brought to popularity is the "brain wallet" approach of removing completely the necessity to have any secret data on any mass-storage to identify users: a single passphrase of at least 35 chars is all a user needs to login on any NXT installation, local or remote, and access her wallet on the blockchain. This opens up a large degree of possible developments facilitating tasks far beyond those envisioned by this document and in general could inform the debate on identity management with practical use-cases that are based on cryptographic blockchains.

At the time of writing this document, NXT has reached a critical mass of users but it hasn't yet made any significant breakthrough in popularity. While we expect this to happen, we also expect the technology to face some challenges for an algorithmical attack surface that hasn't yet received all the attention that was dedicated already by researchers on first generation code-bases. Nevertheless we see NXT cryptographic blockchain technology as a viable platform to build our LEAN UX cycle in D-CENT especially when dealing with community based complementary currencies and SOCIAL POW implementations.

## Third generation codebases

It may be incorrect to group rather different codebases in this section, yet following up on the brief and pragmatic posture we take in this chapter let us briefly mention a few more interesting development cases.

We generally include into the definition of third generation codebase those attempts going into the direction of implementing "smart contracts". Such a vector of innovation has been challenged by the early attempt of ProtoShares and their Distributed Autonomous Corporations concept, while being recently championed by the Ethereum project which basically consists of a Turing-complete language (EtherScript) and a set of implementations in different languages that can operate the blockchain network and execute EtherScript sequences of opcodes.

The Ether language is close to assembler and it may be considered an assembler language that is not bound to a bare-metal CPU, rather to a P2P network of daemons executing it and using the blockchain as the stack and heap of the execution. EtherScript was published as version 1 counting 50 opcodes and is already undergoing a major rewrite at the time of writing; currently authors promise this rewrite will soon result in an improved version 2, however those using it via Ethereum CLL and its compiler (a minimal language resembling Python that is then compiled into EtherScript opcodes) will not be affected by such low level changes to the EtherScript, as the authors struggle for full backward compatibility across these updates.

In addition to Ethereum it is worth mentioning two more efforts. Maidsafe (maidsafe.net) is also following the smart contracts trend of development and is establishing a platform for distributed application developers.And Counterparty is a "one-way sidechain" grafted from the trust accumulated by Bitcoin and created by "burning" an amount of Bitcoins to create its own units; also Counterparty (http://counterparty.io/) is basically aimed at offering a distributed blockchain infrastructure for smart-contract development and has been adopted as a base technology by interesting applications like StorJ (http://storj.io/) aiming at implementing large-scale distributed storage of data on its blockchain.

Let us conclude this overview with a worthwile note about the "pegged sidechains" whitepaper published by Blockstream, a company that groups together several prominent and well experienced Bitcoin Core developers, which has envisioned in detail the possibility to have "two-way sidechains", proposing a scenario in which such sidechains can inherit the integrity and trust accumulated by bigger blockchains (as Bitcoin) without the need to burn its assets.The pegged sidechain approach may have several advantages over other approaches as those forking the Bitcoin Core to bootstrap new alt-coins, making them more sustainable on the long term; in these regards the implementation being worked by Blockstream may be a real game changer in the current cryptographic blockchain technology panorama, but its way too early now to consider it more than a research topic for D-CENT.

## 2.4 Blockchain as collective trust, identity & reputation management in a distributed system

A full copy of a crypto-currency's blockchain contains every transaction ever made with that crypto-currency, in the case of Bitcoin: at the time of writing, the size of this blockchain is 33 GB. Stored in it, there is all the information needed to find out how much value belonged to

each address at any point in history. The blockchain is relevant for D-CENT social currency pilot communities in that it allows for a new way to collectively self-manage trust in a distributed system. Within the bitcoin system, transactions are the most important bio-political element as they digitally represent economic relations of trust among peers in the network. A bitcoin transaction is only 300 to 400 bytes and has to be broadcasted to each of the nodes participating to the network for a fee to the miner based on the size of the transaction expressed in bytes, rather than actual currency (Antonopoulos, 2014)

More than tracking reputations and propagating them, Bitcoin is a trust management system that allows for the exchange of value in a trust-less environment, in the sense that the two participants to the transaction do not need to trust each other in order to be sure that the transaction will go as agreed. This architecture is indeed very different from the one typical of the financial services industry, where vertical inter-mediating hierarchies and compartmentalization are constitutive and trust in them is an issue to deal with mainly through top-down law enforcement, rather than in force of P2P shared mathematical certainty coupled with crowd-sourced rating mechanisms to counter freeriding - as in the case of legal markets like Bitcoin Central and Microsoft AppStore or illegal ones, as the SilkRoad.
This simply means that bitcoin translated money into a data structure making virtually impossible for anyone to stop the creation and transaction of bitcoins in a structurally transparent and democratic (all nodes are equal peers) environment sharing the same sort of public Panopticon.

Another interpretation of the biopolitical implications of the emergence of Bitcoin is offered by an earlier article published in 2013 by one of the authors of this document:
"The computation of mining, and hence the electricity, is designed to strengthen the authentication of Bitcoin. Now let us consider the energy that was required, before the existence of Bitcoin, to authenticate the minting process of currency made in paper and less noble metals. It consists of a secret minting procedure, big machinery, a monumental building with thick walls and armed guards on its perimeter: an unstable kind of energy, very difficult to govern, as it relates to a monopoly on violence imposed by the sovereign state.
This very energy is substituted by Bitcoin with a qualitatively different approach: Bitcoin distributes peers to the task of building trust in its authenticity. The networked computation of all miners serves as a mint and dissolves the need for violence into an unlimited, unreachable and decentralized power.

Clustering the mint gathers the energy necessary to establish and protect the authenticity of the currency. In other words: participation has substituted violence in tphysical implementation of currency authentication: a recognizable pattern when we observe historical manifestations of the digital plane of immanence." (Roio, 2013)

That said, the blockchain technology still needs betterment before envisioning its full deployment in production environments on which institutions and citizens can rely upon. The blossoming of alt-coin implementations that followed the popularization of Bitcoin more than anything else denotes the importance of the innovation we are focusing on, yet this proliferation of blockchain technologies has not contributed in its stability or to the clarity of code implementations.

While theorists keep pointing at possible future u ses for this technology on the wave of enthusiasm for the decentralization of the institutions managing trust, i.e. managing tolerance to

credit risk, we believe the most important step to take now is to keep the complexity of reliable blockchain codebases low.

The main objectives of the Digital Social Currency pilot concern building community needs and capabilities, rather than develop high-tech software potentially more unstable and difficult to maintain. As the following discussion about deployment of blockchains for the social good will make emerge, low complexity needs to be coupled with the individuation of participatory processes of technical innovation that benefit society, rather than increasing the complexity and efficiency of speculative financial operations of the global corporate sector.

As the role for blockchain's technical innovation becomes increasingly relevant for mission-critical authentication of value exchanges, it is of extremely importance that such technology is independently auditable by any stakeholder relying on it: its source must be open to review and fairly intelligible, well documented and written in a way that facilitates its comprehension. Within the scope of this research project we can only hope to progress towards such goals.

## 2.5 Alternative chains and Alt-coins for the social good

*Alternative chains* are those blockchain innovations inspired by Bitcoin that implement the consensus algorithm and distributed ledger as a platform for contracts, name registration, distributed storage, crowd-funding, aggregate consensus, voting, crypto-equity, etc. Their primary outcome is not a currency system, although they may also present a currency in use among community members. By contrast, *Alt-coins* are crypto-currencies modelled around and do descend from Bitcoin. In this section, we proceed with a brief presentation of alternative chains and crypto-currencies that are explicitly focused on the implementation of the Bitcoin protocol for the social good. This exercise will help shaping design pattern and systemic features of the Freecoin Toolchain.

### *Freicoin (Negative Interest Counter-cyclical Alt-coin)*

"FreiCoin[4] is a decentralized, distributed, peer-to-peer electronic currency designed to address the grievances of the working class and re-align financial interests of the wealthy elite with the stability and well-being of the economy as a whole. Whereas inflationary currencies like the U.S. Dollar or Euro are controlled by central bankers under rules that intentionally or not benefit the establishment, FreiCoin is completely decentralized and self-regulating, with a demurrage fee that ensures its circulation and bearers of the currency pay this fee automatically to those community members who contribute work to secure the currency.
FreiCoin is an implementation of the accounting concept of a proof-of-work block chain used by Satoshi Nakamoto in the creation of Bitcoin. It includes a downloadable client for Mac OS X, Windows, and Linux, and an electronic network for transferring funds denominated in Freicoin world-wide. You can download, review and improve the code of this free software project on Github."

[4] http://freico.in/about/

FreiCoin is based on the opposite of bitcoin's deflationary embeddedness as it represents Silvio Gesell's *Freigeld* version of a blockchain based on Bitcoin. FreiCoin presents a *demurrage,* i.e. a parking fee of 4.5% Annual Percentage Rate for coins stored in a user's wallet. As for every demurraged currency, FreiCoin is meant to boost spending by discouraging hoarding, a crypto-stamp-script.
Block generation time: 10 minutes
Total Currency: 100 million coins by 2140
Consensus Algorithm: SHA256 proof of work
Market Capitalization: $ 130k in mid-2014.
Faircoin *(Global cooperative crypto-currency)*

FairCoin[5] is endorsed by Fair Coop, the Earth cooperative with the aim to develop a global fair economy. FairCoin is the first fairly distributed crypto currency. 99.99% Proof-Of-Stake, FairCoin rewards savers. All the coins were pre-mined and fairly distributed to thousands of people from all over the world. Backed by a strong, diverse and committed community. Promotes prosperity and financial freedom with real value. Working to become the coin of fair trade. Faircoin is the first project where the coins are not bought but rather distributed equally between everyone who wants them regardless of their current financial status, and promotes equality.

FairCoin is a crypto currency like Bitcoin. It is a descendant of Peercoin, meaning the block generation is done by PoW/PoS hybrid.

FairCoin is an important example of pre-mining a crypto-currency explicitly for fair distribution of itself as a social good. FairCoin is a decentralized virtual currency, distributed through a vast airdrop process during the 6th and 8th of March, 2014 (view airdrop statistics). An approximate 49,750 addresses were logged for the giveaway, each able to claim 1000 FAIR per hour. Automated airdrop claiming methods had no effect, as each IP address could register once per hour and 2 different captchas had to be solved. These security precautions were hidden till the day of distribution. FairCoin's vast distribution method allowed a good portion of the crypto-currency community to claim a little bit of the 50,000,000 FairCoins each.

FairCoin Specs:

- POW/POS Hybrid
- 50,000,000 Premined Coins distributed through the airdrop on March 6th and 8th, 2014
- Flat 6%/year minting reward, halving every year until reaching the baseline of 1.5%
- 21/90 days Min/Max Weight
- 10 Minutes Block Target
- 30 Minutes Difficulty Retarget for PoS
- DGWv3 retargeting after every block for PoW
- BlockExplorer: https://chain.fair-coin.org/chain/FairCoin (Official)

## Permacredits *(Equity Crowdfunding)*

Permacredits[6] are the complementary currency for the permaculture movement. Permacredits are token currency usable at any business in the network of Colony Earth vendors. They are

[5] http://fair-coin.org/

used to create businesses and purchase goods from Eco Developments, Permaculture Farms, Permaculture Institutes, Eco Resorts, Conscious Festivals and more. Colony Earth is the corporation of the people by the people run as a Member Owned Global Cooperative.

By joining Colony Earth as a Member Owner one gets access to a global internal complementary currency economy, a robust marketplace full of products, and incredible living environments around the world: "You get to decide Colony Earth's direction, decide the projects and businesses we take on, decide the council members, get paid for your contributions, and more. The future of the world is literally in your hands with our easy, secure, fun to use social E-Governance platform that gives you full control.

To access this brave new world of People, Planet, and Profits become a member today, and co create the world of your dreams alongside similar minded inspiring people from across the globe who share your values and are moving the world forward by taking it back." According to one of the project's founders, Xavier Hawk: "They are a currency, an asset, a stock, a ledger, and a tally all rolled into one. All the vendors and villages in our network will accept them as currency, paying for things like rent, salaries, groceries, Permaculture Design Courses, books, apps, and more. We will be selling Permacredits and using the BTC we raise to fund Triple Bottom Line permaculture based businesses around the world."

### StartJoin *(Equity Crowdfunding)*

StartJOIN[7] is a new style of crowd funding technology. Using social media and crowd technology, it has have created a launch pad for projects to progress. It introduced Concepts and Projects, so that you can showcase your idea at different stages of development, and get community feedback and support throughout: "StartJOIN lets the crowd drive the development of dreams. You can support the ideas you love by sharing, commenting, backing and offering your skills to help."

### *Pegged Sidechains (complementary blockchains)*

Sidechains are a qualitatively different approach to alt-coins: instead of forking the code-base of Bitcoin or rewriting it from scratch, creating new blockchains, they keep using existing blockchains and shape digital assets that can interact with them. An early example of one-way sidechain was previously mentioned: Counterparty. The Pegged Sidechain whitepaper (Back et al., 2014) conceptualizes an evolution of this concept: a "two-way" sidechain that does not require the "proof of destruction" of assets from an existing blockchain to base its own chain of trust. We see this as the most advanced frontier for development and experimentation of systems that permit the existence of digital assets in a reliable and efficient manner. Quoting the whitepaper:

> We propose a new technology, pegged sidechains, which enables bitcoins and other ledger assets to be transferred between multiple blockchains. This gives users access to new and innovative cryptocurrency systems using the assets they already own. By

[6] http://permacredits.com/
[7] https://www.startjoin.com

> reusing Bitcoin's currency, these systems can more easily interoperate with each other and with Bitcoin, avoiding the liquidity shortages and market fluctuations associated with new currencies. Since sidechains are separate systems, technical and economic innovation is not hindered. Despite bidirectional transferability between Bitcoin and pegged sidechains, they are isolated: in the case of a cryptographic break (or malicious design) in a sidechain, the damage is entirely confined to the sidechain itself.

The advantage of this approach is avoiding the techno-political negotiation on changes to be operated on existing blockchain protocols, as well the maintainance and propagation of updates across forked codebases. Rather than forking Bitcoin, the pegged sidechain approach will offer a way to relate new technologies to existing blockchains, inherit their strength and at the same time preserve a certain freedom in developing new architectural approaches.

# 3. R&D Elements for the design of D-CENT Freecoin Toolchain

## 3.1 Freecoin Domains of Innovation

D4.4 is an experiment in digital social currency design. We locate innovation in two intertwined domains both contributing to the advancement of the state-of-the-art in decentralized governance through distributed computing.

(1) Complementary currency governance systems

(2) Digital distributed trust & authentication management systems

1) ***Complementary currency governance systems***: in this domain the Freecoin Toolchain innovates by offering a **decentralized participatory social governance structure** for complementary currency systems. Essentially, the opposite of high frequency trading ruled by robo-journalism instructing algorithms, which in turn trade stocks with none or minimal human intervention. (Durbin, 2010) With a minimalistic reinterpretation of the blockchain technology, the Freecoin Toolchain is a toolkit for community members to easily access and decide on the systemic features of the currency system they use. In general, such social interactions aiming at social sustainability will inform the notion of Social proof-of-work (or proofs) within a community, i.e. the proof that a community has decided on the rules of their own currency system, esp. the possibility to condition the trend of the money supply curve in real time by actions users perform in the real world, according to decisions made within a self-governance setting (see section 3.2, below). Hence, with a system for collective deliberation on the decisions to take for the creation of digital complementary currency, users will engage in collective monetary policymaking in real time by conditioning the currency-creation mechanism(s) under agreed upon dynamics of collective deliberation: for instance, through either quarterly or monthly deliberation rounds (Spain), during special events like participatory budgeting (Iceland) or daily, if the system allows for social remuneration operations (Finland and Milan).

2) **Distributed trust management systems**: in this domain the main innovation that the Freecoin Toolchain offers is a system for **decentralized risk self-management**. In the context of trust management research, D-CENT Digital Social Currency pilots are experiments in reputation management. Reputation is the basis for decision-making in trust related contexts. And trust can be seen as tolerance of risk. (Wierzbicki, 2010) Putting together trust and the blockchain, the Freecoin Toolchain allows for the design and prototyping of systems aimed at managing social currency in a community, i.e. reputation in a decentralized fashion: for example by using micro-endorsements as collateral/backing of the underlying complementary currency (Spain), risk is spread evenly among participants; or by participatory rewarding best political contributions (already happening with participatory budgeting in Iceland) and use those credits

as loyalty scheme vouchers in the related municipal area, whereby rewards for good proposals for the common good lower the risk to promote proposals that go against the common interest of the citizenry; or still by publicly recording and rewarding one's contributions to a community supported cooperative in Helsinki, thus testing the behaviours and habits of members belonging to communities that self-process themselves as fair and honest (see Appendix 1, below). In all three pilots, trust management is related to collective risk and Freecoin tools will underpin experiment around decentralised and bottom-up trust management.

## 3.2 Replacing Bitcoin algorithmic proof of work with a Social Proof of Work

Now let us emphasise an important outcome of the techno-political analysis carried out in this paper, building on both the analysis of use-cases in D3.4 and the work of Christian Marazzi[8] it seems to be a limitation for the POW to be a mechanic process, a condition verifiable across all existing blockchain implementations. On the contrary, the main driver for a desirable anthropo-genetic economic model, i.e enhancing human economic development. In effect, in terms of currency creation dynamics, the consensus algorithm that conditions the issuance of new coins is technology driven and mechanistic. This central function of the algorithm that authenticates currency creation is extremely important in view of structurally neutralising counterfeiting. However, this may also be seen as a departure from an active and critical engagement among humans and machines, whereby the creation of money in the system is motivated by social interactions for the common good, rather than by exclusively hashing cycles. Therefore, the task of the research in D4.4 seems to configure as a quest to redefine Bitcoin's 'proof of work' and the reward of a blockchain system, in order to devolve the power into the hands of people through a democratic decisional processes.

We experiment within a scenario whereby human decisions deeply influence the behaviour of algorithms and not the opposite. The literature review on the blockchain technology, its bio-political critique and promising implementations for the social good, make emerge a new way to look at the relation between the participatory democratic process and the blockchain technology in the context of the governance of complementary currency systems. Within the scope of the D-CENT project, the Digital Social Currency pilots will experiment and test a new notion of proof-of-work: **the Social Proof-of-Work**, which is the proof that a member in the system is endowed with coins as a reward to an action in the real world while abiding to community rules and enhancing collective values.

As it is the case with the design of traditional complementary currency systems, also in the case of crypto-currencies and blockchains programmed with Freecoin, **Social POW will be tailor-made and agreed upon by the community of users of the crypto-currency**. For instance, in Spain POW will be in the form of a **Proof-of-Business** as concrete economic transactions in a B2B context. In Iceland, the POW will be a **Proof-of-Political-Participation** as online engagement to reward users on Your Priorities platform, while in Finland it will be

[8] http://mitpress.mit.edu/authors/christian-marazzi

**the proof that somebody performed cooperative work** and had honestly remunerated themselves for that.

In brief, the acts of endorsement, giving reward and social remuneration are three ways to conceive the SOCIAL POW by harnessing the signature capabilities of members in order to condition the supply, circulation or remuneration of money. The design challenge for the Social POW is to replace the strictly deterministic and algorithmic trend of crypto-currency supply (Gold Standard-like) with a more flexible and interactive process of currency creation. Communities act in the real socio-economy, thus the Social Proof-of-Work should reflect communities' democratic agreements and collective needs, and the algorithm should adjust the money supply according to such inputs.

The outcome of this shift in design is twofold: (1) people engage in transactions that have real world desirable impact that they produce and collectively construct; (2) it is possible to go towards self-managed decentralised currency systems (with desirable consequences for credit risk management practices). In this way, new participants can enjoy an egalitarian economic environment by avoiding the undesirable condition of structural advantage by early adopters of a currency. At the same time this would allow to have complete democratic oversight on transaction history and collective deliberation on social currency systems' rules of engagement and reward.

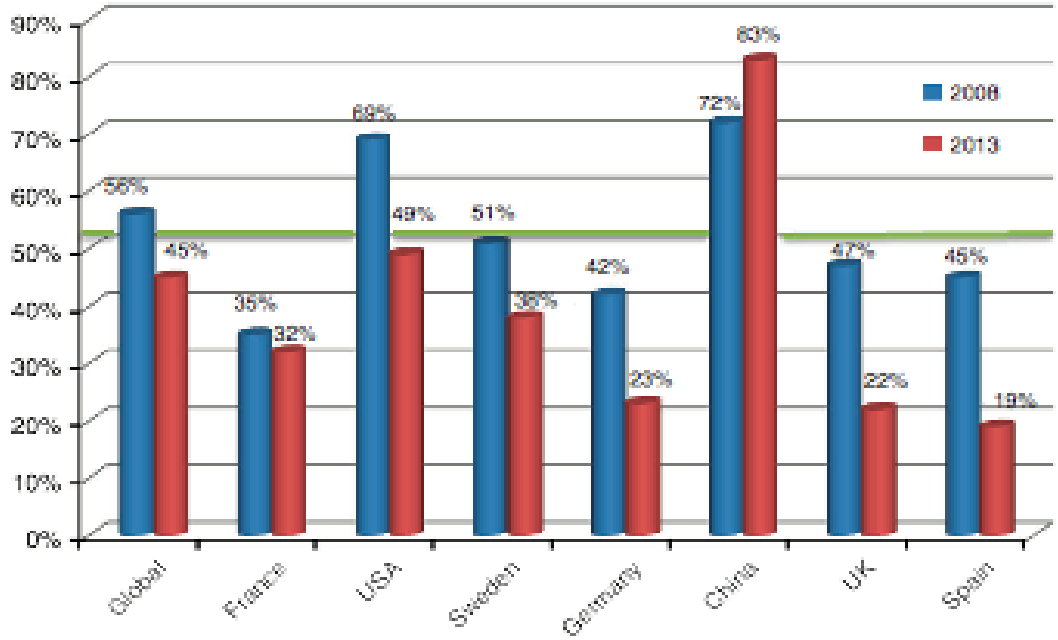
## 3.3 D-CENT Digital Social Currency pilots as experiments in distributed trust management systems

Apart from purely technical issues concerning the blockchain, the design of the D-CENT Digital Social Currency draws also from the most recent findings in Trust Management Research. Trust management dynamics are in fact an element which is common to both the Direct Democracy and the Social Currency domains of the D-CENT Platform. In the collective decision making processes within D-CENT pilot communities that already present a high degree of trust built in the analog world, there is the possibility to exploit such confidence among community members in order to build with the blockchain technology new political and economic incentive mechanisms that foster the social good. In turn, Trust Management Research offers those elements that will then go to frame more in detail the notion of Social Proof of Work, i.e. the proposal to shift the process of authentication and circulation of crypto-currency from an exclusive focus on impersonal mathematical proofing on machines to one where currency creation - albeit supported by machines - is authenticated by users through self-management as the main organizational propeller.

Humans use trust when making decisions under uncertainty. As a working definition of trust within the context of the Digital Social Currency pilots, "trust in some way represents an actor's (trustor) expectations about another actor or object/institution/organization (trustee), that one believes is willing to depend on another party" (Schoorman et al., 2007). Trust is a relational notion. From an institutional point of view, one can see that the institution creates

the actor as much as the actor creates the institution (Kroeger 2013). Moreover, for institutionalized trust to persist it needs to be continuously 'brought to life' through interaction (Berger and Luckmann, 1967). In the context of the social currency pilots, the social relation of trust is to then be translated in the social relation of money as a common good. In other words, within D-CENT, money is an agreement within a community to use coins circulating on a blockchain as a means of payment self-managed as a common good.

The evidence that this issue isn't a trivial one is the massive loss of trust in the conventional money post Lehman-collapse in the financial services industry.. Indeed, collective trust in banks experienced a major decline after the Global Financial Crisis, and this is true on a global basis with the exception of China where data have been questioned (Hurley et al., 2014):




**Source:** Edelman (2013)

**Figure 5: percentage variation (between 2008 and 2013) of people who trust banks to do what is right.**

Even before the Global Financial Crisis, some had noted that the idea of institutionalizing trust may hold the promise of making trust more stable and enduring (Dasgupta 1988). Accordingly, Freecoin Toolchain design is based on this orientation toward trust as an institution innovatively deployed on a Collective Awareness Platform such as D-CENT and backed by *trustless* blockchains.

Trust building can be acknowledged as the expression of a 'symbolic action': actors engage in actions that are apt to signal their trust and/or trustworthiness to each other (Kroeger 2013). In turn, symbolic exchange is clearly a manifestation of 'active trust' (Kroeger 2013). What is more remarkable for the design of the three Digital Social Currency pilots in D-CENT is that in

unstructured settings the introduction of symbolic statements can order perception so that the symbolic presentations is perceived as real (Cuzzort and King, 1989). The Freecoin Toolchain offers indeed tools for the digital management of virtual trust relations that have real world impact.

In this way, users will be endowed with the power to create, assign or simply track digital social currency while using it to exchange value and, therefore, to monitor trust flowing within a community in real time with tools like a decentralized digital payment system, a crypto-wallet and a blockchain explorer, respectively. As the process will take off from prototyping toward the production of a stable Minimum Viable Product, Freecoin interoperable blockchain tools will become an experimental instrument to transparently orient collective perception and awareness toward the circulation of value in a dis-intermediated environment under users' control of their own symbolic statements around trust, i.e. reputation management for credit risk management purposes.

The practice of developing, implementing as Minimum Viable Product and finally using the Freecoin Toolchain in a collective open setting is a way to represent - digitally - the institutionalization of trust, which is a process of 'socialization' (Berger and Luckmann 1967) that from habituation, routinization and typification leads to institutional 'structure', whereby the typifications of trust behavior function as 'trust templates'. (Kroeger 2013) Although it will emerge more clearly with the scenario building for each pilot context of the Digital Social Currency, it is worth noticing here that the institutionalized trust templates provide (1) symbolic cores and (2) a 'writing guide' for symbolic action that suggests how to structure more specific personalized meanings around those cores (Kroeger 2013). In the context of digital social currency systems, the institutionalization of trust is therefore regarded as the process of 'socialization' of trust templates, i.e. the transmission of institutionalized trust patterns between individual actors, in this case related to the social economy in terms of credit risk management institutionalization itself is only complete when the objectified patterns are passed on to third actors and further replicated reliably with the mediation of digital devices.

The process of institutionalization via socialization of trust begins with a new actor entering the scene. Members of the network introduce the newcomer to the typifications they have already created to form the trust relationship, i.e. the Social Proof-of-Work. We envision the Freecoin Toolchain as a set of tools to facilitate the creation of horizontal circuits of value that digitalize trust relationships in a social networking context in order to link unused resources and unmet needs among like-minded peers in terms of endorsement (Spain), reward for political participation (Iceland) and remuneration for work contributions (Finland). According to Kroeger (2013), in this process, the patterns are typically communicated as fact ('this is how things are done'). That is, the new actor encounters the roles and routines for trusting as a pre-existent 'facticity outside of himself' (*Ibid.*)'. At the same time, the fact that the original creators of the patterns witness this process produces a 'mirror effect' through which institutional reality 'thickens' and 'hardens' for them too. (Berger and Luckmann 1967). Throughout this iterative dynamic of trust transmission, the process of objectification is then complete. In this view, Digital Social Currency design for D-CENT pilot communities is an experiment in the institutionalization of trust patterns already present in those communities, but lacking the digital infrastructure to make institutionalization viable.

The main tenet that underpins this inference is that intelligent digital tools for collective social networking can help trust become long term: socialization allows the institutionalized trust

patterns to become a collective characteristic of the organizational team or subgroup. More precisely, trust can be long term, *because* it is collective in nature. (Kroeger 2013) Cross-generational transmission of trust templates allows them to become long term in nature - in particular, more long term than trust, which is a property merely of a dyadic relationship. And this applies also to the codebases for trust management and complementary currency systems that communities will adopt on the D-CENT platform.

In this sense, the main challenge for the design of the Freecoin Toolchain is then to objectify trust - without reifying it and, therefore, the dyad trustor/trustee - and transmit it across generations of organizational actors by means of software codebases for distributed trust management systems. In brief, D4.4 looks at ways to frame the socialization of trust by exploiting the architectural features of the structurally transparent blockchain technology and human engagement in pilot communities.

As findings from trust research in offline settings encouragingly show, the core of an (inter-)organizational trust relationship can therefore be maintained even beyond the point at which the original creators of the trust relation have moved on and left the organization. Counter to the assumption, implicit in much research and practice, that trust disappears when a participant leaves the relationship, this perspective posits that trust (that is ways of signaling, building, using trust) can become an attribute not just of individuals, but of groups, teams and organizations (Kroeger 2012). Since both trust - or a 'promise to pay'/IOU - and codebases are virtual, running trust management on a blockchain is remarkably worth a try.

The notion of Trust Management has been introduced in academic debate by Blaze (2005). In relation to IT and when the users of the system are human, Trust Management is an area of information technology that aims to improve the operation of open, distributed systems by predicting or influencing the behavior of their users. When applied to human users, Trust Management methods attempt to leverage the human capacity for trust or distrust. (Wierzbicki, 2010) Trust management can be seen as a symbol-based automation of social decisions related to trust, where social agents instruct their technical representations how to act while meeting technical representations of other agents. In the context of the D-CENT project, pilot communities are the very settlers of the rules governing the trust management system that they self-manage.

Further automation of this process can lead to automated trust negotiations (e.g. see Winslett, 2003) where technical devices negotiate trust by selectively disclosing credentials, according to rules defined by social agents that they represent. (Wikipedia) As Smart Contracts are already indicating, in the future trust management may become yet another standard service of information security, such as authentication, authorization, privacy or integrity (Wierzbicki, 2010). Most Trust Management systems use simple computational representations of trust. Internet auctions, for example, use a three-valued discrete scale of "negative", "neutral" and "positive" (with the exception of the recent system used by e-Bay, namely the Detailed Seller Rating system).

**The Freecoin Toolchain aims to advance the state-of-the-art in the design of Trust Management Systems, in which trust is collectively self-managed by virtue of ad hoc implementations of the blockchain technology**.

Distributed trust can be measured for example, by Trust Units informing the money supply of a regional complementary currency (Spain), political-reputation rewards tokens (Iceland) and the

social remuneration scheme from a common pool of complementary currency owned in a decentralized framework (Finland and Milan).

## 3.4 The Freecoin Toolchain: a suite for building blockchains *complementary* to Bitcoin

Most of the projects derived by Bitcoin are in alpha stage. They show a wide participation base of developers and are comprised of large amount of fairly complex code, mostly in C/C++ language. It must be noted that the attitudes of all organizations behind these developments are genuinely leaning towards free and open source values and their licensing is compatible with the Free Software Foundation's ethical guidelines for free software. Furthermore, some projects show cooperation among each other, as in the case of Ethereum and StorJ, making it reasonable to think that there can be a multifaceted set of projects surviving the hype on the long term and possibly sharing common components.

It is very difficult to understand at this point in time what codebase will be established as a reliable standard in the coming future: perhaps there will not be a single one, but a range of specialized codebases that are hopefully not duplicating code, but sharing a fair amount of research & development and even security patches necessary to stabilize them beyond beta stage.

In these regards what we call the Freecoin Toolchain should imply documenting and testing a blend of interoperable components from such platforms, with modifications and adaptations to fit the purposes of the pilots we are studying. However, while hoping that our use-cases can inform the general development of blockchain technologies, it is hard to predict whether we can reach stable solutions in the limited span of this project. Having to choose a development direction, we should struggle to find the development path sharing most compatibility with others, yet respecting the particular focus we have on community needs in D-CENT.

It must be noted that most of the blockchain technology projects we have analyzed start from the concrete historical use-case of Bitcoin, but then elaborate in a rather abstract way on the future needs and desires of a user-base that doesn't yet exists or hasn't yet expressed the need for a cryptographic blockchain application. It is often too optimistically envisioned the situation in which users would adopt such technologies for their specialized advantages, as for instance "smart contracts", despite them being far more complex than central authentication and database or filesystem storage. Here probably lays the biggest gap to be filled by the D-CENT project: understanding what feasible and reliable tools can be made, what minimum viable blockchain technologies we can envision, develop and integrate with existing systems, to fulfil the needs of real use-cases dealing with e-democracy and trust management. While doing that we shall keep well conscious of the fact that liquidity and trust can definitely be made abundant by better communication tools, reliable authentication and resilient storage.

We may then envision that our biggest possibility to contribute an advance in this research field lays at the junction between economical analysis, field research, technical awareness and standardization processes, keeping our attention on the reliability, usability and long term

maintainability of the blockchain technologies that we are contemplating. The upcoming implementation phase may engage the contribution of code, documentation and analysis of a certain blockchain toolkit, but we must be cautious about its immediate deployment in pilots, at least until the development phase of underlying protocols reaches a beta stage. As shown by the difficult attempts of colored-coins, the chaotic multiplication of alt-coins and the necessity for a stable and far sighted analysis like pegged sidechains to be conducted by developers of Bitcoin Core, it seems clear that the establishment of a standard will come at a slower pace and will likely be linked to the most popular protocol of all, the Bitcoin blockchain.

# 4. The Freecoin Toolchain Technical Design

## 4.1 Description of systemic features

Features presented at the end of each application to pilots are the result of a deconstruction of the Bitcoin blockchain technology in order to scale bottom up cooperation for the social good.

The existing dynamics observed in pilots show that it is possible to ignite virtuous economic behaviour when users share the same set of values and agree upon the same set of rules for managing their economic relations of trust with a social currency created out of those very interactions: B2B endorsements in Spain or citizen engagement social credits in Iceland are bottom up examples of decentralized collective engagement in monetary policymaking.

With regard to the pilots (See Annex 1), it must be noted that the necessity expressed varies the most between these two cases:

In case of **Eurocat in Spain** the need to withdraw endorsements is expressed clearly, but that collides with the inherent features of blockchain-based credits, which mostly consist of "digital assets" that cannot be controlled by a central authority. In such a case it is recommendable that decentralized technologies and architectures are deployed for the resilience of the data storage (both of transactions and individual wallets), but the Eurocat system itself appears to be designed to be best operated in a centralized fashion, based on a central database.

In the case of **Iceland** there is demand for sustainable innovation of the sort of complementary currency that can be gained through Social Proof-of-Work (socially relevant activities recognized by the community) and then spent independently on relevant services as for instance public transportation, across already digitized infrastructures that could be made compatible with the circulation of blockchain based credits. In such a scenario is easier to envision and deploy a decentralized credit system that is in fact fitting the needs expressed with the basic features offered by the Freecoin Toolchain, and more in general blockchain technologies.

Such a substantial difference between the two pilots leads us to establish priorities and choose as a primary pilot Iceland, where the need for a decentralized system of credits like the blockchain is clear expressed and can be deployed in cooperation with the municipality of Reykjavik. This pilot can be also more easily linked to the overall DCENT platform, since the Icelandic case can be easily replicated in the context of other network democratic experiments we are running in Spain and Finland as part of Pilot 1.

As concerns the Social Proof-of-Work, the algorithm dedicated to currency creation has to be informed to a significant extent by real world engagement dynamics of community members in the respective contexts and with a transparent architecture. In this way, the consensus algorithm for the Freecoin Toolchain should be instructions coming from the social context through democratic users engagement, rather than a priori digitally encoded instructions.

Together with the development and documentation of the Freecoin Toolchain for ad-hoc blockchain development, the link between Social POW based on democratic decision-making and the effective creation of digital coins is probably the biggest challenge ahead for this research. There are two approaches we envision:

1) Creating a new blockchain and adapt its features so that there is a useful and finite amount of pre-mined coins in the hands of the community and that any mining following it is not creating more of them, rather than contribute to the circulation of transactions. In this way, the incentives to gain are not applied to mining (which may be operated by collectively owned mining infrastructure) but to actions whose values are recognized by the Social POW democratic decision process. This is potentially more effective and leading to immediate results to be tested on the ground during our user research and pilots.

2), Creating a sidechain supporting a more advanced scripting setup to link directly the Social POW decision making process to the algorithmic creation of credits, in fact eliminating the human intermediation for the distribution of credits and making them appear in people's wallets, as if Social POW would trigger mining results. This solution is more advanced and experimental, not necessarily leading to immediately deployable results.

The first approach resembles the solution adopted by Faircoin in pre-mining a fixed amount of coins. Changing the software (Bitcoin 0.8 in this case) to reward down to 0.001 for mining basically meant to support the network and not to distribute coins. The advantage of this solution is clear when we consider that it adopts Bitcoin Core as the starting point and, while developing yet another alt-coin informed by this research, it can keep in sync with the most reliable (and de-facto reference) software implementation for blockchains, as well inherit its compatibility with a vast range of tools built for it.

The second approach recalls the efforts made in projects aiming to implement blockchain scripts and "smart contracts" and more advanced features which we possibly see as useful in future, but as of today are too premature and unstable to be adopted within the span of this research project and produce any tangible result that can be effectively deployed in real world large scale pilots.

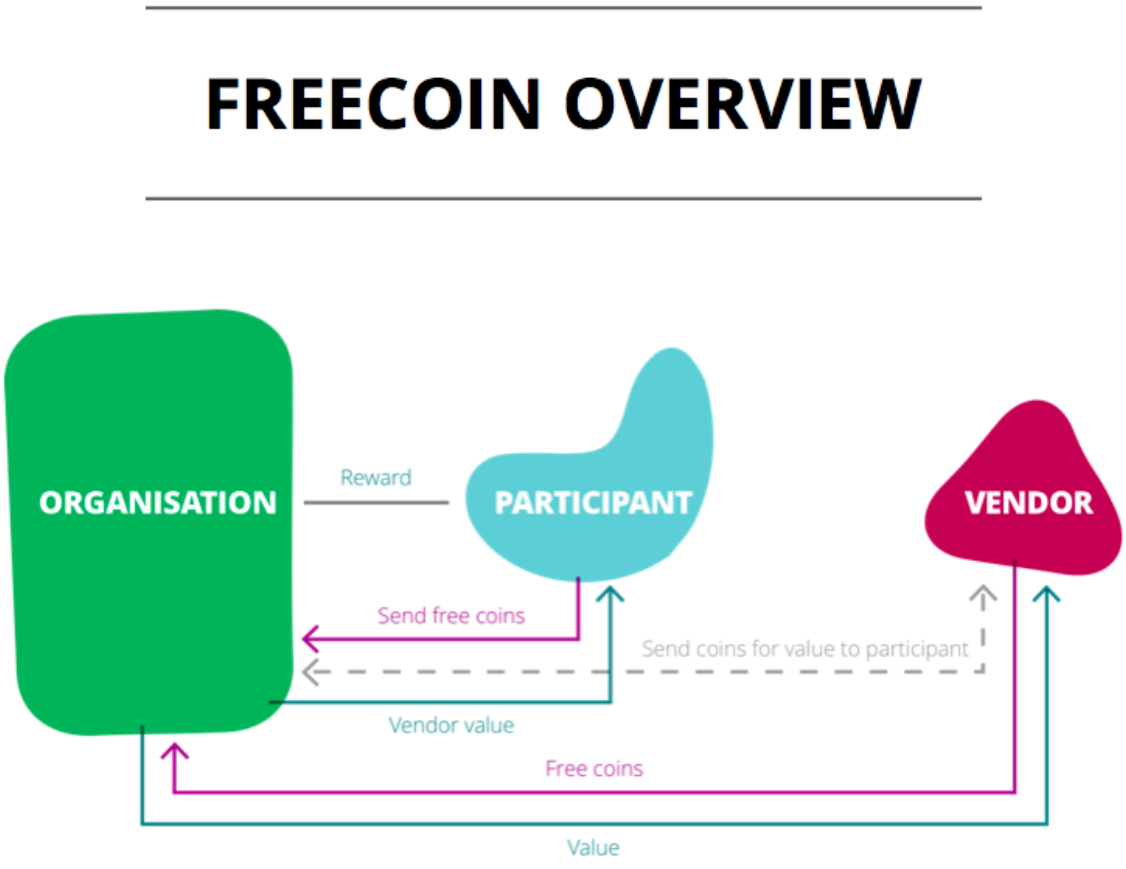
There are two main systemic features we intend to apply to existing and new systems adopted by pilots and they represent a clear innovation, beyond previous implementations of complementary currencies.

1) **decentralized and resilient storage of data commons**, relying on the possibility to establish a relationship of shared stewardship among participants.
2) **ubiquitous wallets** meaning that assets owned by each participants will be stored on the blockchain whenever possible, granting decentralized access to it via a secret and without being bound to any physical device, in fact envisioning the possibility for public points of access.

The latter in particular is a basic ingredients of the Freecoin Toolchain which will further experiment on the parameters that influence the nature of currency, economic or financial systems that a community wants to design and use for decentralized circulation of value backed by the very community's trust patterns. As the application to pilots showed, by playing with this parameters it is possible to define a pattern language for the design and implementation of open-source and tailor-made decentralized trust management - viz. social currency - systems.

These are the implementation elements we see as a Minimum Viable Product for the implementation phase (D5.5) and the integration (D5.6) to follow. Such an MVP will be deployed as much as possible in cooperation with pilots, still considering its highly experimental nature.

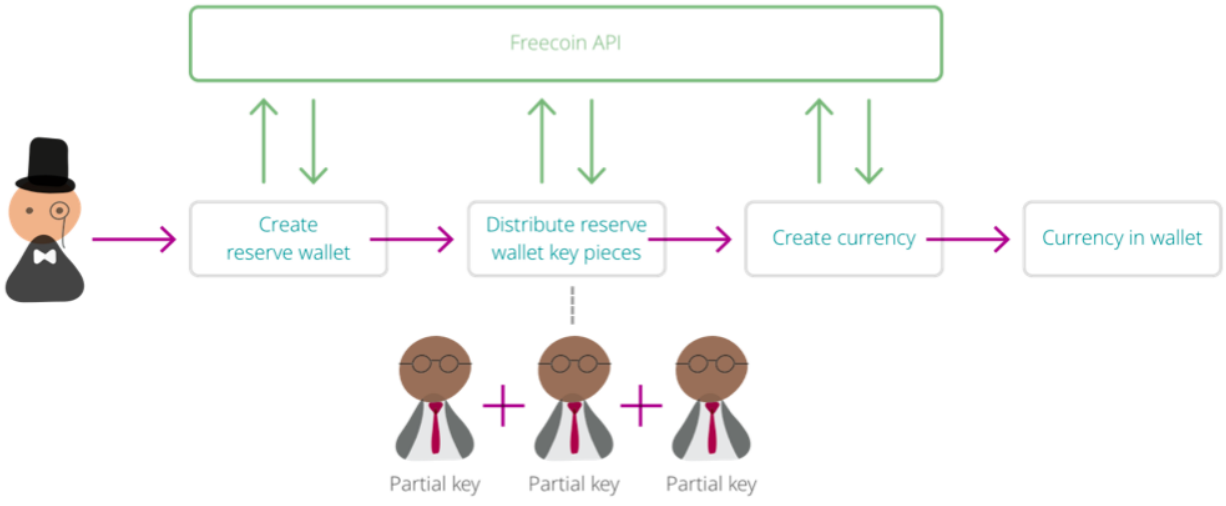
We believe that blockchains were invented specifically for the Bitcoin project but they can be applied anywhere a distributed consensus needs to be established in the presence of malicious or untrustworthy actors. This is the case of the pilots and uses-cases presented in D3.4: D-CENT pilot communities have the need to reach distributed consensus on their respective issues, being them about either trust management for regulating monetary policy of a regional currency system (Spain) or the exchange of social credits and their spendability (Iceland), etc. Notwithstanding, a desirable implementation of a decentralized and transparent digital social currency might be potentially extended to the financial services industry and national public economies.



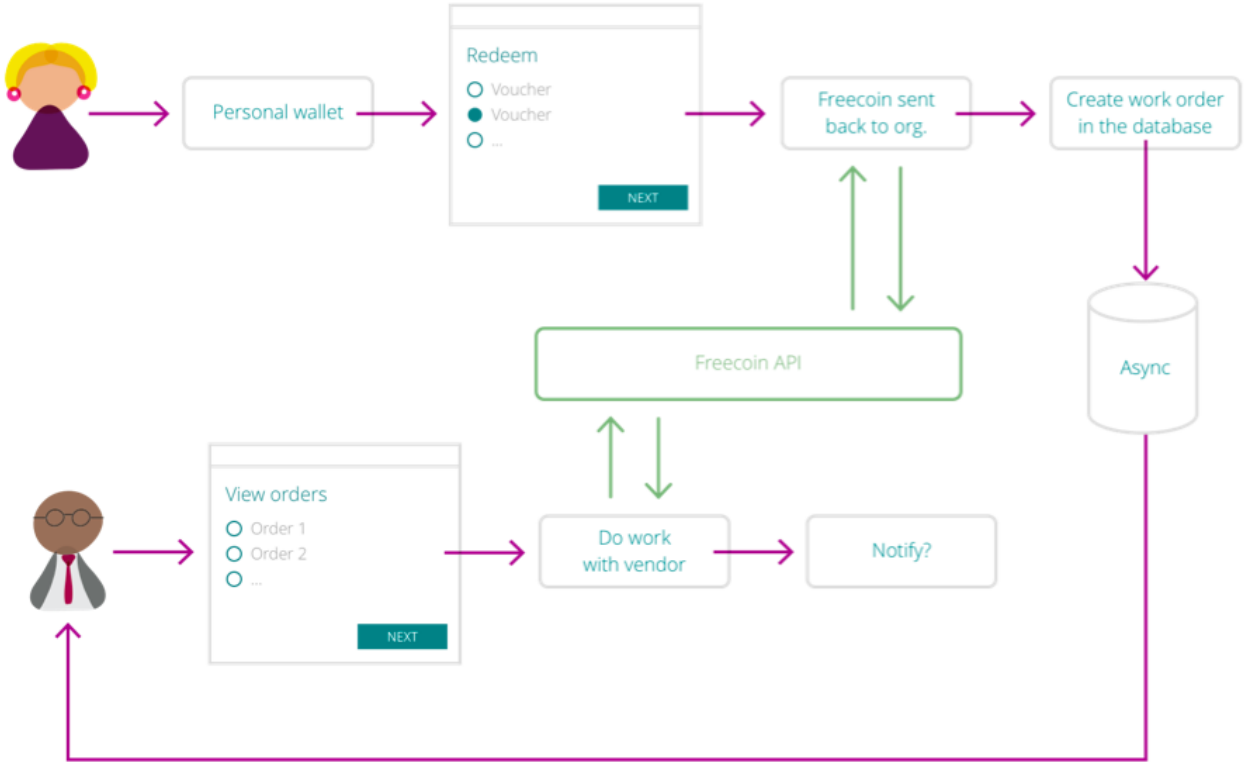
# JOURNEYS OVERVIEW

- ❑ As an organisation I want to create a currency
- ❑ As a participant I want to exchange Freecoins for value
- ❑ As a participant I want to create a wallet
- ❑ As a participant I want to lookup a Wallet
- ❑ Create incentive
- ❑ Check Freecoin balance
- ❑ Transfer Freecoins
- ❑ Award currency

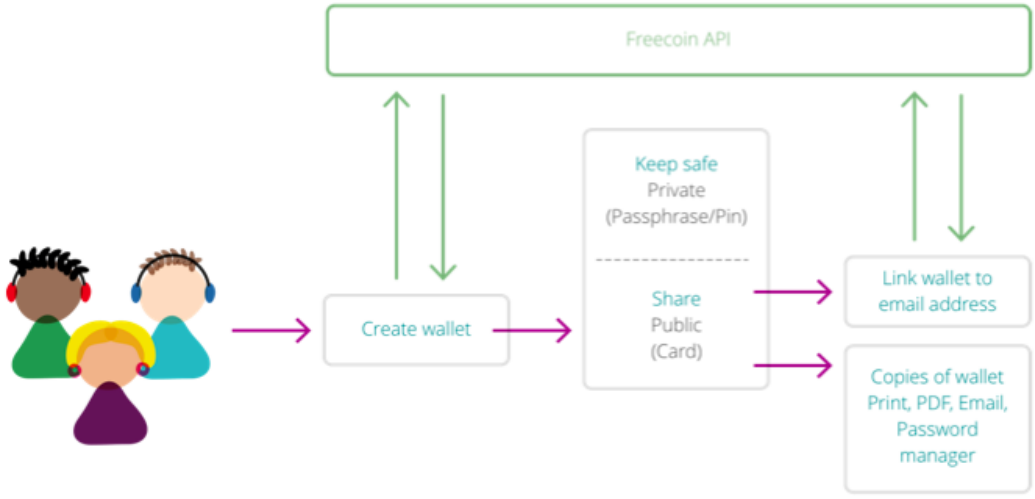
## As an organisation I want to create a currency



## As a participant I want to exchange Freecoins for value




## As a participant I want to create a wallet



## Transfer Freecoins


Participants are able to transfer currency between themselves. This could form the basis for a community reward or 'kudos' system.

## PROPOSED 'LEAN' ARCHITECTURE

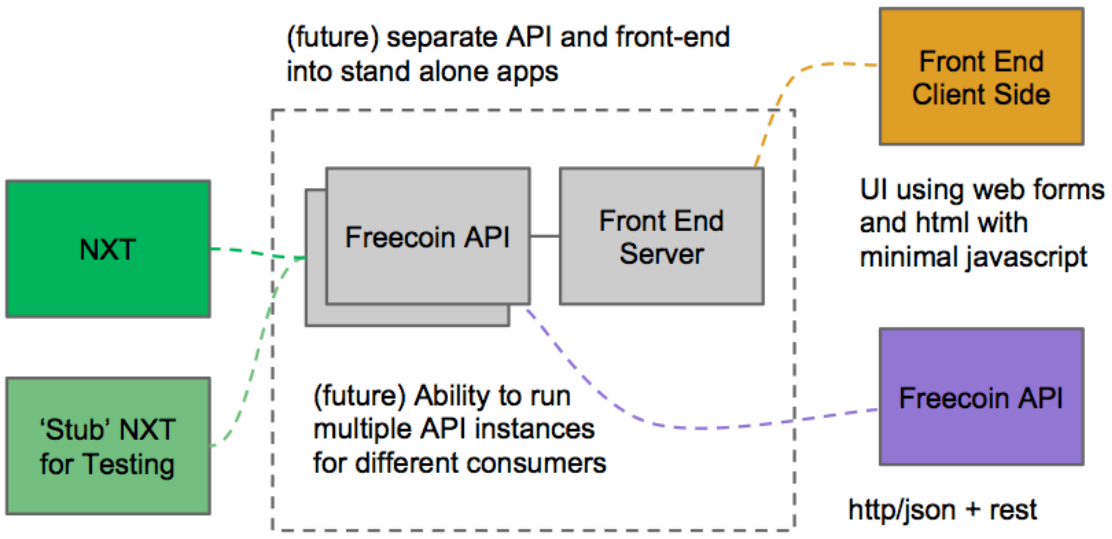



Figure 6: freicoin overview

## 4.2 Exploitation beyond Pilots

Exploitation of the Freecoin tools and features ranges from use-cases that may run in parallel with new governmental innovations for the recovery of national economies such as Greece or the trust management dynamics shaping the structure of the financial services industry at the aggregate level.

From a technical design point of view we believe that even beyond the span of this research and its application to pilots it can be of great interest, both for business and social potential, to develop and document a Freecoin Toolchain software kit based on Bitcoin Core 0.10 and capable of bootstrapping the genesis of new ad-hoc blockchains integrating the work done in the e-democracy D-CENT pilots and the Social POW concept, implementing a sustainable mode for operation of the blockchain, also environmentally sustainable.

The Toolkit should come with client wallets and a server infrastructure that can be operated by ICT professionals and on which more layers of integration can be developed to interface it with the existing "smart city" infrastructure. As we graft such development on the Bitcoin Core codebase and compatible software like Libbitcoin, such layers of integration would obviously feedback into the mainstream open source panorama and interest use-cases even beyond the ones we are contemplating.

Beyond inflation and deflation, the Freecoin Toolchain is an experiment in decentralized digital currency design that aims to allow for a self-adjusting money supply by harnessing the inputs of users in a currency system. By linking democratic deliberation with currency creation through the Social Proof-of-Work, systems can be designed to enable a flexible currency supply set in real time at the light of users trust management dynamics, also taking as example the experiments lead by Freicoin with the demurrage of coins (based on Bitcoin Core 0.8).

# 5 Conclusions: What is success for Freecoin and how to measure it?

In order to propose a set of metrics and indicators to assess community impact and community resilience as an outcome of the use and growth of Freecoin, we have to consider the differences between Freecoin tools and features range from use-cases.

Referring to the main features we individuated for our research to contribute to pilots, we may consider three different cases:

## 1) Distributed storage architecture

A clear indicator of success will be the effective deployment of at least 3 nodes for each formerly central database adopting this feature. Such nodes should be held by participants to the network, whose participation is incentivised, a well-communicated principle of stewardship for data commons. Scaling to more nodes is advisable and such a scaling should tend to be device-centric rather than mixed up on multi-tasking systems.

## 2) Blockchain based complementary currency

Measuring the success of a currency is relatively easy and mostly bound to its quantitative nature. We should also look at the political acceptance of the currency by top-down institutions, which binds the success for this aspect to the overall work done by D-CENT as a whole, in having perceived the application of such tools as a reliable source of information, aggregation and quantification for behaviours contributing to the common good.

## 3) P2P trust management

The success of this feature when applied to pilots is tightly coupled with the developments in e-democracy and the level of integration of the two main pilots in D-CENT, establishing a connection that is as seamless as possible between the distribution and circulation of social credits and the political process of deliberation that take place in the assembly.

When looking to this features themes, it is important to remember that Freecoin is not a currency, but a suite to create P2P currencies**,** in order to scale bottom up cooperation for the social good. This happens by giving pilots a tailor-made Digital Social Currency as reputation management in terms of tolerance of risk to a distributed allocation of credit created among engaged members. Accordingly, the general rationale for success is the following: If the tools of the Freecoin suite will increase both sensibly and reliably such decentralized allocation of credit through the set of features summarized above, Freecoin will be considered a successful codebase for decentralized trust management and complementary currency governance systems.

## 5.1 Indicators of success

In each pilot, we will monitor the usual measures for determining the performance of currency systems and their social impact. We propose to define "social impact" as follows: the social and cultural consequences for pilots' populations of the introduction of Freecoin. Social impacts, in this field, involve the ways in which people relate to one another by means of Freecoin tools, and the way they organize to meet their needs, and generally cope as members of community, as well as changes to the norms, values, and beliefs of individuals that guide and rationalize the political process of deliberation.

Alongside quantitative metrics, we will also measure the impact and related a success of the Freecoin tools in the different contexts through qualitative research mostly in terms of storytelling by the users - Are people happy? How many social events are happening? Are the tools helping developing a more resilient community, and more inclusive economic models? Is there more, political participation, cooperative agriculture work, overall regional economic resilience, more music, art, crafts and theatre than before the Freecoin Toolchain started to operate in each pilot and use-case context? Are citizens protecting and enhancing their local common good?

More generally, it is possible to defined impact indicators by comparing D-CENT pilot outcomes to the success of best practices emerged from the work of researchers and practitioners of complementary currency systems:

**Indicator #1. Increased volume of currency in a local area**

Given that the volume of conventional money in a local area is scarce, evidenced by the level of underutilized human and material resources in a given area, Freecoin tools should increase the *volume of transactions in a local area* to mobilize these resources. The *velocity of money in circulation* may increase. Higher velocity means the same quantity of money is used for a greater number of transactions and is related to the demand for money. It is measured as the ratio of GDP to the given stock of money. Impact indicators can be adjusted to the measurements needs of each pilot during prototyping in WP5.

**Indicator #2. Increased employment opportunities**

Freecoin tools should give their participants a safe way of trying out their new employment choices, by improving the *local rate of employment.*

**Indicator #3. Increased importance of traditionally undervalued activities**

Community members themselves decide the value of childcare, artisan skills or community organizing, by establishing a connection between the distribution and circulation of social credits and the political process of deliberation about the community sector. The *rate of growth of community sector activities* endorsed by means of P2P trust management is a measure of the community impact of Freecoin tools.

**Indicator #4. Increased strengthening of social relationships**

Freecoin tools are intended to help the members of a society to reinforce and create social networks. In order to measure this feature we will use the *increase in the number of individual citizen that actively participate to decision making process by using D-CENT platform* and the

*increasing engagement with local democracy, associations and organizations* by means of Freecoin tools.

### Indicator #5. Counter-cyclical economic tendency

Some complementary currency systems provide a beneficial countercycical impulse to the economy. During periods of recessions, the volume of transactions and the number of participants increases, while the opposite happens during boom periods. The most detailed study in this respect involves the Swiss WIR currency in several studies by Professor James Stodder Stodder 2000, 2009). The WIR is the oldest continuously complementary currency system in the world: it was started in 1934 and involves today some 70,000 Swiss businesses. This provides 80 years of high quality data. Stodder's studies prove that the WIR system plays a significant counterccyclical role in the Swiss economy, stabilizing particularly GNP and employment.

### Indicator #6. Reduced need to migrate to urban areas in a search for money

The last impact indicator refers to a correlation between the implementation of Freecoin tools and the net migration rate of a geographical area. If there is enough income to mobilize local production using local resources to meet local needs, people do not need to migrate to different urban areas in order to earn money.

# Annex 1: Freecoin Toochain Application to Pilots and Use-cases

As we presented in the design document above, the Freecoin Toolchain is the result of the features-building process conducted with LEAN-UX methodology in WP1 and WP3. The design of decentralized complementary currency and trust management systems for T4.4 has been directly informed by the needs of the communities piloting the Digital Social Currency on D-CENT. We analysed the qualitative data gathered during 2014 and below there are the various applications of the Freecoin Toolchain to the pilots' contexts. For each pilot in Iceland, Spain and Finland, a description of system, a scenario and a pilot-specific list of features are proposed. Finally, a variation of the third pilot (Finland) is proposed for one of the use-cases identified in D3.4, namely the experience of art and entertainment workers at Macao, Milan.

- **Iceland:** 'decentralized complementary currency system for Your Priorities;
- **Spain:** Decentralised application to be integrated to the Community Exchange System for Eurocat;
- **Finland and Italy:** Decentralized bottom-up social remuneration for Helsinki Urban-cooperative Farm and Macao cultural workers in Milan.

# Pilot 1 (Iceland): Social Kronas – Political-Reputation Tokens for Your Priorities

The pilot with the richest potential in terms of experimentation on Digital Social Currency is currently the Icelandic one. The Icelandic pilot can be seen as experimentation in distributed reward mechanisms for political engagement, within the prioritization of best political proposals by citizens. Indeed, Your Priorities is a platform that already contains a reputation system that distributes 'social credits'. A member earns rewards called 'social credits' in the form of digital tokens by other members who vote for that proposal during Reykjavik Participatory Budgeting event. Since social credits are assigned to those that deliver the best political proposals in the participatory budgeting events, it became clear during our research that those credits could be spent in the local economy, turning them into Social Kronas recognised by the Reykjavik City Council.

D-CENT's Digital Social Currency pilot in Iceland relates to the experimentation around political participation and political reputation linked - by a reward system - to the local economy of Reykjavik. The basic idea is to translate the civic action and citizen active political participation in the city policies *into* a social credit that can be spent to access real local public goods/facilities and services. In this way citizens serve the community and are served back by the community in a decentralized and self-managed digital network recognised by the city's democratic institutions.

Your Priorities eDemocracy software already provides a reputation system that dispenses social capital in the form of *social credits* to users proposing ideas that are then prioritized by the rest of the community (Social Proof of Work): 165 of them have been formally reviewed and accepted by the City Council since 2010. However, at present these credits cannot be spent in the socio-economy of Reykjavik: rewards are assigned, but they do not translate into real value. Hence, in order to foster citizen engagement with real rewards, D-CENT is co-designing blockchainenabled tools that can transparently manage the creation, storage and circulation flow of Your Priorities social credits within the city economy.

Social credits will be created by users themselves in the act of voting (or distributed to users for voting). By harnessing their political and civic engagement, users will receive *social-coins* / *social-krónas* in their personal wallets: digital tokens or vouchers that - like air-miles in the frequent flyer programs - can be spent as currency within Reykjavik metropolitan area. By rewarding best proposals in a P2P environment, users will be enabled to collectively share their trust with other users in a way that structurally *increase political reputation, while simultaneously decreasing the risk of managing credit* in the political system (that is, bad proposals are not rewarded).

As in D-CENT one speaks of citizen loyalty to commons-enhancing values, rather than costumer loyalty for profit making - initially - a major player to accept *social-krónas* earned though political engagement for the betterment of Reykjavik's *social good* would be the City Council by offering the infrastructure - an escrow account - that would provide access to / accept payment for goods and services: 1) use of public facilities/utilities; 2) use/provision of local transports, health services, etc; or still 3) the access to Reykjavik cultural institutions (museums, entertainment, events, etc.). In brief, this is one of the most advanced experiments in concretely rewarding citizen engagement as a service to the community with the possibility to enjoy, in return, services that better their lives. In effect, the city will be technically paying a small fee to pro-active citizens for making a good idea work for the city.

The following blueprint is adapted from Lietaer and Kennedy (2012).

## The Freecoin Toolchain for Your Priorities: Description of System

**Region served:** Reykjavik Metropolitan Area

**Name of currency / Standard of Value: '**Social Kronas' (SKR) redeemable at 10: 1 ratio with Icelandic Kronas (ISK), i.e. 10 SCR = 1 ISK

**Management:** Betri Reykjavik / Citizen Foundation / City Hall

**Cost recovery:** annual levy Betri Reykjavik / Citizen Foundation / City Hall

**Main purpose:** transforming political reputation into currency. It would be the first time where reward for bettering the social good can be spent for real value within a decentralized and transparent payment system.

**Benefits:** link desirable political participation to life models that enhance human engagement for the development of the common good. Within the context of participatory budgeting, pilot members engage in proposing initiatives for the betterment of the common and social good of

Reykjavik and surrounding areas. Their very ideas can better their community and environment while also rewarding directly those that proposed the best ideas. This would make Rekyavik a city with increased level of political participation, improving the relationship and trust between citizens and elected representatives, thus increasing democracy.

**Participants:** Your Priorities members (12k individuals) within the pilot to be extended to the whole citizenry of Iceland.

**Core mechanisms:** Social Proof-of-work as Proof-of-Political-Participation for the social good connected to a 'Pot of Money'/Escrow Account. The pro-active and crowd-sourced decision-making process for the betterment of the social good that happens on Your Priorities can be linked to a special fund (or 'pot of money') provided by the City Hall (alongside the resources allocated for the participatory budgeting yearly rounds). The pot of money will be an escrow account that would clear social credits into Icelandic kronas to be spent within the circuit, for example to access the city transportation network, pools, cultural life, social services and the like. As for redeeming tokens, the Social Kronas escrow account would release value expressed in Icelandic kronas to the individuals that meet the conditions of the social proof of work for the Icelandic Digital Social Currency Pilot: the proof-of-political-participation. In practice, a user contributing with a highly rated proposal on the YP platform by other users, would have the possibility to redeem this reputation rates (social kronas) in exchange of a specific range of goods and services, those related to the set included into the circuit.

**Governance:** Betri Reykjavik / Your Priorities / Citizen Foundation / Town Hall: participatory governance and policymaking.

### Freecoin Toolchain Features for Icelandic Digital Social Currency

**Feature #1: transforming reputation for the betterment of the common good into money:** Social credits will be coins in users wallets.

**Feature #2: blockchain based complementary currency:** ubiquitous wallets for a custom currency system based on Social POW

**Feature #3: convertibility into ISK through City Hall Escrow Account**


**Figure 7: Icelandic pilot overview**

# Pilot 2 (Spain) Eurocat – a Micro-Endorsement System for the regional currency of Catalunya

The second application of the Digital Social Currency pilots is the Eurocat, a regional complementary currency for Catalunya. The Micro-Endorsement and Mutual Credit System proposed by Eurocat "is both a method of allocating credit and a method of guaranteeing against credit default" within the members of the regional currency system for Catalunya (Spain). Among the various experiences about Spanish communities examined in D-CENT D3.4, Eurocat emerged as an existing system for control of credit within a specific community, part of the CES network (Community Exchange System) and running on a centralized CMS application based on Drupal.

As a result of our research, we concluded that Eurocat does not need a decentralized, blockchain based currency system for its design of endorsements and mutual credit circuit. The Eurocat trust model requires the possibility for a central authority to withdraw tokens (endorsements) from participants: deploying a cryptographic blockchain technology to implement it would be averse to this requirement. But we still believe Eurocat needs to decentralize its architecture incrementally in order to avoid single point of trust and failure and will be working to envision and facilitate the evolution of its technical infrastructure towards more resilient approaches that can be undertaken by the Small and Medium Enterprises sector in Catalunya, which is the primary audience for Eurocat.
The Freecoin Toolchain for Eurocat: Description of System

The following systematization blueprint is adapted from Lietaer and Kennedy (2012):

Region served

Catalunya (Spain), several hundred of thousands SMEs and individuals.

Name of currency / Standard of Value

An eurocat (EUC) relates to a correspondent pair of endorsements (END). One END is one Unit of Trust (UT) given and received), i.e. one company can access EUC to the extent to which that company has been endorsed by - and is endorsing - other companies. UT (Unit of trust) is a unit of account that signal the potential to create a means of exchange denominated in EUC. When a company gives UT to another company, it is providing endorsement to that company.. In turn, EUC is a complementary currency, i.e. a means of payment for measuring mutual credit between members and the standard of value.

Below, convertibility and 'functions of money' aspects of the Eurocat system:

To endorse is to give UT; to be endorsed is to receive 1 UT.
For each UT given and received=1 pair of endorsements (END)

Micro-endorsement System: END : EUC = 1 : 1
(END: Unit of Account; EUC: Standard of Value)

Mutual Credit System: EUC : EUR = 1 : 1
(EUC: Unit of Account/Means of Payment; EUR: Standard of Value/Store of Value)

Micro-endorsement and Mutual credit tiers together form the Eurocat complementary currency system.

Management: Eurocat Management Committee

Cost recovery: Eurocat membership/annual-fee/levy with a leading principle to operate, ie. on an "at-cost" basis (Bogle, 2009). As a result, Eurocat Management Committee will essentially earn a net income of zero. In practice, Euro donations. Local currency fee = 1% of total turnover.

Main purpose

Support the regional economy of Catalunya via social control of credit: Eurocat micro-endorsement and mutual credit system can be seen as a credit risk social-management system, i.e. Social Currency (END) in the form of reputation gained and assigned by members. To denote an endorsement in this context, it may be useful to borrow from transaction cost economics, the notion of 'relation-specific investments' (Noteboom 2013). If one player does not abide to the very commitment she puts in the system, then she may be banned, i.e. micro-endorsements can be withdrawn as it happens on online forums either by peers or moderators/sysadmins.

**Benefits**

Mobilise spare business capacity; makes money go further. Desirable counter-cyclical effect on regional economy by increasing the Local Multiplier Effect while ring-fencing euros inside Catalunya as a geographical and economic region. Essentially Eurocat's proposal is to engage in decentralized trust management (END) for the social control of credit (EUC). This possibility is a way to overcome the structural deficiency of the conventional money system that is currently incapable to exercise its very basic role of intermediary for credit access and circulation in the regional economy. As noticed in D3.4, in Catalunya, the absence of a steady recovery is being experienced as an impossibility to access liquidity, hence ushering in a sharp contraction of total SMEs sector turnover in the region.

**Core mechanisms: social proof-of-work as Proof Of Business**

Everyone gets the same amount in the Eurocat Payment system (EUC) as it has in Trust Capital (END): you have 25k in Trust Capital (ENDs), you get 25k EUC in your Eurocat account in the payment system.

The social proof-of-work within the Eurocat system, i.e. the parameter that benchmarks whether a company is either functional or dysfunctional for the system is called 'Proof Of Business' (Business POW): the proof that a company is respecting its Minimum Activity.

'Minimum activity is a systemic rule that refers to the number of exchange cycles that each member completes in one financial year. The Minimum activity is the minimum annual spending and minimum sales a company has to undertake in one year, and it will be a function of the Trust Capital and the Velocity expected for the type of credit the company has. For instance, for M1 accounts' Velocity expected is 2, so the minimum activity for the company will be 2xTC. i.e. a company with a trust capital of 50.000 EUC should sell and purchase for a minimum value of 100.000 EUC per year. non-functional members are the ones below 2TC purchases or sales (whichever is lesser).

A decentralized list should detail the company name, balance and the date of the oldest transaction, and if they are in the grace period (see credit conditionality). Members whose Minimum activity is not achieved are potential problems. They either have EUC they don't spend, or have debt and don't redeem it, or have not made any transaction yet. They have to be reviewed and it is necessary to find out why they have such a low activity. If the low activity of a company is caused by a lack of engagement in the Eurocat system, there is the need of a feature that allows for withdrawal of the UT, i.e., endorsement (END) would be undone, i.e. Eurocats (EUC) would be withdrawn. This collides with the architectural features of the blockchain, thus the practical advantage to switch to more traditional and centralized clients like CES/Drupal. Within D-CENT, further engagement with Eurocat will be about testing useful features of the Freecoin Toolchain.

**Governance** Social Control of Credit for Distributed Monetary Policymaking: the community decides the level and the ways to spread risk - in view of securing a common interest, maintaining the social good, i.e. the integrity and reliability / resilience of the currency system itself: money as a commons. For instance, users can collectively set the agenda about the UPPER LIMIT / highest risk of the Minimum Activity parameter (or velocity target for each credit line) benchmarking the micro-endorsement system. By deliberating on the risk of allocation of credit within the rules of endorsement and the Proof-of-Business, collectively, member companies have credit risk self-management capabilities through an in-direct, measurable, transparent and concrete collective policymaking process. In fact, by fixing the level of trust in real time and in a transparent architecture, it is potentially more probable to supply the optimal quantity of currency at each point in the time series of the business cycle.

**Freecoin Toolchain Features for Eurocat**

**Feature # 1:** to facilitate the decision-making process (integration with e-democracy module)

**Feature #2: decentralized storage:** the database of the system is stored in a resilient fashion and can be recovered from the personal computer of custodian participants: stewardship of data commons.

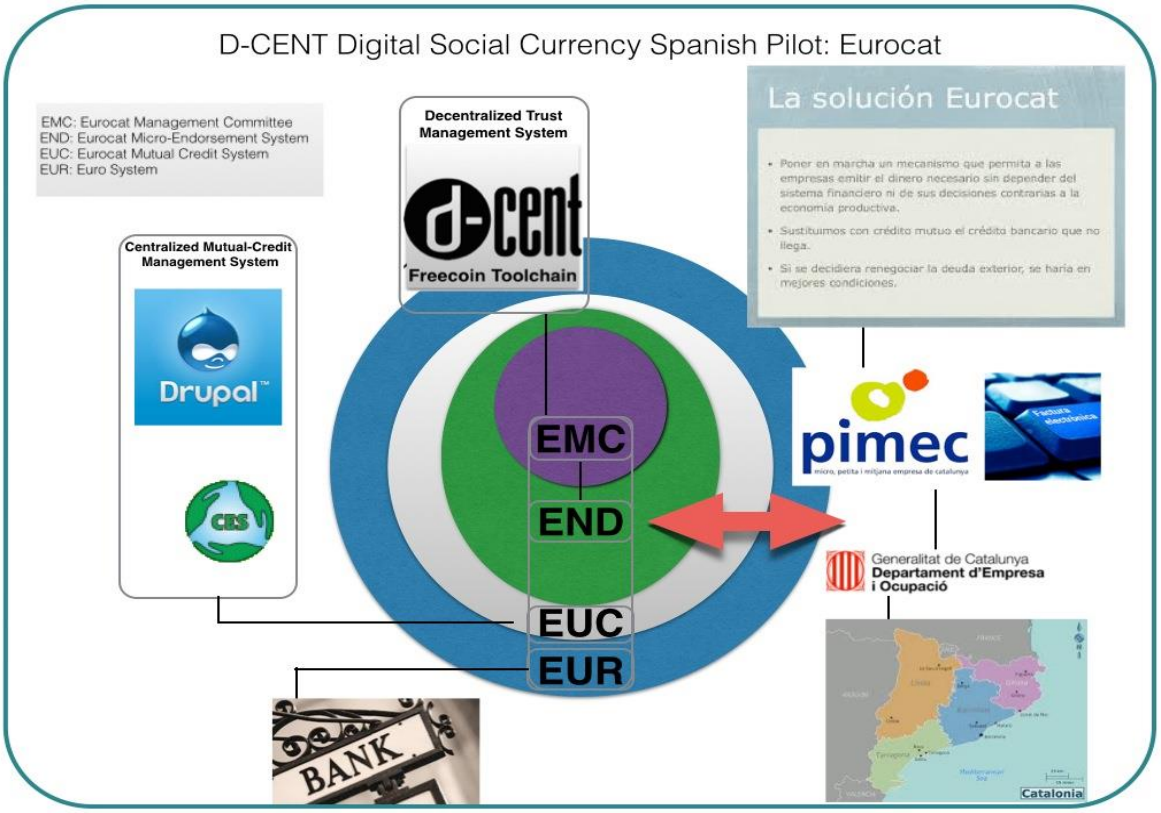



Figure 8: Eurocat pilot overview

# Pilot 3 (Finland) Multapaakku – a Decentralised Currency for Community-Supported Agriculture

Community-supported agriculture (CSA; sometimes known as community-shared agriculture) is an alternative, locally based economic model of agriculture and food distribution. A CSA also refers to a particular network or association of individuals who have pledged to support one or more local farms, with growers and consumers sharing the risks and benefits of food production. CSA members or subscribers pay at the onset of the growing season for a share of the anticipated harvest; once harvesting begins, they periodically receive shares of produce. In addition to produce, some CSA services may include additional farm products like honey, eggs, dairy, and meat. Some CSAs provide for contributions of labor in lieu of a portion of subscription costs. (DeMuth, 1993).

Helsinki Urban Co-operative Farm is an ongoing Community-supported agriculture experience started in 2011. As every CSA, it is a cooperative run by its own members, who decided to initiate the project in order to satisfy common need: uncomfortable within the constraints and absence of transparency of big agribusiness, the community wanted to be sure that one eat vegetables whose origin and growth process had to be clear and under the control of seedlings

to the end user. The Urban Co-operative Farm concept originated with the idea that participants each get an area of a farm the size of a normal allotment, with a professional grower (whom we call a Personal Farmer) looking after it. The Personal Farmer cultivates your piece of the farm and keeps you up to date with what is being done there.

Nobody can afford to hire a grower on their own, but in the Urban Co-operative Farm concept about people hiring one collectively which makes it possible. The grower doesn't cultivate one are, but a hectare. Participants can volunteer to work in the field anytime they wish, albeit there is the agreement on 10 hours of work per year to be delivered by each member of the cooperative. Overall, 200 households invest an annual 450 Euros fee in advance and the harvest from the field is distributed amongst participants weekly during the harvest season in 4 points of sale scattered around the city, one of which is the Helsinki Public Library.

After five years of growing food and increasing the number of participants taking part in Helsinki Urban Co-operative Farm, also complexity and transaction types and numbers are beginning to become an issue to address. On the one hand, some members do not deliver the basic quota of 10 hours of work per year. On the other, there are members who put way more than 10 hours per year into the betterment of the cooperative. Some work extensively in the fields, others execute administrative and management paperwork and even more dedicate time serving the community during distribution days while advertising upcoming events organized by Helsinki Urban Co-operative Farm.

All these contributions are accounted for as volunteering work, which members began to have rewarded in the local time-bank currency unit, the Tovi by Helsinki Timebank discussed in D3.4. In brief, Helsinki Urban Co-operative Farm board has been experiencing an increase in volume of contributions that members supply to the maintenance and/or betterment of the common good, the cooperative itself. More than monetize volunteer work, the aim for a Digital Social Currency for Helsinki Urban Co-operative Farm is to find a decentralized way to track contributions and reward them in a self-governance setting for the sake of fairness toward those who dedicate themselves to the betterment of the common good of the community. In a nutshell, the social remuneration service is conceived as a meritocratic trust management system for rewarding contributions to Helsinki Urban Co-operative Farm and, by extension, to other Finnish CSA initiatives and around Europe.

The experimentation in this pilot will be on a social remuneration scheme that will process contributions to the cooperative in real time by the very members of Helsinki Urban Co-operative Farm, who perform them. By having a public ledger for the registration of hours of contributions in the various areas of occupation (almost 20 streams) that volunteers can choose what to be busy in and by storing a backup copy of Helsinki Urban Co-operative Farm Escrow Wallet on each device connected to the network, cooperative members will self-record and self-remunerate their contributions. In the Finnish pilot, each member will have stored on her device a copy of the total amount of currency of the network, and every time she will self-remunerate herself, she - and all members - will see an adjustment on the Escrow

Wallet containing the tokens. In this case, governance is spread to every participant and risk is the highest as anybody can compromise the system, thus damaging all the others.

## The Freecoin Toolchain for Helsinki Urban Co-operative Farm: Description of System

**Region served:** Helsinki Area 500 people, viz. 200 households (200 members). Each household has a share in the cooperative and there is a scheme for food delivery once a week in one of the 4 spots in the city that give the products during winter. Each of the 200 members does at least 10 hour of work per year of work for the cooperative.

**Name of currency / Standard of Value:**

10 Multapakku = 1 working hour = ~10 Euros

**Management:** Helsinki Urban Co-operative Farm.

**Cost recovery:** 450 Euros for both join and harvest fees.

**Main purpose:**
To ignite a fair and meritocratic process of economic growth of Helsinki Urban Co-operative Farm. The idea is to compensate more efficiently people's work by choosing the kind of activity one wants to join and be active into one of the 20 working groups in which the cooperative is framed around: fieldwork, events grouse, finance management, membership registry management, fundraising division Need to track who works for what and compensate thus a meritocratic and self-managed system (Social POW). The need is to be able to reward who is executing a task for the cooperative and remunerate them by tracking their contributions. Already using CES from Helsinki Timebanking used for paying those that work for weeding the fields. Difficulties and cost of running the marketplace itself.

**Benefits:** better management of the cooperative, solid business model that can both increase membership in Helsinki Urban Co-operative Farm and, if the test will be successful, it could be adopted in other similar contexts. In particular, the Social POW here is an experiment around a community that can monitor in real time both collective trust as contributions to the cooperative and individual trust as honesty in that everybody will have an eye on the movements of the main Helsinki Urban Co-operative Farm Escrow Wallet.

**Participants: Urban Co-operative Farm members.** 200 households / 500 individuals. Another stakeholder would be Helsinki Public Library, which interested in urban agriculture and is also one of the pickup points of harvest produce coming from Helsinki **Urban Co-**

**operative Farm.** Also house-sharing and collective purchase rings may be involved in the piloting of the codebase.

**Core mechanisms:** Social POW as Proof-of-Contribution: If a member abides to the cooperative subscription rules by performing 10 hours/year of cooperative work (on filed, administrative, commercial, etc.) and wants to contribute more to the social sustainability of Helsinki Urban Co-operative Farm, she can apply to have a Urban Co-operative Farm member wallet. In order to explore decentralized tracking processes of trust management dynamics within a community, contribution will be rewarded by members themselves: each time a member execute one or more hours of work, she will simply pay her wallet from the Helsinki Urban Co-operative Farm Escrow Wallet, a common wallet where all digital tokens are parked. In particular, inside each new individual wallet, each member will find a credit of 450 tokens equivalent to 45 hours that can be exchanged also with Helsinki Timebank users and the instructions for measuring contributions to the cooperative and pay one own's wallet. To add a further level of security, it is possible to conceive human involvement by granting signing rights to the manager of the membership address book or executive board members.

**Governance:** Urban Co-operative Farm board in general and especially the person in charge of membership address book to monitor the blockchain.

**The Freecoin Toolchain for Helsinki Urban Co-operative Farm: Features**

**Feature #1: P2P trust management.** Meritocratic system for rewarding contributions to the common good of Helsinki Urban Co-operative Farm.

**Feature #2: 'Common Account' decentralized storage.** Every member will have access to the common wallet containing the money supply for the self-reward of contributions by members themselves. This features will test the levels of trust and distrust among members of a currency system. If the system will not be abused unsustainably, then this pilot will have demonstrated that self-reward is an option to further explore in the study of economic relations.

**Feature #3: blockchain based complementary currency:** the coins and wallets are based on a customized blockchain system based on Social POW and ubiquitous wallet technology.


**Figure 9: Finnish pilot overview**

# Pilot 4 (Italy): Commoncoin – a Decentralised Currency for the cultural sector

Similarly to the Finnish and Icelandic pilots, also in the case of Macao we face the need to find mechanism to self-reward contributions in a decentralized and transparent way. By overlapping with the social Proof-of-Contribution in cooperative work (Finland), in the Italian use-case will relate to a similar framework but applied in a different social context. In Milan, contributions relate to the work performed in the cultural industry within already existing webs of trust that cannot scale up due to the lack of a means of exchange that can facilitate the mobilization of all the possibilities for reciprocity in the city. The bottom up engagement practice of social remuneration as a reward for the Proof-of-Contribution give enormous power on users, since they can take advantage of the possibility to control the whole common good at will. As the problem is not so much the one about tracking contribution, but that of decentralizing the process itself, a way to test the tools of the Freecoin Toolchain is to endow the users with

both the power to transparently track their contribution and self-reward themselves while looking at the effect of free-riding in real time on the balance of the 'common account', the Escrow Wallet that contains the pre-mined tokens, the common money supply.

## Macao A-Platform

The history of Macao has been documented in D3.4. Nowadays (Q2 2015), Macao is about to launch A-Platform in June 2015. A-Platforms is a network of production centres conceived for pooling spaces and equipment for artistic production within the city of Milan: "A-Platform is When you start to design in a flat style, it can be hard to stop — harder than you think! That is exactly what happened to us when we designed the icons for Smallicons. It turned into a big project, which we hope will help designers and other professionals whose work is based on graphics one way or another." In order to maximize members participation, organizers of A-Platform are willing to prototype the Freecoin Toolchain as an internal scheme that tracks the contributions of A-Platform members and allows them to self-remunerate themselves while both offering and searching for in the art industry in Milan.

## Commoncoin

Commoncoin is the concept of a currency that would measure engagement and that will shape reputation within the cultural industry network pilot in Milan. It is thought of as a new complementary currency that transforms trust into a circulating medium of exchange as for the social remuneration procedure sketched out in the Finnish pilot. Organizers at Macao conceive Commoncoin as an internal currency for financing cooperative production, anti-accumulation and anti-speculative uses, developed with a media and digital technology, but politically controlled by the communities that use it. Indeed, as it will be the prototyping in Finland, also in this case members of A-Platform will carry with themselves a backup copy of the total amount of tokens that will be pre-mined for A-Platform. Thus, although in a different context than urban agriculture, also in this use-case on the cultural industry of a city like Milan members' trust and distrust relations to the common good will be tested, as everybody will be allowed to steal all the funds and transfer them to his or her personal wallet from the Commoncoin Escrow Wallet.

Therefore, trust management will be a central element of study also for the Italian use case at Macao and Milan at large.

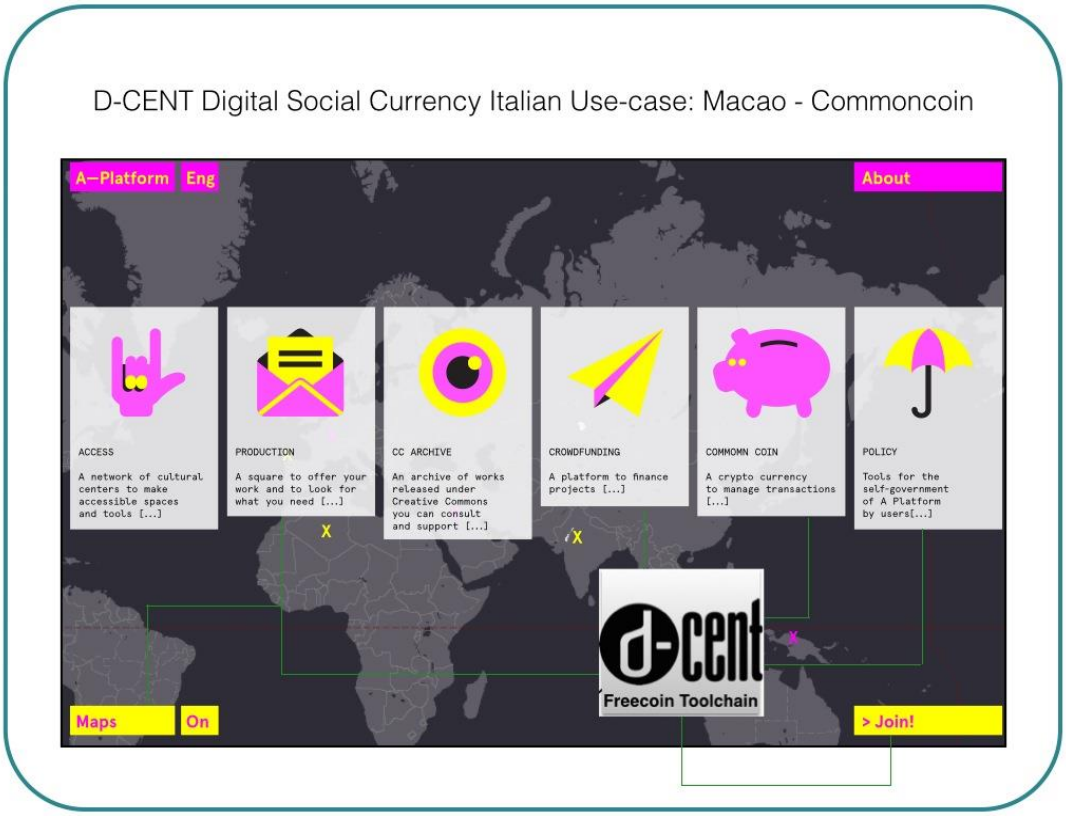



**Figure 10: Macao pilot overview**

# References

Anderson, S. et al. (2005) Web Services Trust Language (WS-Trust) available at http://specs.xmlsoap.org/ws/2005/02/trust/WS-Trust.pdf]

Antonouplulos, Andreas, *Mastering Bitcoin,* O'Reilly, 2014.

Arnsperger, Christian, *Critical Political Economy - Complexity, rationality, and the logic of post- orthodox pluralism*, New York: Routledge. 2008.

Back, Adam at alia, 'Enabling Bitcoin Innovatiions with Pegged Sidechains', Blockstream, 2014.

Berger, P.L. and T. Luckmann, The Social Construction of Reality: A Treatise in the Sociology of Knowledge, London: Allen Lane. 1967.

Bogle, J.C., Enough. *True Measures of Money, Business, and Life*, John Wiley & Sons. 2009.
.
Cuzzort, R.P. and E.W. king, (eds) *Twentieth Century Social Thought*, Chicago: Holt, Reinhart and Winston, 1989.

Dasgupta, Partha, "Trust as a Commodity." In *Trust: Making and Breaking Cooperative Relations*, edited by Diego Gambetta, 49-76. New York: Basil Blackwell, 1988.

DeMuth, Suzanne (September 1993). "Defining Community Supported Agriculture". United States Department of Agriculture.

Durbin, M., *All about High Frequency Trading*, McGraw Hill, 2010.

European Central Bank, 'Virtual Currency Schemes', report, October, 2012 ISBN 978-92-899-0862-7 (online)

Hurley, R., X. Gong and A. Waqar,"Understanding the loss of trust in large banks", *International Journal of Bank Marketing*, Vol. 32 Iss 5 pp. 348 - 366 (2014) Permanent link to this document: http://dx.doi.org/10.1108/IJBM-01-2014-0003

Illiceto, Michele, *La persona: dalla relazione alla responsabilità. Lineamenti di ontologia relazionale*, (approx. translation: The person: from relation to responsibility. Elements of relational ontology) prefazione di Attilio Danese, Città Aperta, Troina (EN) 2008.

Ingham, G. (1996) "Money is a Social Relation," Review of Social Economy, 54(4): 243-. 75

Ingham, G. (2013). "Revisiting the Credit Theory of Money and Trust," in J. Pixley (ed) (2013). New Perspectives on Emotions in Finance, London: Routledge, 121-139.

Kennedy, Margrit, Bernard Lietaer, John Rogers, *People's Money - the Promise of Regional Currencies*, Triarchy Press. 2012.

Kroeger, F., 'How Trust is Intitutionalized? Understanding collective and long-term trust orientations', in Bachmann, R. and Zaheer, A. (Eds), *Advances in Trust Research*, Edward Elgar, Chichester, pp. 261-284. 2013

Kroeger, F., 'Trsting organizations: the institutionalization of trust in interoganizational relationships', *Organization*, 19(6), 743-63. 2012.

Lietaer, Bernard, *The Future of Money*, London-NY: Randomhouse. 2001.

Lietaer, Bernard, Christian Arnspenger, Sally Groener and Stefan Brunnhuber, *Money and Sustainability - the missing link*, Triarchy Press, 2012.

Lietaer, Bernard, Robert E. Ulanowicz, Sally J.Goerner and Nadia Mclaren. "Is Our Monetary Structure a Systemic Cause for Financial Instability? Evidence and Remedies from Nature", in *Journal of Future Studies*, Special Issue on the Financial Crisis (April 2010).

Nakamoto, S. (2008) "Bitcoin: A Peer-to-Peer Electronic Cash System".

Noteboom, B., 'Trust and Innovation', in in Bachmann, R. and Zaheer, A. (Eds), *Advances in Trust Research*, Edward Elgar, Chichester, pp. 106 - 121. 2013.

Ostrom, Elinor (1990). *Governing the commons: the evolution of institutions for collective action*. Cambridge New York: Cambridge University Press.

Ostrom, Elinor; Walker, James; Gardner, Roy (1994). *Rules, games, and common-pool resources*. Ann Arbor: University of Michigan Press.

Ostrom, Elinor; Walker, James (2003). *Trust and reciprocity: interdisciplinary lessons from experimental research*. New York: Russell Sage Foundation.

Roio, Denis, 'Bitcoin: the End of the Taboo on Money', Planetary Collegium, April 2013.

Schumacher, E. F., *Small Is Beautiful: Economics as if People Mattered*, Harper Perennial, 1989.

Schoorman, F.D, R.C. Mayer and J.H. Davis, 'An integrative model of organizational trust :past, present and future, Academy of Management Review, 32 (2), 344-54. (2007).

Stodder, James "Complementary Credit Networks and Macroeconomic Stability: Switzerland's Wirtschaftring", *Journal of Economic Behavior and Organization*, vol. 72 (2009), pp. 79-95.

Stodder, James "Reciprocal Exchange Networks: Implications for Macroeconomic Stability", paper presented at the International Electronic and Electrical Engineering (IEEE), and the Engineering Management Society (EMS), Albuquerque, New Mexico, August 2000.

Varoufakis, Y., 'The Future of Finance', speech delivered in Seattle in the context of the CFA Institute's Annual Conference, 5th May 2014 (http://yanisvaroufakis.eu/2014/05/08/digital-economies-markets-money-and-democratic-politics-revisited/).

Wierzbicki, Adam, *Trust and Fairness in Open, Distributed Systems,* Springer Science and Business Media, 2010.

Winslett, M. 'An Introduction to Trust Negotiations.' In: P. Nixon and S. Terzis (eds.): *Trust Management* 2003, LNCS 2692, pp. 275-283. (2003)