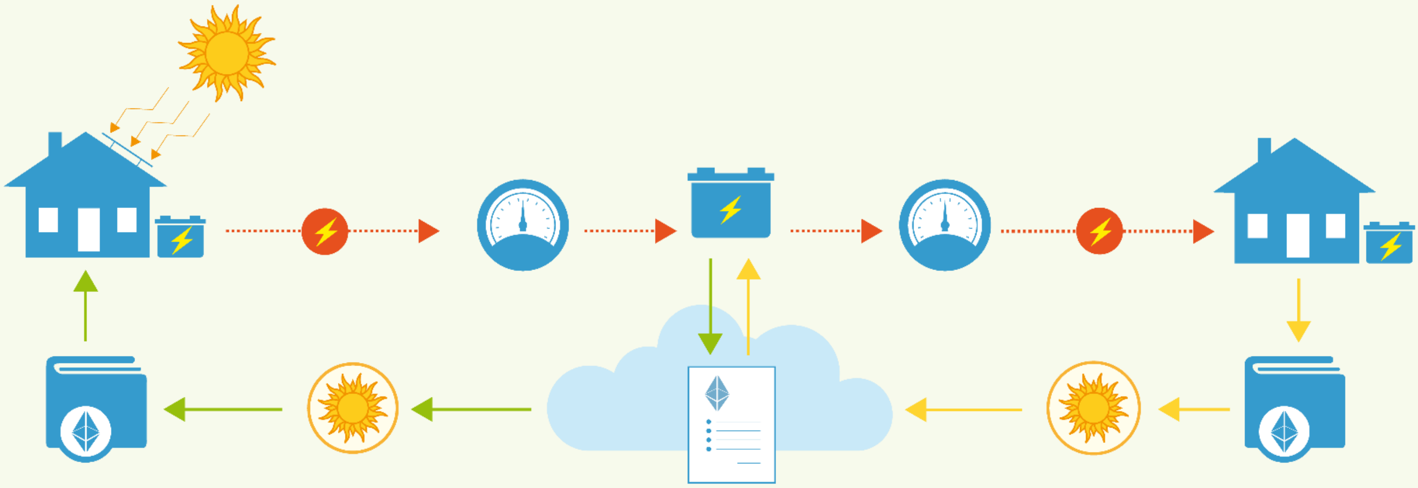
JRC TECHNICAL REPORTS

Blockchain in Energy Communities

A proof of concept

Kounelis Ioannis, Giuliani Raimondo, Geneiatakis Dimitrios, Di Gioia Rosanna, Karopoulos Georgios, Steri Gary, Neisse Ricardo, Nai-Fovino Igor

2017



Joint Research Centre

EUR 29074 EN

This publication is a Technical report by the Joint Research Centre (JRC), the European Commission's science and knowledge service. It aims to provide evidence-based scientific support to the European policymaking process. The scientific output expressed does not imply a policy position of the European Commission. Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use that might be made of this publication.

Contact information
Name: Ioannis Kounelis
Address: JRC, TP 361, Via E. Fermi 2749, 21027 Ispra (VA), Italy
Email: ioannis.kounelis@ec.europa.eu

JRC Science Hub
https://ec.europa.eu/jrc

JRC110298

EUR 29074 EN

PDF ISBN 978-92-79-77773-8 ISSN 1831-9424 doi:10.2760/121912

Ispra: European Commission, 2017

How to cite this report: Author(s), *Title*, EUR, Publisher, Publisher City, Year of Publication, ISBN, doi, PUBSY No.

All images © European Union 2017, except:
Page 10, Roger E. M., Figure 3, Innovation Adoption Lifecycle by Roger E.M
Page 12, Council of Europe, Figure 4, Council of Europe's competences for Democratic Culture (CDC) "butterfly"
Page 13, Walker and Devine-Wright, Figure 5, Understanding of community renewable energy in relation to project process and outcome dimensions
Page 14, F. Geels and J. J. Deuten, Figure 6, Phases in the development of shared technological knowledge

Contents

Abstract

This report aims at exploring the use of the distributed ledger paradigm to incentive the participation of the citizen to a truly free, open and interoperable energy market, producing a feasibility study and a first demo testbed, taking also into consideration privacy, cybersecurity and big-data issues of the smart-home in the Energy market context.

This study is intended to support point 4.1, 4.2 and 4.3 of the DSM (COM(2015)192) and point 2.2 of the Energy Union package (COM(2015)80.

1 Introduction

Micro-generation is the capacity for consumers to produce electrical energy in-house or in a local community. The concept of "market" indicates the possibility of trading the electricity that has been micro-generated among producers and consumers, where a user acting both as a producer and consumer is called a "prosumer". Traditionally, this market has been served by pre-defined bilateral agreements between prosumers and retail energy suppliers. This means that until now, electricity-generating prosumers have not had real access to the energy market, which remains a privileged playing field for the institutionalised energy suppliers. This fact has, so far, heavily impacted on the real diffusion at large scale of micro-generation due to the limited economic advantages this energy generation approach would bring to the prosumers.

Indeed, the main options considered so far by the technical literature, were completely centralised and their viability (under a prosumer perspective) was in general challenged as they introduce additional management fees and costs and assume the intervention of a trusted third party reducing once again the potential gains of end-users. New approaches should be developed enabling end-users to have free access to the energy market. In this context the advent of distributed ledgers, i.e., blockchains, can be considered beneficial.

In particular, the use of a blockchain for energy representation and exchange provides several advantages. First of all, it gives the possibility to have a trusted and decentralised direct exchange between two parties. No intermediaries or third parties are needed in order to fulfil transactions. The data on the blockchain are public, easily verifiable by interested parties, consistent, and always available. Even if the data are available, the users remain pseudonymous, as for the transactions blockchain addresses and not personal data are used. Moreover, due to their decentralised nature and therefore lack of a central point of failure, blockchains are very resistant to denial of service attacks. Finally, data on the blockchain are immutable, meaning that once inserted in the blockchain it cannot be altered, providing therefore a reliable point of reference. By having these features, blockchain provides a trusted technology that can be used as an Information and Communication Technology (ICT) backbone for an open energy market.

According to our approach, self-generated electricity could normally be either consumed within the house, accumulated in batteries for later use, or simply given back to the grid, where, thanks to the distributed and pervasive nature of the blockchain, the produced energy could be redeemed elsewhere. For example, when charging an electric vehicle abroad, or sold through the blockchain to the best buyer, according to a mechanism similar to that of a stock-exchange market.

Exploiting the potentialities of blockchains and distributed ledgers, in this report we propose a solar energy production and distribution architecture that uses smart contracts to support automatic and distributed energy exchange, thus allowing the development of an energy micro-generation market more open and fruitful, from an end-user perspective. More in detail we introduce a platform named Helios that facilitates microgenerators to exchange energy freely in a limited geographical area. In this setup a custom made Internet of Things (IoT) smart meter is used to account and register the micro-generated energy in the blockchain, while the smart contract supports the monitoring and accounting of energy exchange in terms of a financial transaction. The model has been implemented and validated through an in-house developed test-bed composed by a real physical energy infrastructure and the related control and ICT layers. To the best of our knowledge, Helios is among the first solutions built on off the shelf devices and open source technologies, enabling prosumers to access the energy market.

The rest of the report is organised as follows: in chapter 2 we introduce to the reader the concept of the blockchain technology by briefly describing how it works and what advantages it has. In chapter 3 we discuss the people's perception of an energy community. We first explain what a community is and then go deeper in the notion of virtual communities and what the motivations for joining a community are. In this section we also analyse how people perceive the use of blockchains as a means of payment and as a technology in general. In chapter 4 we describe our prosumer energy model and the different ways energy exchange can be achieved. In chapter 5 we explain how the hardware infrastructure can be built by describing our own implementation on top of which we have based our energy model. In chapter 6 we describe in detail our own proposal of the Helios Coin. We explain all the components that are necessary for it to properly function, including the application logic. In chapter 7 we discuss the privacy and security issues that a smart home may encounter. To do so we list all the possible threats and attacks that could be performed in such a system. In chapter 8 we list the related work. Finally, in chapter 9 we conclude our report and discuss possible topics for future work.

2 Overview of Blockchains

In this section we briefly describe the main characteristics of blockchains and smart contracts technologies our proposed solution relies on. Blockchains are the backbones of cryptocurrencies, such as Bitcoin [1]. They are the technology on which cryptocurrencies are built on, and on which transactions can succeed without the need of having a trusted third party. In particular, a blockchain is a tamper-proof and shared data structure composed of a list of blocks of transactions. The blocks are distributed to all nodes of the network and contain all the transactions that took place from the creation of the cryptocurrency. New transactions are inserted in the end of the chain and are linked to the previous block of transactions, as each block references the previous block's hash.

The intrinsic nature of blockchains presents some interesting advantages:

- Disintermediation and trustless model: exchanges (or transactions) do not require intermediaries or trusted third parties; moreover, the parties have full guarantee that the transactions will be executed as expected
- User empowerment: transactions and data are in control by the users' community
- Resilience: due to their decentralised nature, blockchains do not have a central point of failure
- Transparency and immutability: every modification in public blockchains is visible to everybody, moreover, the transactions stored in a blockchain cannot be altered or deleted as it is not computational feasible to do so
- Low transaction costs: being completely unsupervised, the intermediaries' costs are eliminated

For these reasons, blockchain can be used to implement other decentralized services apart from currency transactions in which trust is built-in based on blockchain intrinsic properties. Furthermore, blockchain is supported with additional functions to enhance trust. One of the most promising is smart contracts.

A smart contract is a computer program that is capable of executing or enforcing a predefined agreement using a blockchain, when and if specific conditions are met. Its main goal is to enable two or more parties to perform a trusted transaction without having the need of intermediaries. Moreover, smart contracts inherit the characteristics of blockchains and thus have no downtime, censorship or third party interference.

In the model presented in this report we build up on the open-source Ethereum Virtual Machine (EVM)[1] blockchain-based distributed computing platform. The main goal of the EVM is to keep a distributed record of transactions performed using the Ethereum digital currency, Ether (ETH). A blockchain-based platform such as the EVM can be seen as a distributed database that can be accessed/managed by many people that do not necessarily trust each other and do not share a common trusted 3rd party. In contrast to other blockchain-based platforms that target mainly mining of the digital currency and transaction management, Ethereum also provides smart contracts as a core functionality. In Ethereum, an obligatory payment fee, named gas, is required in order to finalise the transactions.

The functionalities that the Ethereum smart contracts provide along with its wide and well documented use make it ideal for the development of our prototype. Moreover, it provides a user friendly JavaScript Application Programming Interface (API) for accessing the smart contract's functionalities from a third application. We have used this feature for developing our middleware controller, as described in Section 6.

[1] https://www.ethereum.org/

3 Social, psychological and cultural aspects of an energy community

With micro-generation, we refer to the small-scale generation of electric power by energy communities composed by citizens, small businesses and public administration to meet their own needs, as alternatives or supplements to traditional centralized grid-connected power.

The concept of energy community is indeed a key point in the design of the future European energy infrastructure and it implies the strict collaboration of market players (utilities), "energy designers" policy makers and citizens all aiming together to develop "intelligent" (smart) energy delivery, fostering the use of renewable sources and technology innovation in distributed generation. This to gain benefits on economy, sustainability and energy security.

The success of the energy community paradigm relies on several factors such as renewable sources and generation system availability, innovative technological solutions, normative regulation, political, psycho-social and cultural dimensions. Those conditions need to be sustainable for all community members.

In this section we will treat those elements with a focus on community aspects, digital competences, energy citizenship, attitudes and motivations as they are key factors for the success of every technological paradigm (see Figure 1).

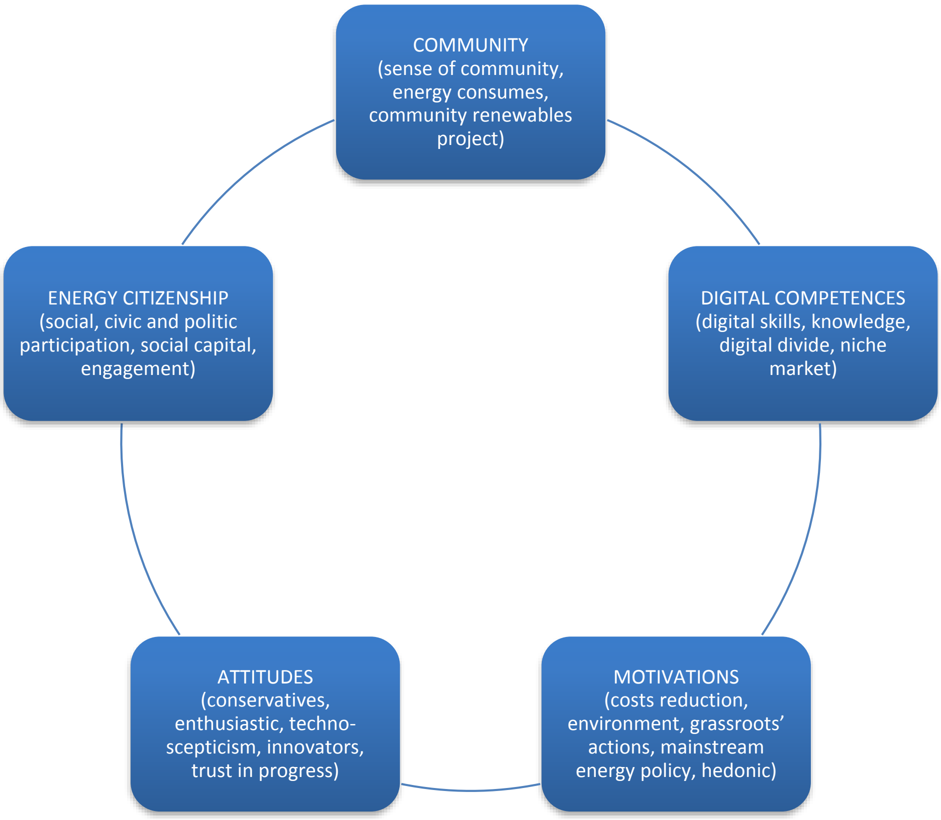

COMMUNITY (sense of community, energy consumes, community renewables project)
DIGITAL COMPETENCES (digital skills, knowledge, digital divide, niche market)
MOTIVATIONS (costs reduction, environment, grassroots' actions, mainstream energy policy, hedonic)
ATTITUDES (conservatives, enthusiastic, techno-scepticism, innovators, trust in progress)
ENERGY CITIZENSHIP (social, civic and politic participation, social capital, engagement)

Figure 1. Energy community – Social, psychological and cultural aspects

What is a community?

Community is a common and widespread word in several areas of interest with different facets and interpretations. We assume that it is worth to define the concept of community and then make a focus on the specific energy community.

Communities building, participation and the role of culture have been mainstream subjects of study and research in social and community psychology. These themes can be traced into the thinking of psychologist Kurt Lewin, who, through his field theory of group dynamics, claimed that groups are more than the sum of their parts. This premise is explained by the principle of interactionism, which assumes that the behaviour of people in groups is determined by the interaction of the person and the environment. This means that when a group comes into existence, it becomes a unified system with properties that should be analysed and understood following a holistic approach rather than by piecemeal examination of each member. In this sense, Lewin applied the Gestalt dictum the whole is greater than the sum of the parts [2].

Revisiting the concept of sense of community

In this view point, we consider a second concept. The sense of community, that has been studied in the social sciences domain, as well as many contexts as urban, rural, tribal, workplaces, schools, universities, recreational clubs and internet communities.

The sense of community concept was originally proposed by Sarason [3, p. 157], who defined it as:

"[…] the perception of similarity to others, an acknowledged interdependence with others, a willingness to maintain this interdependence by giving to or doing for others what one expects from them, and feeling that one is part of a larger dependable and stable structure".

According to Moreland and Levine [4]. The sense of community is:

"The perception that each member is part of a same unit. The definition of a horizontal structure where individual commitments and roles are identified".

Other primary theoretical foundation of *psychological sense of community* can be found in McMillan and Chavis's [5] theory. The authors defined sense of community as:

"A feeling that members have of belonging, a feeling that members matter to one another and to the group, and a shared faith that members' needs will be met through their to be together."

Moreover, Chavis, Hogge, McMillan, and Wandersman proposed a framework and developed the Sense of Community Questionnaire and Index (SCI) based on the perception of four elements and their interrelated dynamics:

1. Membership;
2. Influence;
3. Integration and meeting needs;
4. A shared emotional connection.

A second index (SCI2), which is based on the offline equivalent sense of community, has been recently developed by Chavis et al. with the aim of understanding the dynamics of virtual communities [6].

Box 1. Summary of Mc Millan Theory

<u>Four elements of sense of community</u>

There are four elements of "sense of community" according to the McMillan & Chavis theory:

Membership includes five attributes:

1. boundaries
2. emotional safety
3. a sense of belonging and identification
4. personal investment
5. a common symbol system

Influence

Influence works both ways: members need to feel that they have some influence in the group, and some influence by the group on its members is needed for group cohesion. Current researches [7] on rural and urban communities have found that sense of community is a major factor in

Integration and fulfilment of needs

Members feel rewarded in some way for their participation in the community.

Shared emotional connection

The "definitive element for true community" it includes shared history and shared participation (or at least identification with the history).

Dynamics within and between the elements

The reason to report such theories and assumptions is that, even thought, at a first glance, those statements can be seen as old-fashioned, we believe that they are still very present in the distributed ledger paradigm. Moreover, community building, as incentive to citizen participation in the micro-generation market, can be enumerated among the intrinsic nature of blockchain schema among with disintermediation and trustless model, user empowerment, resilience, transparency and immutability.

What about virtual communities?

Membership, identity, emotional connection, sense of belonging and the existence of a common objective to be reached through interaction, are also elements of a virtual community?

The term *virtual community* is attributed to the book of the same title written by Howard Rheingold in 1993 [8], where he defined the concept of virtual community as:

"Social aggregation emerging from a network when a certain number of individuals are engaged in a discussion in a long term and with a discrete human feeling realising interpersonal relations in the cyberspace".

This oft-cited definition has been revised by other theorists and Rheingold himself has declared:

"One major difference between what I know now and what I knew when I wrote the first edition of this book is that I've learned that virtual communities won't automatically emerge or grow... simply by adding a forum or chatroom to a web page" [9].

The idea of virtual community illustrated by Rheingold has been criticized as utopian position. The application of social network analysis [10], in this model of virtual community, reveals that steps have been taken in the right direction, but much remains to be done.

In our opinion many other factors need to be considered to better understand how community and virtual community operate. In the following sections we will illustrate some of them.

How do people engage in virtual community?

Do people need to acquire digital competences to be active member of virtual community? Do people need to be computer literates and share social and political vision for computer technology, as well as Internet culture [11]?

Education and user awareness are fundamental dimensions of an effective engagement and participation in virtual communities.

As also set out in the last Joint Communication to the European Parliament and the Council [12] to better place EU to face cybersecurity and privacy threats, EU needs to affirm a resilient and complete strategy to boost citizen's skills in term of technology, awareness and education.

To respond to this need, already in 2013 the Institute of Prospective Technological Studies of the Directorate General JRC, on behalf of DG Education and Culture and after on behalf of DG Employment, has developed and published a detailed Digital Competence framework [13]. This framework, developed with intensive consultation of stakeholders, is tied to needs that every citizen faces while interacting with digital devise and environments and it has become a general reference model for all EU member States for many digital competence initiatives with the aim to create a common language on the development of digital competences. Dedicated frameworks are available for enterprises, teachers [13], consumers [14] and organisations.

The DigComp framework foresees 21 competences (with three proficiency levels), divided in five areas, which can be summarised as below:

1) Information and data literacy
2) Communication and collaboration
3) Digital content creation
4) Safety
5) Problem solving

DigComp is experiencing different phases. Result of phase 1 is an update of the framework, named DigComp 2.0 with a focus on the conceptual reference model, new vocabulary and streamlined descriptors. In comparison with the first version for example, the new focuses on mobile devices, new environments, data literacy, privacy legislation and social inclusion.

Today, a new version is available. The current version is labelled DigComp 2.1 [15] and it focuses on expanding the initial three proficiency levels to a more fine-grained eight level description as well as providing examples of use for these eight levels. Its aim is to support stakeholders with the further implementation of DigComp.

The eight proficiency levels of DigComp 2.1

In our discussion we started from the assumption that citizens aiming at being part of a virtual community, need to acquire digital competences. Among those citizens there will be heterogeneous groups of individuals with foundation, intermediate, advanced and highly-specialised levels digital competences. New version of DigComp framework for citizens present eight proficiency levels that are briefly summarized in Table 1.

Table 1. Citizen's eight proficiency levels

No.	Level	Complexity of tasks	Autonomy	Cognitive domain
1	Foundation	Simple tasks	With guidance	Remembering
2	Foundation	Simple tasks	Autonomy and guidance where needed	Remembering
3	Intermediate	Well-defined and routine tasks, and straightforward problems	On my own	Understanding
4	Intermediate	Tasks, and well-defined and non-routine problems	Independent and according to my needs	Understanding

5	Advanced	Different tasks and problems	Guiding others	Applying
6	Advanced	Most appropriate tasks	Able to adapt to others in a complex context	Evaluating
7	Highly-specialised	Resolve complex problems with limited solutions	Integrate to contribute to the professional practice and to guide others	Creating
8	Highly-specialised	Resolve complex problems with many interacting factors	Propose new ideas and processes to the field	Creating

Should we assume to apply this model to the micro energy community generation, this stratification of competences should be taken into account in the community life-long cycle. Starting with the conception of those tools (hardware, software, user interface, etc.) necessary to initiate the community building, thus to the operative phase including maintenance, updating and problem-solving phases.

Within the community there will probably be:

- a percentage of users with foundation digital competences. They would just need to remember simple tasks that should be guided by a user-friendly interface application. Concepts as block chain, digital ledgers, crypto currencies, smart contracts, etc. do not need to be understood in their functioning yet;
- for intermediate users a level up is desirable as concerns understanding of those tools holding up the common energy micro generation. Autonomy and independent tasks are part of this level;
- advance users might have higher level of understanding and autonomy as well as active role in problem solving and guiding less-experienced users;
- those citizens with highly specialized competences might cover roles necessary to guide others, resolve complex problems and contribute with their professional experience and knowledge. More interesting is the creative nature of their participation in the community as the innovative proposals and solutions.

In this perspective, micro generation through innovative digital paradigms should take into account the stratification of users’ digital competences. This with the aim to open Digital Single Market and Society and enhancing collaborative and participatory practices to different skilled citizens and minimize digital divide. Consequently, we argue that tailor-made micro generation resources addressing the different types of citizen’s skills can be more effective for the support and spread of energy communities.

Which are the motivations beyond community building?

Energy communities can be both grassroots and policies initiatives as part of the politics of modern governance. Nevertheless, motivations are heterogeneous. The firsts invest in clean energy in order to meet consumption needs and produce energy independently. Their motivations lead on different values, such as environment protection, energy saving, supporting the local economy, the value of working for the community and sustainability. Economic reasons are also among the drives of such community choices. Reduction of prices for energy consumes is indeed found as one of the most attractive motivations. Even though, most community members claim that environmental and innovation advantages play an important role, however financial benefits remain important elements in the decision and project development and management.

The literature on individual motivations for investing in renewable energy is diverse. A recent literature review based on the analysis of 18 articles [16] on different types of motivations suggests the following summary:

Table 2. Summary of motivations associated with adopting micro generation

Motivations	
Financial	Save or earn money form lower fuel bills and government incentives Increase the value of my home
Environmental	Help improve the environment
Security of supply	Protect against future higher energy costs Make the household more self-sufficient/less dependent on the utility companies Protect the household against power cuts
Uncertainty and trust	Use an innovative/high-tech system
Impact on residence	Improve the feeling or atmosphere within my home Show my environmental commitment to others

Interesting findings about individual motivations for investing in renewables at community level are suggested by Dóci and Vasileiadou[17] that adopted a socio-psychological approach for studying renewable energy communities. According to this research held in Germany and the Netherlands, results show that, in addition to decreasing of energy costs and addressing climate change, although if less important, *hedonic* motivations are also present. People, being creative, have fun, and integrate in an already existing strong community, where trust is relatively high. This seems to be an important condition for the realization of local energy projects.

These different facets of motivations should be taken into consideration to inform policy debates on how to support such communities. Tailored incentives to different types of motivations can be desirable.

And what about attitudes?

As a general point of view, general attitudes towards innovation can be found at opposite poles. Enthusiasm versus techno scepticism and innovation and trust in progress versus conservative approach (Figure 2).

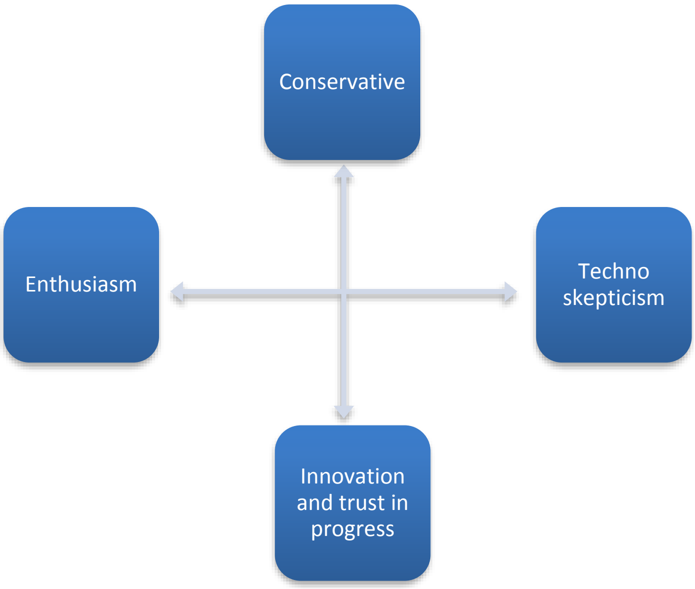


Figure 2. Attitudes towards innovation

According to Rogers [18] and its technology adoption lifecycle sociological model adoption or acceptance of a new product or innovation depends on the demographic and psychological characteristics of defined adopter groups. The process of adoption over time is typically illustrated as a classical normal distribution or *bell curve* (Figure 4). The model indicates different adoption groups that can summarized as follows:

- innovators: more educated, more prosperous and more risk-oriented;
- early adopters: younger, more educated, tended to be community leaders, less prosperous;
- early majority: more conservative but open to new ideas, active in community and influence to neighbours;
- late majority: older, less educated, fairly conservative and less socially active
- laggards: very conservative, oldest and least educated.

The model has subsequently been adapted for many areas of technology adoption in the late 20th century.

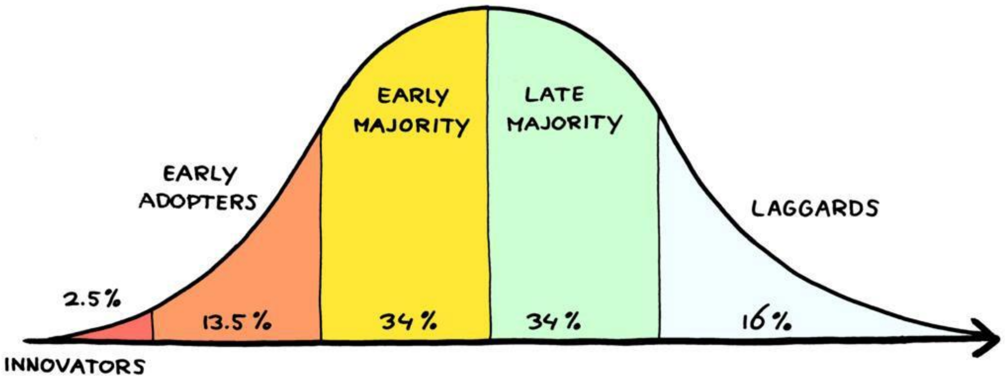


Figure 3. Innovation Adoption Lifecycle by Roger E.M

Taking into consideration the above mentioned model, we consider for blockchain to be in the phase of entering the early majority group. In fact, if we take Bitcoin as representative of blockchain technologies, its massive adoption over the last days probably demonstrates this hypothesis.

Bitcoin's price has doubled from $8000 on 20Nov reaching $16500 on the 7th of Dec[2]. The price rise is caused mainly from the increased interest in purchasing Bitcoins. This trend can be seen from the new wave of registrations on major exchanges. For instance, on Coinbase[3], one of the largest exchanges in the USA, 100,000 new users registered in only one day [19]. The price increase in most of the DLTs is not a recent development. In Table 3 the price change on some of the most commonly used cryptocurrencies can be observed. The original prices are taken from our cryptocurrency report in 2015 [20] .

Table 3. Price comparison of commonly used cryptocurrencies[4]

Name	Price (23/09/2015)	Price (11/12/2017)	Change %
Bitcoin	$230.53	16,640.90	**7219%**
Ripple	$0.01	0.25	**2498%**
Litecoin	$2.87	183.43	**6391%**
Ethereum	$0.89	475.36	**53411%**
BitShares	$0.01	0.17	**1750%**
Dash	$2.43	744.32	**30630%**
BanxShares	$1.75	---	**----**
Peercoin	$0.39	3.45	**885%**
MaidSafeCoin	$0.02	0.48	**2424%**
Nxt	$0.01	0.66	**6623%**
Namecoin	$0.37	2.95	**797%**
Monero	$0.46	262.96	**57165%**
Counterparty	$0.86	23.48	**2730%**
BlackCoin	$0.03	0.32	**1070%**

The increase in most of the currencies is incredibly high. The biggest change can be observed for Ethereum and Monero which have increased more than 50000%. There are cases however that the currency does not exist anymore, such as BanxShares. Nonetheless, it is evident that there is an increased interest not only on the most well-known currency, Bitcoin, but also on the rest.

To what concerns the adoption of Bitcoins and looking back to past money revolution, these thoughts by Andreas Antonopoulos [21], a technologist and well-respected figures in bitcoin can give some hints on how general public perceives crypto currency:

"If you think people find Bitcoin weird, imagine a time when they told them gold is no longer the money, bits of paper are… they were like you gotta be kidding me. So that idea was so radical, it took 400 years before it became broadly deployed in mainstream society."—Andreas Antonopoulos

Energy Citizenship

"Energy citizenship goes beyond the role of the energy consumer. The concept represents political ideals related to democratic participation and empowerment. Energy citizenship is produced through public engagement in policy-making and planning, where the potential for action is framed by notions of equitable rights and responsibilities across society for dealing with the consequences of energy consumption, notably climate change. This includes participation in energy dialogues, which comprise a wide variety of exchanges about energy issues among professional stakeholders in the energy industry, among policymakers, in research as well as among the public" [22].

[2] https://www.coindesk.com/price/

[3] https://www.coinbase.com/

[4] Prices taken from https://coinmarketcap.com/

According to Knut H. Sørensen, Professor of Science and Technology Studies at NTNU (Norwegian University of Science and Technology), *energy citizenship* and energy dialogues are mutually constructed or co-produced with respect to sustainability and citizens' empowerment.

Citizens, in their role of *prosumers* and as member of communities can become a driving force of the low carbon energy transition.

Citizens, rather than being consumers only, have the potential to be energy producers, in particular of renewable energy. Moreover, prosumers can play an active role in the generation of energy, energy storage and management through smart meters, smart contracts and innovative technologies such as blockchain, digital ledgers and crypto currency payment. Citizens and communities need to be provided with the capacity to become knowledgeable participants and to exercise their rights to effectively participate in the political dimension of energy policy.

This concept is perfectly in line with the more general one of Digital Citizenship by the Council of Europe.

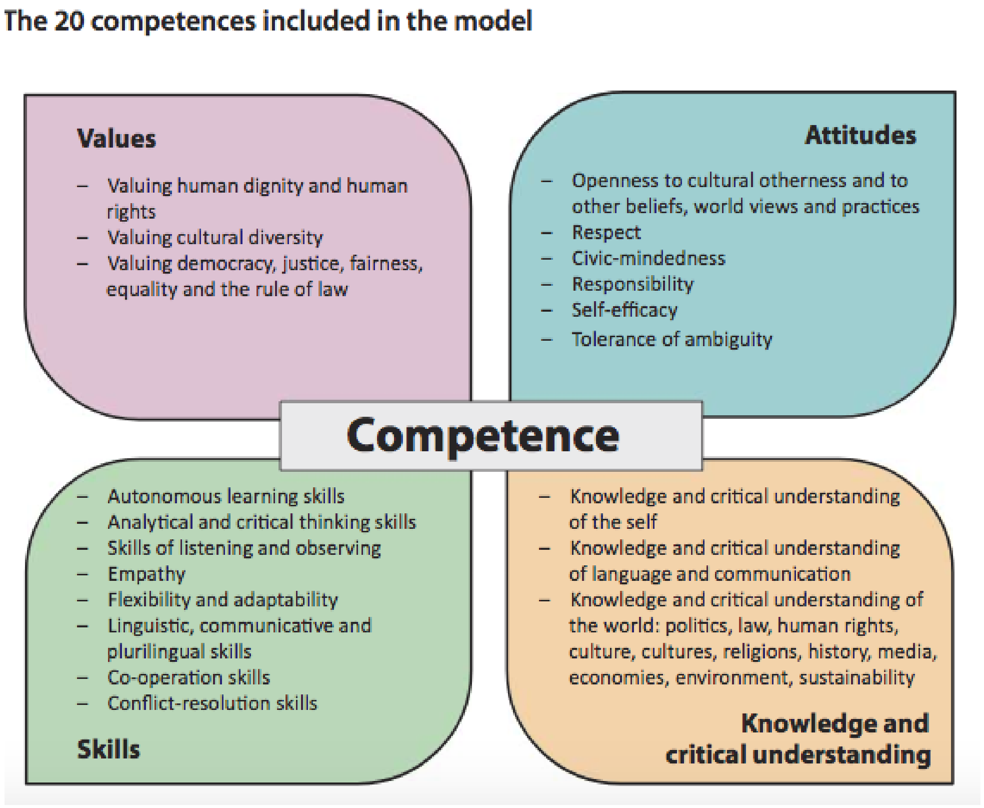

The 20 competences included in the model
Values
– Valuing human dignity and human rights
– Valuing cultural diversity
– Valuing democracy, justice, fairness, equality and the rule of law
Attitudes
– Openness to cultural otherness and to other beliefs, world views and practices
– Respect
– Civic-mindedness
– Responsibility
– Self-efficacy
– Tolerance of ambiguity
Competence
– Autonomous learning skills
– Analytical and critical thinking skills
– Skills of listening and observing
– Empathy
– Flexibility and adaptability
– Linguistic, communicative and plurilingual skills
– Co-operation skills
– Conflict-resolution skills
Skills
– Knowledge and critical understanding of the self
– Knowledge and critical understanding of language and communication
– Knowledge and critical understanding of the world: politics, law, human rights, culture, cultures, religions, history, media, economies, environment, sustainability
Knowledge and critical understanding

Figure 4. Council of Europe's competences for Democratic Culture (CDC) "butterfly"

This model is the result of areas of digital competences most frequently cited by experts and organization in the field, and finally proposed 1o domains within which competences should be examined:

1. Privacy and Security
2. e-presence and Communications
3. Media and Information Literacy
4. Learning and Creativity
5. Access and Inclusion
6. Rights and Responsibilities
7. Health and Well-being
8. Ethics and Empathy
9. Consumer Awareness
10. Active participation

Energy Community

Community energy initiatives are on the rise. In recent mainstream energy policy, the term *community* has been attached to Renewable Energy Community (REC) or Community Renewable Energy (CRE)[23] projects", however some researches have demonstrated that this word is interpreted in quite different ways. Some interpretations were legally driven, as the project had charitable status and no commercial interests. Other had a physical rationale as they involved public buildings used by member of the community. Other stressed the importance of local people being involved in the project.

An interesting scheme is proposed by Walker and Devine-Wright [24] with a *Process and Outcome* model (Figure 5).

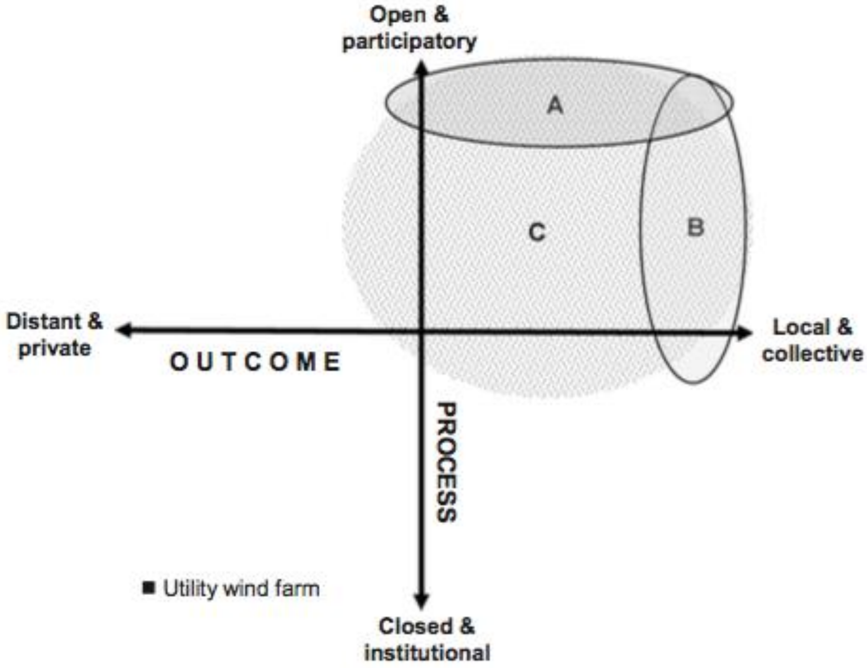


Figure 5. Understanding of community renewable energy in relation to project process and outcome dimensions

First, a *process dimension* concerned with *who* a project is developed and run *by*, *who* is involved and has influence.

Second, an *outcome* dimension concerned with how the *outcomes* of a project are *spatially and socially distributed*. In other words, *who the project is for*, *who* it is that *benefits particularly in economic or social terms.*

Many different possible combinations of process and outcome are deemed acceptable (C) under the community label.

The importance of *process* (A) of project development seems to be an important element for realizing meaningful and substantial local involvement in renewable energy community. Nevertheless, research suggests that, in terms of outcome (B) energy community can become more locally divisive and controversial if benefits are not generally shared among local people.

The European Energy Union Package encourages those enterprises belonging to the Social Economy model including cooperative and group of citizens that can take ownership of energy transition, benefit from new technology and participate actively in the market:

"[…] the set of private, formally-organised enterprises, with autonomy of decision and freedom of membership, created to meet their members' needs through the market by

producing goods and providing services, insurance and finance, where decision-making and any distribution of profits or surpluses among the members are not directly linked to the capital or fees contributed by each member, each of whom has one vote, but take place through democratic and participative decision-making processes. The Social Economy also includes private, formally-organised organisations with autonomy of decision and freedom of membership that produce non-market services for households and whose surpluses, if any, cannot be appropriated by the economic agents that create, control or finance them".

[..] organisations of people who conduct an activity with the main purpose of meeting the needs of people rather than remunerating capitalist investors" [25]*.*

All in all, we can conclude that Community Renewable Energy projects can be considered as socio-technical and economic system for the energy provision. Their development lies down on several reasons such as rising concerns over climate change impacts, environmental sustainability, security of supply and technology innovation. Drivers in this raise can be found on individuals' attitudes and motivations. In addition, research and policy reasons play a determinant role in the community building and management process.

Furthermore, Renewable Energy Communities are often seen as social niches. Niches are complex systems in which both technological and social innovations develop simultaneously and that during a transition entire niches link up with the regime.

Transitions

Can renewable energy communities be drivers of energy transitions?

To what extend renewable energy communities, as social niches, have the potential to scale up and contribute to energy transitions?

What should we do if we want to transform the current centralized and fossil-based energy system to a sustainable one?

Community Renewable Energy projects are often considered as protected, robust and influential *niche* spaces and seedbeds of radical innovation [26].

Recent Strategic Niche Management (SNM) literature makes a distinction between (i) market niches (small market segments), (ii) technological niches (a sort of laboratories for experimenting with new technologies) and (iii) social niches (which refer to specific social groups, such as NGOs, governmental organisations or local communities that develop new methods and solutions for their own social problems [26].

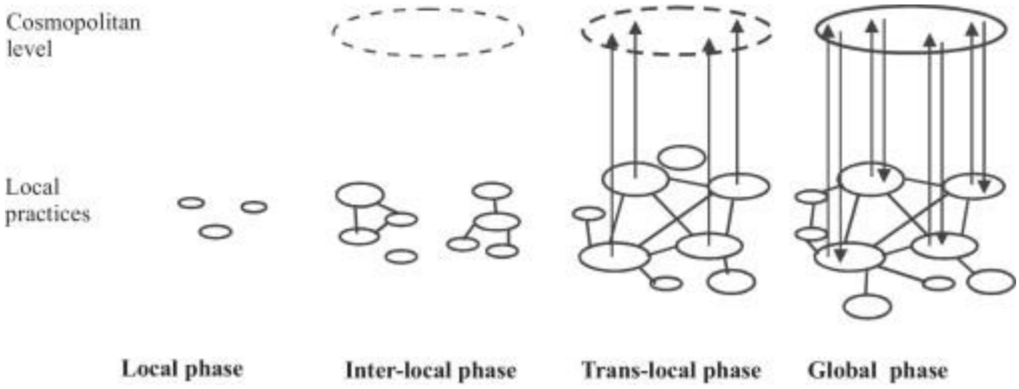


Figure 6. Phases in the development of shared technological knowledge [27]

According to SNM, niche can become influential, with the potential to diffuse their innovations into wider society and have identified three areas:

- expectations: the development of shared expectations and visions is considered a pre-requisite for robust niche development, and the role of local projects in this process is somewhat less immediate than in the previous sections, as this role is normally coordinated by intermediaries.
- social networks: community energy projects engage in networking activities in a variety of ways, with a diverse set of partners, to gain support, information, and share their experiences.
- learning: sharing learning not only as accumulate facts, data and first-order lessons about how to improve the innovation, but also generation of second-order learning about alternative cognitive frames and different ways of valuing and supporting the niche.

Moreover, niches can differ with respect to their actors and their purposes. Niches can be *internally and externally oriented* [28]. On one hand the externally oriented niches are organized around a technological innovation and the other components of the niche are subordinated to it. On the other hand, in the internally oriented niche, the emphasis is not on the technology itself, that it is considered as a tool to reach specific objectives. It comes out that social niches are more internally oriented, whereas market and technological niches are typically externally oriented.

As *niches* develop according to a bottom-up approach and to solve local problem, it is possible that niche members would not break-out their status of small groups and scale up into wider society. This consideration need to be taken into account by policy makers, who should investigate motivations and needs of niche communities.

4. Blockchain Energy Model

As explained in Section 3, blockchain can be understood as an enabler for energy communities. In this section we provide a high level description of a blockchain based energy model we conceived to establish a truly open Energy Community Market.

In our model called Helios, we assume a local grid where energy is produced and consumed in a limited geographical area, such as a local neighbourhood, in order to build an energy community benefit. Energy produced by a prosumer may be saved in the user's local battery for later use or may be immediately injected in the local grid. Recall that a prosumer is an entity that is capable of generating and consuming energy. The main aim of our model is to enable micro-grid prosumers to produce, consume and trade energy without any barrier. Currently such a system is not widely accepted as it requires the "collaboration" of central energy distributors. In our solution, as previously mentioned, we envision the use of a blockchain system with the support of smart contracts in order to provide decentralisation.

Once the energy leaves the producer's house we envisage two possibilities on how it can reach the consumer. The energy can either be saved in a central neighbourhood energy storage or be directly sent to the consumer. Both cases are described in detail in the following sections.

Neighbourhood Central Storage

The first option is to have a central to the neighbourhood energy storage. The energy is sent there from the producer and is stored until a consumer claims it. In this case our proposed model enables the prosumers to:

- Produce energy and store it in an in-house cache battery (for local energy consumption)
- Consume the stored energy
- Release excess energy to the grid and receive virtual coins in return
- Transfer/Exchange the virtual coins
- Redeem the virtual coins in exchange with energy

In order to better explain how this is achieved, it is important to understand the different layers in which the model is divided. As it can be observed by the high-level overview of the Helios model in Figure 7, the energy grid model main components model is divided in three layers:

- the energy grid,
- the middleware controller, and
- the smart contract.

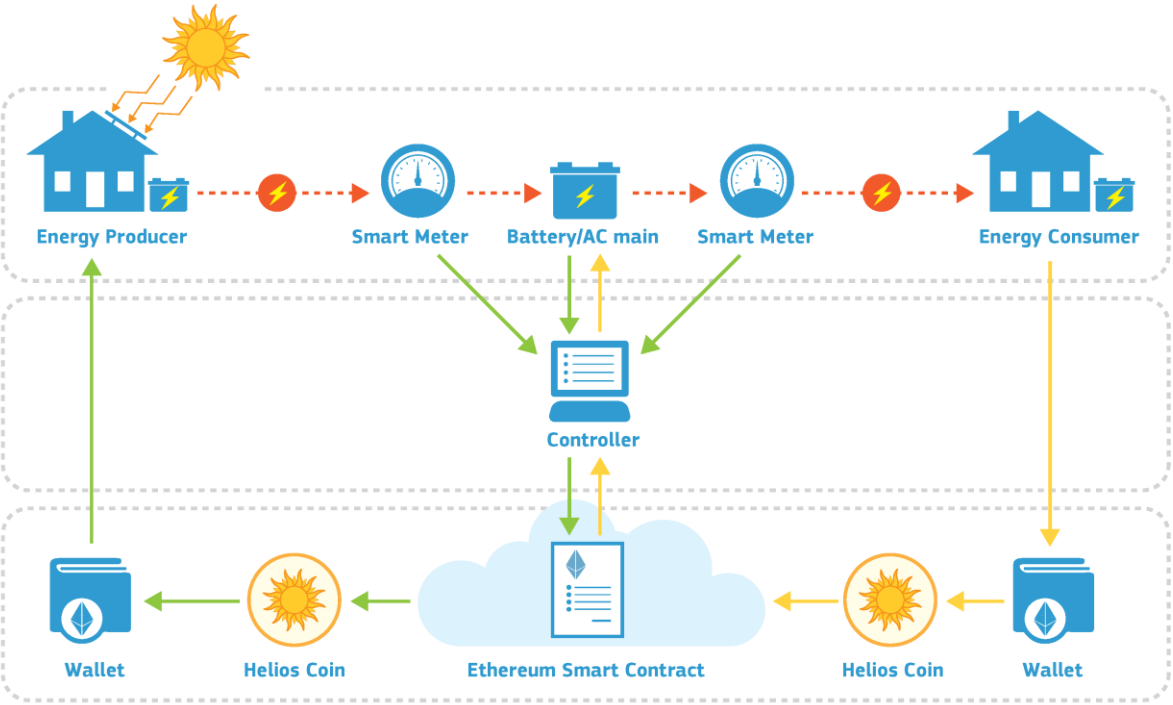


Figure 7. Helios model overview

When energy is sent to the central storage a smart meter linked to each producer continuously measures how much energy has been injected in total. These smart meters, along with the software that handles their output, i.e. a middleware controller, are the input source for our smart contracts. After a predefined amount of energy has been sent to the storage, a Helios Coin (HEC) is awarded to the corresponding prosumer.

The middleware controller interconnects the central storage with the smart contract since these systems cannot communicate directly with each other. As a result, the controller plays the role of invoking the smart contract on one end, and on the other receiving the readings from the grid, thus facilitating communication between the two entities.

The energy grid is handled by its own smart contract. It is aware of the entities connected to it, it can transfer a specified amount of energy to a connected energy consumer, and it is aware of how much energy for consumption is available at any time, i.e. how much energy is stored in the central storage. The grid's smart contract takes as input HECs and then releases the energy that corresponds to the amount of HECs received in the payment by the sender.

The way HECs can be circulated in a market depends on their owners' interests and strategies. The simplest way would be for each owner to have a smart contract in which he sells HECs in exchange for another asset or coin. It should be noted that the smart meters, and the electrical grid in general, is considered a trusted party; meaning that its measurements and operations are considered reliable and are treated as such.

Direct Energy Exchange

In this scenario the consumer receives energy directly from the producer(s) without using a central energy buffer, like the one mentioned in the above described scenario.

The consumer will ask for energy from the smart contract. The smart contract will automatically check if the requested amount of energy is currently available at one or more producers. If this is the case, it will forward to them the consumer's request. At this phase, the automatic price negotiations between the consumer and the producer take place.

The producers can have already defined a fixed price for the energy they sell or they can use a more dynamic approach and set the price per request, adapting it to the current supply and demand. In both cases the contract negotiations can be automated and do not necessarily have to be performed manually by the involved entities.

For example, the consumer may have set a maximum price on which he would be interesting on buying energy and in a similar way the producer may have set a minimum price for selling energy. The negotiations can be then carried out by a smart contract that will seek to find an ideal compromise. The advantage of using smart-contracts here lies on the fact that smart contracts are immutable, and can be seen by everybody. Hence when relying on a smart contract to conduct the negotiation, the parties have the guarantee that it will behave always in a transparent and predictable way.

Once the price has been agreed both parties digitally sign the agreement, always through a smart contract, and the money that will be involved in the transaction is sent to a predefined address that functions as an escrow account.

The final step is to perform the actual energy exchange. As in the first scenario, the middleware controller is the entity that handles the energy exchange. It controls the energy flow from both the producer's and the consumer's smart meter. The overview of the direct energy exchange can be seen in Figure 8.

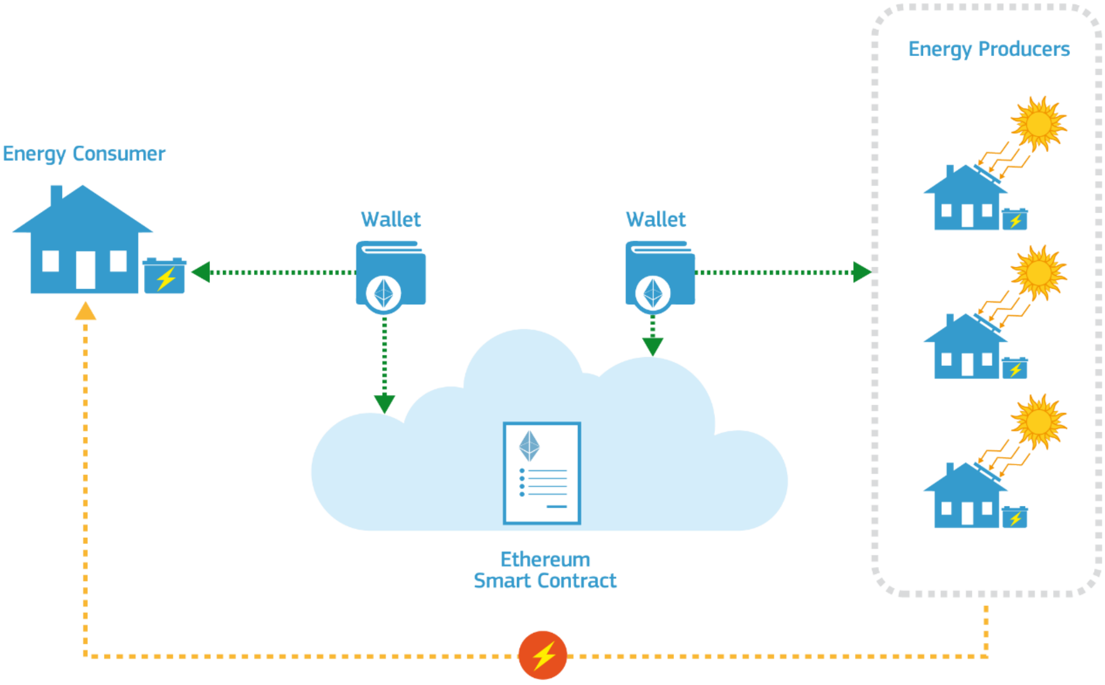


Figure 8. Direct energy exchange with the use of a smart contract

What changes in this scenario is the digital currency associated with the energy exchange. Unlike the Helios coin, where the currency is given to the producer as a reward for every predefined amount of energy stored in the central battery, in this case there is no direct reward from the system. The producer is paid directly by the consumer.

However, the means of payment has not been defined yet. Two possible solutions exist:

i. the entities perform the transaction with a third, independent, means of payment (e.g., Euro, Bitcoin, Ether, etc.)

ii. the system produces on demand energy voucher which are sold a priori to the interested consumers. The consumers can then redeem the vouchers at the producers. In other words, the consumers pay the energy with the vouchers they have already purchased.

Automatic Energy Detection from Neighbour Nodes

In all the scenarios described so far, energy detection is measured directly by a smart meter that is dedicated to each user. The smart meter is the entity that measures all incoming and outgoing energy and on its measurements rely the actions of the middleware controller.

As one can easily imagine this provides a point of trust that has to be accepted by all parties and more importantly cannot be easily verifiable. It is very difficult for a user of the system to know for sure that the smart meters have not been tampered with and their measurements can be considered absolutely trusted and reliable. To enhance users', and systems' trust on smart meter measurements, trusted computing using Trusted Platform Module (TPM), Trusted Execution Environment (TEE), Secure Element (SE) or any similar component can be introduced in smart meters supported by a remote attestation service. This way, both the users and the energy system component can verify the software and/or hardware configuration of a smart meter in order to determine whether it has been tampered or not.

Complementary to trusted computing we introduce automatic energy detection service from neighbour nodes. What this means in practice is that when a node injects energy in the grid its neighbour nodes detect the injected energy and validate it using a consensus-like mechanism in order to accumulate the measurements received for every expected energy transfer. From the voting nodes, only the non-tampered ones are taken into account; if the incoming "votes" verify that the transfer has indeed happened, it is registered in the system.

5. Testbed: Hardware Infrastructure

The model presented in Section 4, has been physically deployed in the JRC labs to study its concrete feasibility.

The hardware infrastructure deployed in the lab as a testbed for the energy generation and exchange across different entities includes all the components involved at each stage, i.e. generation of the electricity, storage, metering, consumption, simulation of an AC (alternating current) mains.

In the setup there are three different entities or nodes able to generate electricity through solar panels, store it in batteries and exchange it through a common electricity bus. An overview of the overall architecture is provided in Figure 9,

Figure 9. Overview of the hardware infrastructure

where the nodes 1, 2 and 3 contain exactly the same components, so that the details are shown only for node 1.

Specifically, it is composed of an AC Mains single phase distribution line using a bus topology. The line provides power exchange among nodes, while power is exchanged using a locally generated frequency at 220 Volt 50 Hz nominal. Within the island there are at least two nodes that are capable of generating, consuming and storing power. The basic rules regulating the nodes are:

- They must conform to the frequency provided by the AC Mains line
- They must comply to a fixed capped maximum power that can be exchanged with the line
- The cap can be different for power injection or withdrawal
- Power and energy metering must be provided by the nodes in the point where it exchanges power with the local grid

Any node complying with the above rules can be added to the network as a producer and/or a consumer. Any node can access the local line provided it respects the above-mentioned rules. This model can represent both the on grid or off grid operation of the network. In the setup there are three nodes able to generate electricity through solar panels, store it in batteries and exchange it through a common electricity bus. The hardware infrastructure deployed in the lab as a testbed for the energy generation and exchange across different entities includes all the components involved at each stage, i.e. generation of the electricity, storage, metering, consumption, simulation of an AC mains.

Each node includes an AC and a DC subsystem. The DC subsystem is made of a 12 V battery (300 AH), a solar panel (130W) and a power controller for charging the battery. Two inverters and an AC to DC battery charger are found in the AC subsystem.

Within the island there is also a special gateway node with the following characteristics:

1. It must provide AC synchronization frequency to the line
2. It must provide energy absorbing capabilities up to the sum of the maximum production rating of all nodes
3. It must provide energy injection capabilities up to the sum of the maximum consumption rating of all nodes
4. Power metering of total incoming and outgoing power must be provided.

Each node includes a photovoltaic panel directly connected to a DC (Direct Current) smart meter ("DC METER" in the figure) that measures the amount of electricity exchanged with the battery. To the same meter, the battery that stores electricity either produced by the panel or coming from the mains and two inverters, an "Off grid inverter" and a "Bidirectional grid tie inverter" are connected.

The first one converts the direct current coming from the panel and/or the battery to alternating current that can be used by internal loads (these loads are meant to be appliances or devices used inside the node, e.g. domestic appliances in a house). Between the off grid inverter and the loads there is an AC smart meter that measures the AC used by the loads and a switch that controls their starting on and off.

The second inverter converts DC from the production to AC that can be injected to a local AC bus and exchanged among the nodes, but also converts AC coming from this bus to DC that can be used to recharge the battery (for the battery to be recharged from AC coming from the local bus, there is also a battery charger that is not shown in the figure). The flow of outgoing or incoming AC is controlled by a switch and measured by the second AC meter. The latter, depicted for all the three nodes, is the interface to the local AC bus to which all the nodes are connected.

Up to the local AC bus, we could consider the exchange system "complete" in a way. However, nodes must be connected to an AC mains (grid power) that provides energy to the nodes in case the solar production or the energy stored in the batteries is not sufficient. This corresponds to the "SIMULATED AC MAINS" shown in red in the figure, which simulates the electric power supply coming from a normal grid. In the lab, this component was simulated using a UPS (Uninterruptible Power Supply) that, in turn, is connected to the real AC power of the building where the architecture has been deployed ("AC POWER" in black in the figure).

Between the simulated mains and the local AC bus that connects the nodes, there is a check point node equipped with an AC meter that controls the overall amount of AC exchanged, in both directions, between the nodes and the simulated mains. This is a double check to verify that, in total, the amount of AC injected or consumed by the nodes really reached or was taken from the common bus. Finally, also in the simulated mains there are some loads, which have the double purpose to simulate external sources of consumption (e.g., street lights, houses not equipped with solar panels, etc.) but also to simulate activities in the grid and to help using the electricity when the batteries are fully charged and there is still production coming from the panels. The details of the hardware components used for our architecture are described in Annex 1.

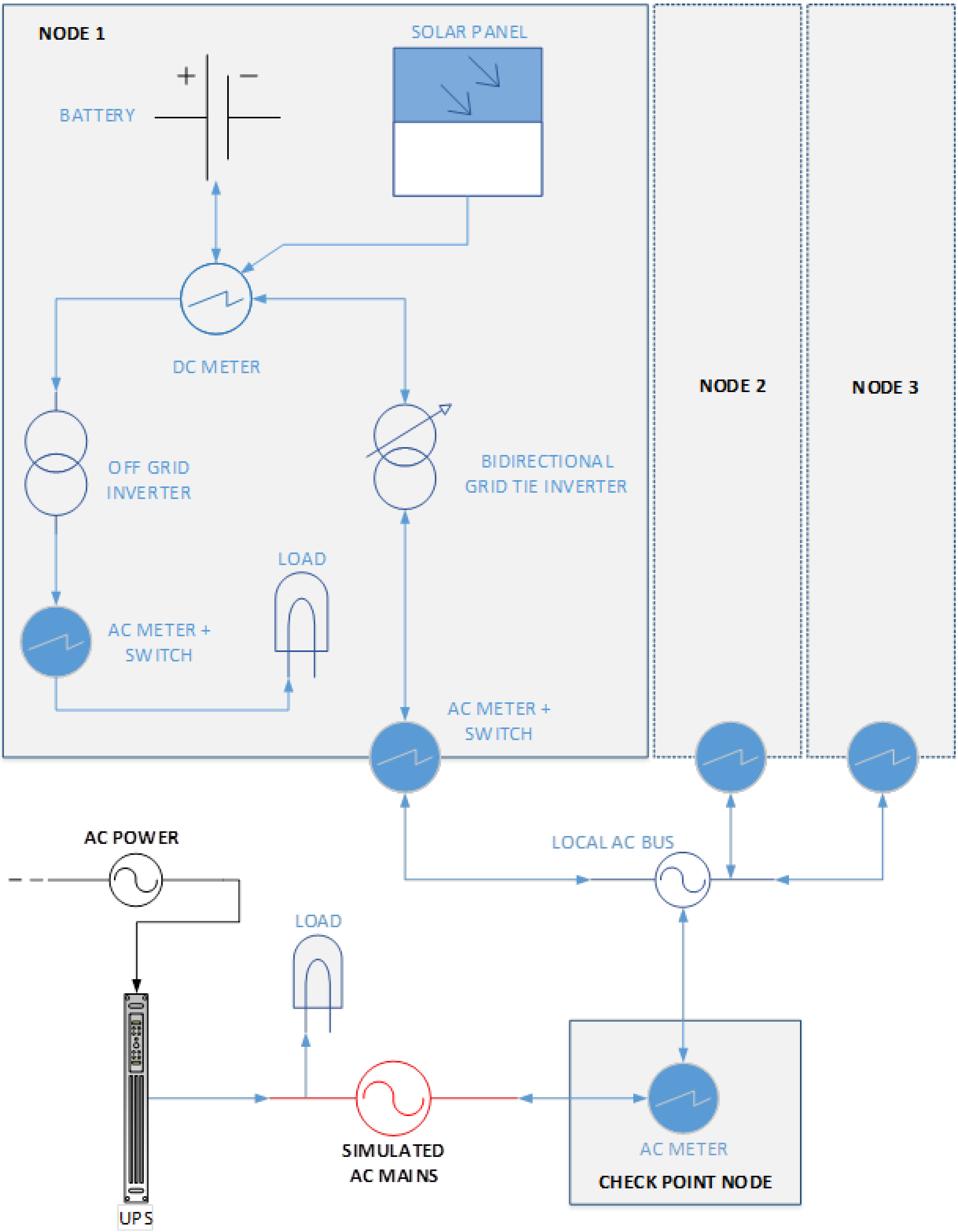


Figure 9. Overview of the hardware infrastructure

6. Testbed: Control Logic (The Helios Coin)

The approach we have followed for our first implementation is similar to the first approach as described in section 4; the energy producers send any energy excess to the grid/energy storage and receive in return energy virtual coins, called Helios Coins – HEC, that can be used in order to get back the same amount of energy from the system. The implementation of the direct energy exchange has been foreseen for future work.

At this point we should mention that a viable solution for enabling prosumers to be active on smart-grid requires, from a data management perspective, a decentralized architecture that provides, among others, **accountability** without the involvement of a central third party entity. Currently, IP infrastructure is not capable of providing such a service, however, blockchain that builds over IP supports accountability for decentralized services.

From our point of view, there are two main approaches that can be followed when it comes to the implementation of a prosumer scenario, always to what concerns the use of blockchain.

The first approach is to use a distributed ledger that natively supports smart contracts, such as Ethereum or Hyperledger. In such case all the logic will be implemented in the smart contract and can be seen in a transparent way by all involved actors. The smart contract will create the Helios coins, will negotiate the price between consumers and producers, will keep the accounting for all the transactions that occurred in the system, and will be the entity that handles the reliable "neighbourhood voting" mechanism.

The alternative approach is to use a blockchain without the support of smart contracts and with the use of other means, e.g. metacoins, provide support for the requested functionalities. For example, when using Bitcoin, HECs could be created with the use of coloured coins as described in Annex 2. What is missing however in this case is the logic that the smart contract implements. This can be replaced by a central application running off the blockchain or by a trusted entity such as the middleware controller.

As in our implementation, we wanted to eliminate any unnecessary trust grounds, we selected the first option. As a result, the system's logic is implemented on a smart contract using the Ethereum platform while the communication between the smart contract and the grid is performed through a middleware controller application.

Middleware Controller

In order for the smart contract to communicate with the grid, to get the measurements of the smart meters and issue commands to release the requested energy towards a client, a middleware application is needed to facilitate the communication between the two parties (as seen in the middle part of Figure 7). This application, is the node controller application. The controller interacts with the physical model with the Arduino Yun board. As a result, the controller has in real time the data transmitted by the smart meter and can immediately issue HECs. The controller is a single application that handles simultaneously all the smart meters of the local grid. It is also the entity that is the owner of our smart contract. On the other end, the controller communicates with the smart contract using the Web3 JavaScript Đapp API[5].

The controller reads from the smart meter every hour. It then calculates the difference with the previous measurement and is thus in position to determine how much energy has been put in the grid from the corresponding user. Once the energy committed to the network has been calculated, new coins will be issued and assigned to the energy creator. The controller will have to call the mint function, i.e. the function that issues new coins, of the smart contract and pass the two necessary parameters: the address of the creator and the value of energy created in Wh (watt-hour). To do this, however, it will first need to unlock the account as for this transaction a fee for the gas consumed[6] has to be paid to the network (in Ether). As the creation of coins assumes a cost for the controller, and thus

[5] https://github.com/ethereum/wiki/wiki/JavaScript-API

[6] "Gas" is the unit used in Ethereum to measure the cost of execution of a smart-contract

for the smart contract owner, the transaction frequency should be well estimated. Even if the cost is small, it is still an extra burden that will in the end affect the energy producer.

As a result, the frequency of the control of the smart meter and thus the coin creation should be set up taking into account the average amount of energy that is produced by the user and his preference on receiving immediately coins for the energy that has been committed into the network. These parameters can be set up during the registration of the user on the grid and then fetched when needed by the controller.

For our demo, we assume this factor not relevant and have it accumulated with the estimated loss of energy during the energy transactions. Moreover, as our scope is to test the proposed solution and monitor its behaviour, we have set the coin generation frequency to a low limit of one Wh. For a market ready application the limit will need to be adapted to higher values, always depending on the solar panels output.

When it comes to releasing energy towards a user, when coins have been returned to the smart contract owner, the controller gets informed by incoming transactions by following the smart contract's event that announces coin transfers on the network. When a new transaction towards the contract owner's address arrives, the controller communicates with the Arduino board and it issues a command to release an amount of energy that corresponds to the coins received towards the sender of the transaction. The coins then remain at the contract owner's address and are considered spent. The controller's functions that create coins and monitor the transfers in the network in order to release energy can be seen in Listing 1.

```
// creation of contract object
var myContract = web3.eth.contract(abiHEC);
var myContractInstance = myContract.at(addressHEC);
var events = myContractInstance.Transfer();
events.watch(function(error, result){
if (!error) {
if(result.args.to == addressOwner){
console.log('Releasing ' + valueTransfer + ' Wh to ' +
fromTransfer);
releaseEnergy(fromTransfer, valueTransfer);} } });
//Coin creation
function createHEC(addressProducer) {
var Wh = smartMeterReader() - lastSmartMeterReading;
//unlocking account
web3.personal.unlockAccount(allAccounts[0], password,
function(error, result){
if(!error){console.log(result);} });
//Mint tokens
myContractInstance.mintToken(addressProducer, Wh, function(
error, result){
if(!error)

console.log(Wh + 'Wh sent to ' + addressProducer); }); } _
```

Listing 1 - Creating and utilizing Helios Coins from the controller

Smart Contract Implementation

The smart contract we have deployed (as seen in the lower part of Figure 7) has the role of the record keeper, with the corresponding reward mechanism. The smart contract is written in Solidity, Ethereum's native programming language, and is deployed on Ethereum, both on Ethereum's official testnet and on our own private network. Every time a user commits energy in the grid, the smart contract will issue coins that correspond to the energy produced and automatically send them to the energy producer.

More specifically, the smart contract has a mint token function that takes as input two parameters: the address of the entity that has produced the coins and an unsigned integer that represents the number of HECs to be issued. What this function does is to issue new coins and assign them directly to the indicated address. The energy producers will need to follow the token in order to detect incoming transactions and thus see their newly created coins. They can easily do so from the graphical interface of the Ethereum wallet; the only parameter needed is the smart contract's address. Once they are in possession of the coins they can circulate them freely according to their desires; they can choose to sell, use or exchange them.

From the smart contract's address, one can verify at any time the balance of any address, view the total supply in coins, view the smart contract's name and symbol, view the smart contract's owner, and follow live the transactions related to the smart contract that occur in the blockchain. The functions of the contract are viewable for everyone, but apart from the transfer function, i.e. the function to transfer coins from one user to another, are only executable by the contract's owner who in this case is the node controller. In order to watch the contract and see its functions, apart from the contract's address the metadata description of its interface is needed. The smart contract's code can be seen in Annex 3.

According to the description done previously, the deployment of the contract has to be done on the controller node, which is commonly used by all the users of the electric system. In this optic, in order to guarantee transparency and the application of the same rules for everyone, we envisage that the deployment of the contract and the management of the controller node is done by a consortium composed of all the neighbours connected to the electric subsystem.

With the deployment of the smart contract we have managed to create a fully working smart grid energy trading system. The system is now able to automatically detect energy inputs and through the controller issue coins with the smart contract. The coins are then circulated as virtual tokens on Ethereum and when they are redeemed they are returned to the controller's address, which on its side communicates with the electric grid in order to release the equivalent to the coins energy. Moreover, the coin transfers and addresses' balance are public and can be monitored by any interested party, as usually expected from a blockchain-based approach.

7. Privacy, cybersecurity and big-data issues of the smart home

The paradigm presented in the previous sections can be understood as the ultimate evolution of the smart-grid, where local prosumers and their devices (the leaves of the grid) actively participate to the energy system, and where a fully distributed digital layer act as the glue keeping the entire system together in an almost self-orchestrated fashion.

Under this perspective, the smart-grid becomes a complex system, built for energy optimization, that interconnects physical elements with cyber-space and enables among others two-way communication both for information and energy exchange. Customers in such an architecture are not only capable of having better info about their energy needs but can also become an active entity in the energy market. The management communication is accomplished mainly using IP networks, thus this interconnection introduces many challenges especially in security and privacy that were not previously faced in the energy grid domain.

In this section, we overview different security issues that can influence the normal function of this "extended smart grid architecture" and possible mitigation schemes based on [29]–[34]. In fact, any security flaw in smart grid is instantly inherited by the prosumer's architecture and vice versa, as the latter relies on different smart grid functions. In the current analysis we discuss the different threats that smart grids should deal with, as its predecessor does not expose any interface to public networks, such as the Internet. To handle these threats, the conventional confidentiality, integrity and availability security services are discussed.

Threats

A local electricity market can bring financial and environmental benefits, while at the same time create opportunities for some entities to misbehave in order to reduce costs or maximize profits. Table 4 lists potential security and privacy threats for the smart grid in general, providing also a brief analysis of their motives.

Table 4. Security and privacy threats to the smart grid

Adversary	Description
Bot-net operators	Attackers infect target systems with malware and take over their control to mount attacks like: DoS, spam, bitcoin mining , information theft etc.
Organized crime	"Traditional" criminal groups (e.g. gambling, drugs, trafficking etc.) taking advantage of the opportunities offered by the Internet. Organized and well-financed
Other criminals	Small not well-organized or financed groups
Hackers	Individuals that attack systems trying to exploit vulnerabilities for their own benefit
Hacktivists	Individuals or groups using computers or computer networks to promote political ends. The results are similar to protest and activism
Insiders	Individuals that are active or ex- employees trying to benefit, disgruntled/angry/dissatisfied employees, careless or poorly trained employees

Nation states espionage	State-run, well-organized and financed. Foreign countries try to gather classified information from countries viewed as hostile
Corporate espionage	Espionage conducted for commercial purposes in order to acquire industrial secrets from competitors
Phishers	Attackers trying to acquire sensitive information such as passwords and credit card numbers by masquerading as a trustworthy entity in an electronic communication
Malware authors	Creators of malicious software which is used to disrupt systems operation, gather sensitive information, or gain access to computer systems
Terrorists/Cyberterrorists	Individuals or groups operating domestically or internationally using violence or the threat of violence to provoke fear
End customers	Energy consumers that try to tamper with smart meters to lower their bills

Security objectives

The addition of two-way communication capabilities to the power delivery infrastructure towards creating a smart grid involves both information technology (IT) and electricity system operations and governance. However, this increased interconnection and integration also introduce cyber-vulnerabilities to the grid. The smart grid will be a potential target for malicious, well-equipped, and well-motivated adversaries, as those presented in Table 4.

Traditional IT security protection measures, like virtual private networks (VPNs), intrusion detection systems (IDSs), public key infrastructure (PKI), anti-virus software, firewalls, etc., cannot be applied to the smart grid as-is due to the inherent differences of the two systems. These differences can be classified as follows:

- **Architecture**. IT networks have flexible and dynamic topology, while central servers require more protection than clients. The smart grid, on the other hand, has a stable topology where distributed devices need to have the same security level as central servers.
- **Technology**. Regular IT networks hosts use many different operating systems and communications are based on IP creating public networks. The smart grid utilizes proprietary operating systems and communication protocols to create private networks.
- **Quality of Service**. Transmission delays, occasional failures and host rebooting are generally tolerated in IT networks. The smart grid, being a critical infrastructure, is very time critical, while rebooting is not acceptable.

In general, the priority of security objectives in IT systems is: Confidentiality, Integrity, Availability, going from higher to lower priority. The aforementioned characteristics of the two infrastructures, led NIST to define these priorities for the smart grid as follows [31]: Availability, Integrity, Confidentiality, going from higher to lower priority. In the following sections we present attacks and mitigation techniques that target each of these objectives.

Attacks and mitigation on availability

This section describes attacks that target the availability of smart grid entities, like smart meters and aggregators. Table 5 provides an overview of such attacks and possible mitigation techniques.

In more detail, these attacks on the device level are:

- **Remote shut down** [35]. According to this attacks, the adversary tries to remotely interrupt the power supply targeting a smart meter. Considering the attack in a large scale, it would be the equivalent of a deliberate blackout. In the traditional power grid this could only happen by attacking generation, transmission and distribution infrastructures, which are, however, well defended.
- **Smart meter tampering**. A straightforward way to attack the availability of power supply to a building is to destroy the smart meter.

An adversary might try to attack the smart grid on the network level:

- **DoS/Jamming/Collision**. A Denial-of-Service (DoS) attack on the network level is targeting towards not allowing a host to communicate with the rest of the network. This can be accomplished with jamming, i.e., by emitting radio signals on the same frequency as the smart meter in order to create packet collisions in the wireless channel.
- **DDoS**. A more sophisticated technique is the Distributed DoS (DDoS), where the attacker uses many (often in the order of thousands) unique IP addresses to flood the victim with useless traffic, so that legitimate traffic cannot be transmitted to or from the attacked node.

When the smart grid is organized in a mesh network then the following attack is also possible:

- **Blackhole attack**. In this attack, the adversary positions himself between a source and a destination node and, instead of relaying packets, it discards them, thus, making communication impossible.

Mitigation techniques that can alleviate these attacks include the following:

- **Authentication**. When two nodes want to communicate they should engage into an authentication procedure where each party attests its authenticity. This procedure assumes that each node has in its possession the appropriate shared keys or pairs of keys.
- **Physical protection**. Smart meters are deployed at consumers' premises. For this reason they should be physically protected in order to prevent unauthorised access to its hardware.
- **Frequency hopping**. A solution against jamming attacks is frequency hopping, where both the transmitter and the receiver change frequency channels in a predetermined way, so that the adversary cannot jam their signals.
- **Authorization**. A complete access control solution should also include an authorization procedure to match authenticated entities with allowed actions. This way, for example, not all smart grid entities would be entitled to function as critical data relays.
- **Reputation systems**. Reputation systems allow entities to rate each other based on their activity in order to build trust through reputation. Their role is to gather a collective opinion in order to build trust between entities of a network or community.

Table 5. Attacks on the availability of the smart grid and mitigations

Attack	**Mitigation**
Device level	
Remote shut down	authentication (secret keys, shared keys, PKI)

Smart meter tampering (destroy)	physical protection
Network level	
DoS/Jamming/Collision	frequency hopping
DDoS	authentication
Mesh network	
Blackhole attack	Authorization/access control, reputation systems

Attacks and mitigation on integrity

This section summarizes attacks and mitigation on the integrity of the smart grid's entities. An overview is presented in Table 6.

On the device level, these attacks include:

- **Smart meter tampering**. This attack refers to the manipulation of energy consumption data so that a consumer can lower his/her energy bill or increase the energy bill of others.
- **Firmware modification**. An attacker can modify the firmware of smart grid devices in order to control their operation.

On the network level, the following attacks can be mounted:

- **Man-in-the-Middle (MitM)**. This is an active attack where the attacker intercepts all messages passing between two communicating parties and injects new ones. The two victims believe they are directly communicating with each other.
- **Replay**. In a replay attack, the adversary repeats a valid data transmission. The re-transmitted data can be either the original data or a modified version.

When the smart grid is organized into a mesh network, the following attacks are possible:

- **Traffic injection**. This attack refers to the process of interfering with an established network connection, by means of constructing packets and injecting them to the network, which appear as if they are part of the normal communication stream.
- **Node impersonation**. In impersonation attack, the adversary is using an identity that was previously stolen by a legitimate node, in order to appear as the latter to the rest of the network.
- **Route injection**. In a route injection attack, the adversary advertises routes between networks that pass from routers that he/she controls in order to either get access to the data exchanged between these networks or disrupt communication.
- **Message modification**. The adversary tries to modify the exchanged messages in order to alter data like energy consumption readings or signalling.

There is also an attack that can be mounted on the application level:

- **SQL injection**. It refers to an attack where an adversary can execute malicious SQL statements against a database server. By mounting this attack, an attacker can bypass authentication and authorization mechanisms and retrieve the contents of an entire database, providing an attacker with unauthorized access to sensitive data including, customer data, personally identifiable information, trade secrets, intellectual property and other sensitive information. SQL injection can also be used to add, modify and delete records in a database, affecting data integrity.

Some of the mitigation techniques presented in the previous section apply also here. In addition, the following mechanisms can be employed:

- **Message authentication**. Message authentication or data origin authentication is a procedure that ensures that a message has not been modified while in transit (data integrity) and that the receiving party can verify the source of the message.
- **Update through authenticated sources**. In order to prevent unauthorised modification of the device's software/firmware, the update procedures must be executed only through authenticated sources.
- **Input validation**. In applications that utilize a database for storing/retrieving data there should be validation of data input in order to avoid attacks based on malformed data (e.g. SQL injection).

Table 6. Attacks on the integrity of the smart grid and mitigation

Attack	Mitigation
Device level	
Smart meter tampering (manipulate sensing data)	message authentication (digital signatures)
Firmware modification	access control, update through authenticated sources
Network level	
Man-in-the-Middle (active)	message authentication
Replay	message authentication
Mesh network	
Traffic injection	message authentication
Node impersonation	authentication
Route injection	message authentication
Message modification	message authentication
Application level	
SQL injections	input validation

Attacks and mitigation on confidentiality

Table 7 presents an overview of attacks that can be mounted against the smart grid, targeting the confidentiality of data. The same table lists appropriate mitigation techniques for each attack.

More specifically, on the device level the following side channel attacks can be observed:

- **Timing analysis**. Here the attacker attempts to compromise a smart grid device by analyzing the time taken to execute cryptographic algorithms. Every logical operation in a computer takes time to execute, and the time can differ based on the input; with precise measurements of the time for each operation, an attacker can work backwards to the input.
- **Power analysis**. In this attack, the adversary studies the power consumption of a cryptographic hardware device (such as a smart card, tamper-resistant trusted computing module, or integrated circuit) that can reside in a smart grid entity. The attack can non-invasively extract cryptographic keys and other secret information from the device.
- **Electromagnetic analysis**. This attack is performed by measuring the electromagnetic radiation emitted from a device and performing signal analysis on it. Different operations emit different amounts of radiation and an electromagnetic trace of encryption may show the exact operations being performed, allowing an attacker to retrieve full or partial cryptographic keys.

On the network level, the following attacks are possible:

- **Wiretapping/eavesdropping**. This attack refers to secretly capturing data packets transmitted between communicating parties without their consent, in order to extract private and potentially useful information. In the smart
- **Traffic analysis**. This is a special case of the aforementioned attack, where the adversary is interested in the metadata of communications (e.g., IP addresses, communication duration, unique sequence number identifying the communication, communication type, start and end time).

Some other attacks that cannot be classified above are the following:

- **Unsafe interaction of meters with home appliances**. In a smart home environment, a smart meter interacts with appliances to calculate their energy consumption and send commands. These communications can leak sensitive information (e.g., consumption readings, personal identifiers) if not properly protected.
- **Phishing**. By mounting this attack, an adversary attempts to obtain sensitive information such as usernames, passwords, and credit card details (and money), by disguising as a trustworthy entity of the smart grid. Typically, email spoofing or instant messaging are used in order to direct users to enter personal information at a fake website.

Mitigation techniques that can be utilized in these cases and have not been referenced above include:

- **Encryption**. This is the process of encoding a message or information in such a way that only authorized parties can access it. As an example, in the smart grid, encryption can be applied to energy consumption data and customer personal information.
- **User training**. End user training can enhance smart grid security, taking into account that the lack of knowledge is the main target of security threats. Users should be able to identify scams and potential targets, as well as be aware of concepts as cybersecurity, privacy and access control.

Table 7. Attacks on the confidentiality of the smart grid and mitigation

Attack	Mitigation
Device level	
Timing analysis	physical protection
Power analysis	physical protection
Electromagnetic analysis	physical protection
Network level	
Wiretapping/eavesdropping/MitM passive (surveillance of customers)	encryption
Traffic analysis	encryption
Other	
Unsafe interaction of meters with home appliances	authorization
Phishing	authentication, user training

At this point it should be noted that besides the above mentioned issues on confidentiality the advent of smart grid has an impact on end-users' privacy albeit the advantages it offers to them. This is because of the large amount of data the smart grid collects (e.g. through end-users' smart meters) in order to provide energy optimization services.

On one side the more granularity on data collection there is the better services can be provided. On the other side, the invasion on end-users' energy data can violate users' privacy. For instance, various research works ([36], [37]) have demonstrated different privacy issues that can influence end-users, such as (a) which device is in use, (b) when user is out of the house, etc.

Though such an issue might not be considered as a significant constraint for the development of the infrastructure, it can still influence the adoption of the service. As a result, we have foreseen for our future activities the identification of optimal parameters that have the minimum impact on users' privacy.

Attacks on other security properties

This section summarises attacks that, while they disrupt the smart grid when successfully mounted, do not directly target availability, integrity or confidentiality. An overview is presented in Table 8; more details on each one of them is given below:

- **Logic bombs**. A logic bomb is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met (e.g.

delete log files when a host is identified as malicious). When the trigger is a certain date and/or time it is called a “time bomb”.

- **Malware: Trojan horses/Viruses/ Worms**. Malicious software (or malware) refers to a variety of forms of software used by adversaries, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, scareware, and other malicious programs. It can take the form of executable code, scripts, active content, and other software that is executed on the victim’s host without his/her consent.

The aforementioned attacks can be alleviated using the following mitigation techniques:

- **Incident recovery strategy**. If nothing else has stopped a logic bomb from intruding to a system (like antivirus and firewalls) then an incident recovery strategy should exist in order to minimize consequences. The recovery strategy is a documented process or set of procedures, which describe the actions to be taken before, during and after a disaster, in order to recover and protect the IT infrastructure in the event of a disaster.
- **Antivirus**. The main purpose of an antivirus software is to prevent, detect and remove malicious software. While originally developed to detect and remove computer viruses, with the proliferation of other kinds of malware, antivirus software started to provide protection from other computer threats.
- **Intrusion detection**. An intrusion detection system (IDS) is a device or software application that monitors a network or systems for malicious activity or policy violations. Any detected activity or violation is typically reported either to an administrator or collected centrally, where input from multiple sources (IDSs) can be combined.

Table 8. Attacks on various security properties of the smart grid and mitigation

Attack	**Mitigation**
Logic bombs	incident recovery strategy
Malware: Trojan horses/Viruses/ Worms	antivirus, intrusion detection

8. Related Work

In this section we describe existing approaches applying digital currencies in the energy area and how they differ from our proposed approach. Bankymoon [38] is a startup in South Africa proposing to use smart meters connected to the blockchain allowing users to load Bitcoins in order to enable the energy flow. In this approach the cryptocurrency is simply used as a prepaid payment option.

Other solutions also using simply cryptocurrencies as a payment option are Solether and BlockCharge. Solether[7] is an open source proposal of an autonomous node for energy management consisting of a solar panel, a battery, and an Intel Edison board that interfaces with the Ethereum blockchain.

The node is associated with an Ethereum address and it is therefore considered an Ethereum entity. Whenever a payment is received the energy flow is enabled through the USB port, which can be used to charge or power a device. The amount of energy flow allowed is automatically accounted according to the amount of the received payment. In the long term the amount of money received in the device account could surpass the cost of the device itself, allowing for the device to actually work as an asset producing money for its owner.

BlockCharge uses the Slock.it technology that proposes a Smart Plug to enable on the go charging of electric cars using a cryptocurrency. Slock.it is a blockchain-based approach to rent or sell anything directly without intermediaries, which in the case of BlockCharge is selling of electrical energy. BlockCharge itself concentrates on the energy market but the Slock.it technology has a broader coverage of smart contracts for any application domain.

More advanced applications of blockchain technology are the SolarCoin[8] and GrünStromJeton[9] reward programs. SolarCoin is a global rewards program for solar electricity generation created in 2014 by a group of volunteers interested in helping the environment. The idea is to award producers of solar energy globally with a digital currency named SolarCoin where 1 coin represents 1 megawatt-hour (MWh) of solar electricity generation. In their technical implementation the SolarCoin infrastructure is described as a lite version of Bitcoin, using scrypt as a proof-of-work algorithm. The source code is open source and available online[10]. Similarly to the SolarCoin program, the Gr¨unStromJeton is a proposal for awarding customers with tokens that serve as an indicator of sustainability of current use and production, as well as to determine their CO2 footprint.

Some startups also propose to use blockchain technology to enable home energy producers and consumers to exchange energy credits in a distributed and dynamic way. A pioneer work on this domain is the TransActive Grid technology, which has been applied in the world's first peer-to-peer blockchain energy solution, employed in the Brooklyn Microgrid[11]. Similarly to our proposal, in the TransActive Grid architecture each house in a neighbourhood acts as an energy producer and consumer. When the house generates energy the smart meter detects energy production/injection and energy tokens are generated to the home owner. The home owner can sell the tokens to neighbours that can then use them. Once used, the tokens are destroyed by the energy consumer's smart meter when it detects the inflow of energy. Consumers can purchase renewable energy credits from 3rd party retailers or buy tokens/credit from their neighbours directly enabling a local microgrid energy market. Whenever a house generates energy, the smart meter detects it and it is usually consumed by the nearest loads.

Another startup example is GridSingularity[12], which targets the energy finance market using a blockchain-based platform. The platform is based on Ethereum and the beta version is currently under development.

All these startups including TransActive Grid and GridSingularity, in contrast to our work, do not provide technical details of their solutions for strategic reasons. For example, there

[7] http://solether.mkvd.net
[8] https://solarcoin.org
[9] https://stromdao.de/gruenstromjetons
[10] https://github.com/onsightit/solarcoin
[11] http://brooklynmicrogrid.com
[12] http://gridsingularity.com

are no details on the smart contract implementation, how the smart contracts interact with the smart meters, what the architecture of the system is, etc.

In the academic literature the concept of energy tokens for trading of energy was discussed in a high-level by Dimitriou & Karame [39], where producers of energy receive tokens directly from the utility provider when energy is injected in the utility grid. In their work also security and privacy issues are highlighted. More recently, Aitzhan & Svetinovic [40] also propose a multi-signature approach to enable security and privacy in a decentralised energy market.

The NRGcoin [41] is currently the only decentralised digital currency proposed in the academic context targeting exchange of energy in smart grids. Together with the NRGcoin currency the authors also propose a novel trading paradigm for buying and selling green energy using a double action process. The main difference with our proposal is that the NRGcoin is a separate coin, built on its own blockchain, while Helios Coin is based on a smart contract. Moreover, there are no technical details on how NRGcoins are created and how the proof of work functions in practice. It seems to be a theoretical proposal, focusing mostly on the NRGcoin trade market.

Close to our approach is the issue of US Renewable Energy Credits (REC) as a cryptocurrency on Ethereum’s blockchain, described in [42]. Here the purpose is to represent the RECs as a new cryptocurrency on Ethereum that can be exchanged or traded. However, also this paper does not provide a description of the physical or software implementation.

9. Conclusions and Future Work

Current technological developments allow prosumers to produce electrical energy in-house or in a local green energy community; however, the energy market is still dominated by big energy players. This means that until now, the majority of prosumers have access to the (energy) market only by using bilateral agreements. This fact has, so far, heavily impacted the real diffusion of micro-generation due to the limited economic advantages the energy generation approach brings to the prosumers.

In this report we presented a prosumers energy model in order to study the feasibility of deploying an in-house micro-generation energy solution enabling the energy exchange at a community level leveraging on the disruptive potentialities of blockchain technologies. The proposed system is based on a solar energy distribution system and is running on a blockchain platform, Ethereum.

The advantages of this approach are manifold:

- It allows to truly engage prosumers in the energy market acting as enabler for the creation of energy communities
- It enhances the transparency and trust of the energy market system
- It guarantees a high level of security, integrity and resilience (thanks to the intrinsic nature of blockchains)
- It guarantees accountability while preserving privacy requirements
- It promises to open-up an entirely new set of business opportunities on top of the concept of energy community

To gather evidences on the viability of the described paradigm, we have developed and tested the whole infrastructure of the system, from the assembly and configuration of all the devices at the physical layer (solar panels, batteries, smart meters, IoT control devices) to the implementation, and deployment of the smart contract based on Ethereum.

The physical part presents a certain degree of flexibility, and it can be configured to work in an autonomous island or connected to a main grid. For what concerns the logic, the one adopted in our approach is the first release of the smart contract.

We already envisage improvements for our energy model and will gradually pursue them in the next phase of the implementation. We plan to study the effectiveness of the system when used in a commercial mode i.e., interconnection with a real market energy platform. The business model of the system must be studied well in order to implement an end product that can be used in a real environment.

Furthermore, we will study other important factors that could have an impact on a prosumer based energy model such as:

(a) Enhancing trust in the system by using TPM enabled smart meters

(b) Increasing systems measurements reliability by introducing a consensus mechanism on top of the proposed architecture

(c) Study in more detail the security and privacy issues presented in this report with focus on the prosumer model

(d) Extend the current implementation of smart contract with more complex functions and allow the use of coins from third parties, automatic control of transaction fees from each owner's account, and a market for exchanging HECs.

(e) Calculate the energy loss during transfer, which should be considered in the implementation of the system logic and transactions.

Overall, considering our initial design the deployment of a prosumer energy model is considered feasible. To facilitate its large scale adoption, on the digital single market, trust and cyber-security in such a critical service should be provided at the highest standard.

References

[1] S. Nakamoto, ‘Bitcoin: A Peer-to-Peer Electronic Cash System’, 2009.

[2] M. H. Kuhn, ‘LEWIN, KURT. Field Theory of Social Science: Selected Theoretical Papers. (Edited by Dorwin Cartwright.) Pp. xx, 346. New York: Harper & Brothers, 1951. $5.00’, *Ann. Am. Acad. Pol. Soc. Sci.*, vol. 276, no. 1, pp. 146–147, Jul. 1951.

[3] S. B. Sarason, *Psychological Sense of Community: Prospects for a Community Psychology*. Place of publication not identified: Proquest/Csa Journal Div, 1974.

[4] J. M. Levine and R. L. Moreland, ‘Progress in Small Group Research’, *Annu. Rev. Psychol.*, vol. 41, no. 1, pp. 585–634, 1990.

[5] M. McMillan, D.W., & Chavis, D.M. D. W., ‘Sense of community: A definition and theory.’, *Am. J. Community Psychol.*, vol. 14, no. 1, pp. 6–23, 1986.

[6] D. M. Chavis, K. S. Lee, and J. D. Acosta, ‘The Sense of Community (SCI) Revised: The Reliability and Validity of the SCI-2’, presented at the 2nd International Community Psychology Conference, Lisboa, Portugal, 2008.

[7] U. E. Chigbu, ‘Rurality as a choice: Towards ruralising rural areas in sub-Saharan African countries’, *Dev. South. Afr.*, vol. 30, no. 6, pp. 812–825, Dec. 2013.

[8] ‘The Virtual Community: Table of Contents’. [Online]. Available: http://www.rheingold.com/vc/book/. [Accessed: 25-Nov-2017].

[9] Rheingold, H., ‘The virtual community: homesteading on the electronic frontier.’, in *The virtual community: homesteading on the electronic frontier.*, vol. Cambridge, Mass., MIT Press., 2000, p. 341.

[10] B. Wellman *et al.*, ‘The Social Affordances of the Internet for Networked Individualism’, *J. Comput.-Mediat. Commun.*, vol. 8, no. 3, Apr. 2003.

[11] M. Castells, *The Internet Galaxy: Reflections on the Internet, Business, and Society*. OUP Oxford, 2002.

[12] Council of the European Union, ‘JOIN (2017) 450 final. Joint Communication to the European Parliament and the Council Resilience, Deterrence and Defence: Building strong cybersecurity for the EU.’, Sep. 2017.

[13] ‘Digital Competence Framework for Educators (DigCompEdu) - EU Science Hub - European Commission’, *EU Science Hub*, 15-Jun-2016. [Online]. Available: https://ec.europa.eu/jrc/en/digcompedu. [Accessed: 25-Nov-2017].

[14] ‘European Framework for Digitally Competent Educational Organisations - EU Science Hub - European Commission’, *EU Science Hub*, 17-Aug-2015. [Online]. Available: https://ec.europa.eu/jrc/en/digcomporg. [Accessed: 25-Nov-2017].

[15] ‘DigComp 2.1: The Digital Competence Framework for Citizens with eight proficiency levels and examples of use - EU Science Hub - European Commission’, *EU Science Hub*, 28-Apr-2017. [Online]. Available: https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/digcomp-21-digital-competence-framework-citizens-eight-proficiency-levels-and-examples-use. [Accessed: 25-Nov-2017].

[16] P. Balcombe, D. Rigby, and A. Azapagic, ‘Motivations and barriers associated with adopting microgeneration energy technologies in the UK’, *Renew. Sustain. Energy Rev.*, vol. 22, no. Supplement C, pp. 655–666, Jun. 2013.

[17] G. Dóci and E. Vasileiadou, ‘“Let׳s do it ourselves” Individual motivations for investing in renewables at community level’, *Renew. Sustain. Energy Rev.*, vol. 49, no. Supplement C, pp. 41–50, Sep. 2015.

[18] E. M. Rogers, *Diffusion of innovations.* New York: Free Press, 2005.

[19] E. Cheng, ‘Bitcoin tops $8,700 to record high as Coinbase adds 100,000 users’, 26-Nov-2017. [Online]. Available: https://www.cnbc.com/2017/11/25/bitcoin-tops-8700-to-record-high-as-coinbase-adds-100000-users.html. [Accessed: 11-Dec-2017].

[20] I. Nai Fovino and G. Steri, ‘Crypto-currencies, Cyber-Security analysis of current architectures’, Technical Report JRC99976, 2015.

[21] A. Antonopoulos, *Bitcoin Q&A: How long until mainstream adoption?* 2017.

[22] S. Knut, ‘Energy dialogues and Energy Citizenship: Public Engagement in Energy Sustainability Transitions | Global Health Institute’, 2017. [Online]. Available: http://ghi.wisc.edu/event/energy-dialogues-and-energy-citizenship-public-engagement-in-energy-sustainability-transitions/. [Accessed: 26-Nov-2017].

[23] N. Šahović and P. P. da Silva, ‘Community Renewable Energy - Research Perspectives -’, *Energy Procedia*, vol. 106, no. Supplement C, pp. 46–58, Dec. 2016.

[24] G. Walker and P. Devine-Wright, ‘Community renewable energy: What should it mean?’, *Energy Policy*, vol. 36, no. 2, pp. 497–500, Feb. 2008.

[25] EESC, ‘The Social Economy in the European Union.’, 2012.

[26] G. Seyfang, S. Hielscher, T. Hargreaves, M. Martiskainen, and A. Smith, ‘A grassroots sustainable energy niche? Reflections on community energy in the UK’, *Environ. Innov. Soc. Transit.*, vol. 13, no. Supplement C, pp. 21–44, Dec. 2014.

[27] F. Geels and J. J. Deuten, ‘Local and global dynamics in technological development: a socio-cognitive perspective on knowledge flows and lessons from reinforced concrete’, *Sci. Public Policy*, vol. 33, no. 4, pp. 265–275, May 2006.

[28] G. Dóci, E. Vasileiadou, and A. C. Petersen, ‘Exploring the transition potential of renewable energy communities’, *Futures*, vol. 66, no. Supplement C, pp. 85–95, Feb. 2015.

[29] U. S. G. A. Office, ‘Cybersecurity: Challenges in Securing the Electricity Grid’, no. GAO-12-926T, Jul. 2012.

[30] J. Liu, Y. Xiao, S. Li, W. Liang, and C. L. P. Chen, ‘Cyber Security and Privacy Issues in Smart Grids’, *IEEE Commun. Surv. Tutor.*, vol. 14, no. 4, pp. 981–997, Fourth 2012.

[31] V. Y. Pillitteri and T. L. Brewer, ‘Guidelines for Smart Grid Cybersecurity’, *NIST InteragencyInternal Rep. NISTIR - 7628 Rev 1*, Sep. 2014.

[32] F. Aloul, A. R. Al-Ali, R. Al-Dalky, M. Al-Mardini, and W. El-Hajj, ‘Smart Grid Security: Threats, Vulnerabilities and Solutions’, *Int. J. Smart Grid Clean Energy*, pp. 1–6, 2012.

[33] W. Wang and Z. Lu, ‘Cyber security in the Smart Grid: Survey and challenges’, *Comput. Netw.*, vol. 57, no. 5, pp. 1344–1371, Apr. 2013.

[34] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, ‘A Survey on Cyber Security for Smart Grid Communications’, *IEEE Commun. Surv. Tutor.*, vol. 14, no. 4, pp. 998–1010, Fourth 2012.

[35] R. Anderson and S. Fuloria, ‘Who Controls the off Switch?’, in *2010 First IEEE International Conference on Smart Grid Communications*, 2010, pp. 96–101.

[36] U. Greveler, B. Justus, and D. Loehr, ‘Multimedia content identification through smart meter power usage profiles’, in *in Computers, Privacy and Data Protection (CPDP*, 2012.

[37] F. D. Garcia and B. Jacobs, ‘Privacy-Friendly Energy-Metering via Homomorphic Encryption’, in *Security and Trust Management*, 2010, pp. 226–238.

[38] ‘Smart meters prepaid: Bankymoon develops Bitcoin solution’, *Metering.com*. [Online]. Available: https://www.metering.com/smart-meters-payment-bankymoon-develops-bitcoin-solution/. [Accessed: 31-Oct-2017].

[39] T. Dimitriou and G. Karame, ‘Privacy-friendly tasking and trading of energy in smart grids’, 2013, p. 652.

[40] N. Zhumabekuly Aitzhan and D. Svetinovic, ‘Security and Privacy in Decentralized Energy Trading through Multi-signatures, Blockchain and Anonymous Messaging Streams’, *IEEE Trans. Dependable Secure Comput.*, pp. 1–1, 2016.

[41] M. Mihaylov, S. Jurado, N. Avellana, K. Van Moffaert, I. M. de Abril, and A. Nowe, ‘NRGcoin: Virtual currency for trading of renewable energy in smart grids’, 2014, pp. 1–6.

[42] R. D. Leonhard, ‘Developing Renewable Energy Credits as Cryptocurrency on Ethereum’s Blockchain’, Social Science Research Network, Rochester, NY, SSRN Scholarly Paper ID 2885335, Dec. 2016.

[43] A. M. Antonopoulos, *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*, 1 edition. O’Reilly Media, 2014.

List of abbreviations and definitions

AC	Alternating Current
DC	Direct Current
DDoS	Distributed DoS
DIN	Deutsches Institut für Normung
DLT	Distributed Ledger Technology
DoS	Denial of Service
IDS	Intrusion Detection System
IP	Internet Protocol
IT	Information Technology
MitM	Man in the Middle
PKI	Public Key Infrastructure
REC	Renewable Energy Credits
SNM	Strategic Niche Management
SQL	Structured Query Language
UPS	Uninterruptible Power Supply
VPN	Virtual Private Network

List of figures

List of tables

Annexes

Annex 1: Hardware Components Details.

This section provides some technical details about the components installed in our laboratory.

Solar panels

Three solar panels have been installed on the roof of the building in order to have production of electricity. Each of them have a size of 119 by 54 cm with an instant power of 80 Watts, and a peak production of up to 400 watthours per day.

As shown in Figure 10, three pairs of cables (positive and negative from each panel) come down from the roof to the lab to be connected to the to the batteries and the DC meters.

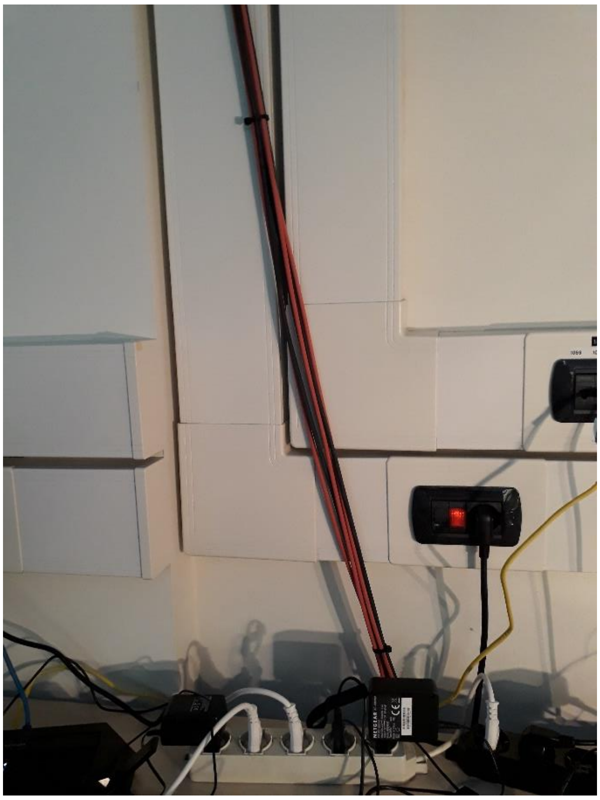


Figure 10. DC cables coming from solar panels on the roof of the building

Batteries and battery chargers

As explained before, energy produced by the panels can be stored in batteries. For each of the three panels there is a valve regulated lead-acid battery (model Yuasa SWL 2500EFR) with a nominal voltage 12 Volts and a capacity of 90 ampere hour (Ah)[13]. The discharge power at 20° C to 9.6 Volts is 2500 Watts, and weight is 32 Kgs. Each of them is placed in water-proof box that provides cabling and a charging controller (Figure 11).

Charging from the panels is done directly, while charging from AC supply needs the interconnection of a battery charger. Therefore, three battery chargers (model RS AC1012A) providing a maximum charging current of 10 Amperes have been installed. They do not take energy from external supplies but only from the local AC bus and then from the simulated mains when the former is not able to provide enough energy or there was no agreed energy exchange between nodes.

[13] 10-hr rate Capacity to 10.8V at 20°C

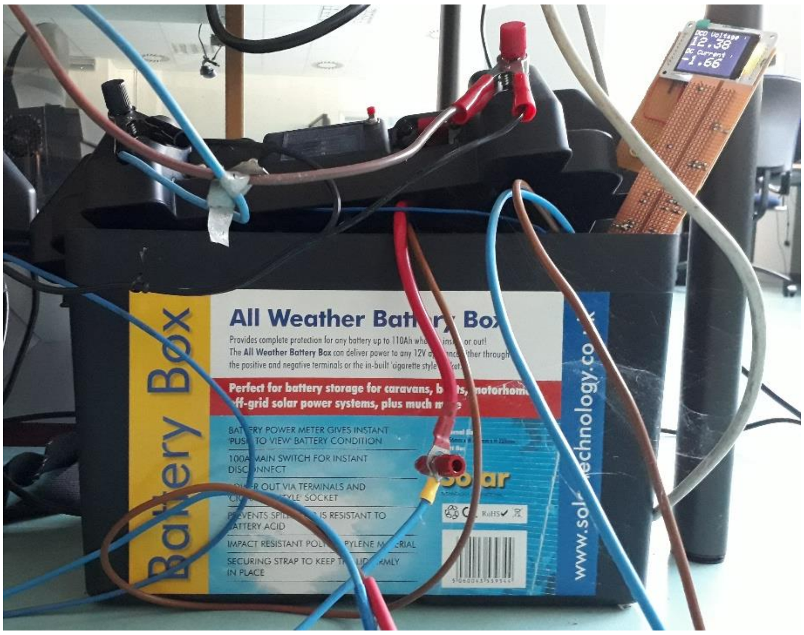


Figure 11. A battery box with cabling and voltage display

Off grid inverters

When a load internal to a node needs to use electricity, this is provided through an off grid inverter that converts DC to AC that can be used by the device acting as a load (e.g., a lamp). The inverter installed in the system were of two different types, one with 300 Watts of power (model Mercury IMS300-12) and another with 700 Watts (model Mean Well TS-700-212) (Figure 12). This difference is of course reflected on the number and types of load that can connected to the inverters.

The first inverter has in input voltage between 10.8 and 15.5 Volts (DC), and an output voltage of 230 Volts (AC) at 50 Hz with a modified sine wave form. It also provides a low battery protection with warning and critical shutdown.

The second inverter provides similar input range (10.5-15 Volts DC) and a selectable output voltage (200/220/230/240 Volts AC) at 50 or 60 Hz with true sine wave form. Similarly to the previous one, it provides also battery protection.

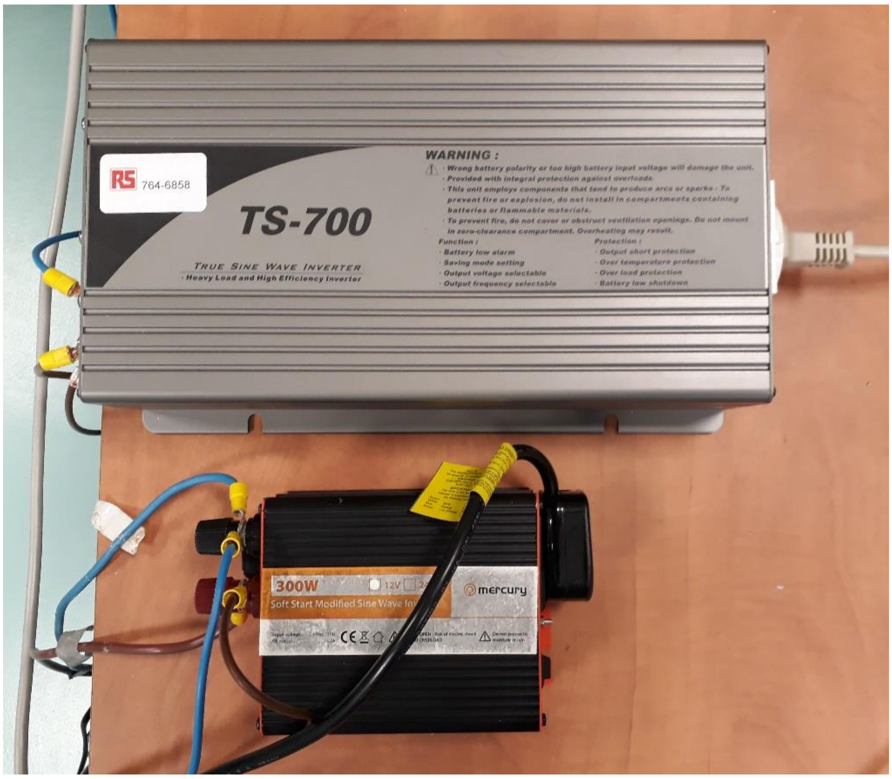


Figure 12. Off grid inverters

Bidirectional grid tie inverter

The bidirectional grid tie inverter seen in

Figure 9. Overview of the hardware infrastructure

is a key component of the system. It allows the node to exchange energy in both directions with the local AC bus and then with the simulated mains (i.e. the grid).

In our setup this device is implemented using two components:

A grid tie inverter, an inverter that can be connected directly to a main grid where energy utilities and other nodes trade energy. This inverter is monodirectional (from DC to AC) self-synchronising, meaning that it is able to sense the phase of the mains and inject current in a synchronous manner

A simple 12 volt battery charger (Figure 13) is used in order to withdraw alternating current from the grid and convert it to DC to recharge the battery or to power the internal loads (upon new conversion to AC done by the off grid inverter).

Figure 13. Battery charger

The grid tie inverter installed in the lab (model SUN-250G)(Figure 14) is able to provide a continuous power of 225 Watts (with a peak of 250) with an AC output voltage range between 190 and 260 Volts at 46-65 Hz. The DC input voltage range is 10.8-30 Volts.

The use of a grid tie inverter like the one employed in the infrastructure is very simple in a real scenario where a user can just connect it to any outlets of utility grid in the house. Like in the lab however, a smart meter should monitor and control the exchange of energy.

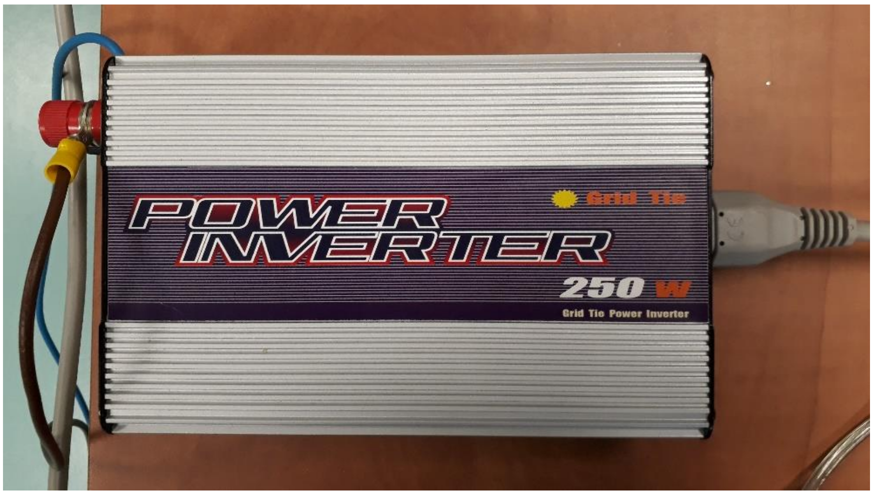


Figure 14. Grid tie bidirectional inverter

DC meters

The DC meter uses a current reading chip and a resistive partition circuit, it is useful for checking battery consumption in a solar system. Arduino YUN is used so the meter readings can be made available via WIFI on an ordinary web server. The circuit is powered by the battery itself. The measurement is set up so the power consumption of the device is not measured. This way the meter with no external loads should read zero current. Figure 15 and Figure 16 present the key componets of the smart meter: the current measurement chip and the DC-DC power supply. Figure 17 and Figure 18 show the schematic of the circuit and its actual look as implemeted.

Components:

- Pololu ACS709 Current Sensor Carrier[14] -75A to +75A

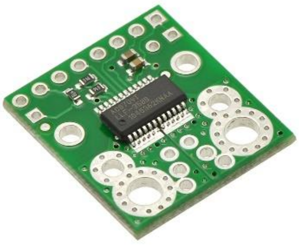


Figure 15. +- 75 Amps current meter

- DC-DC converter: Astec ASA01A18-LS 9-36 Vin 5 Vout @ 1Amp

[14] https://www.pololu.com/product/2199

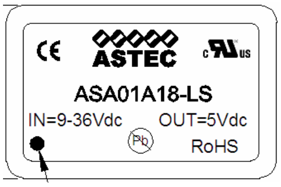
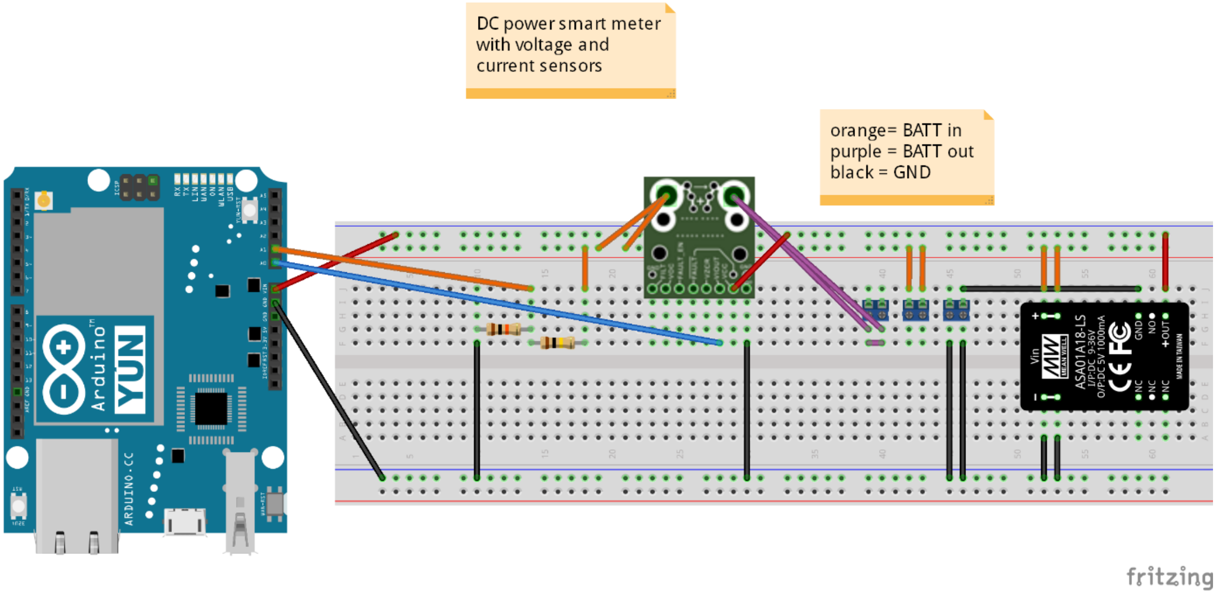


Figure 16. DC-DC converter


DC power smart meter with voltage and current sensors

orange= BATT in
purple = BATT out
black = GND

Figure 17. DC meter schematic

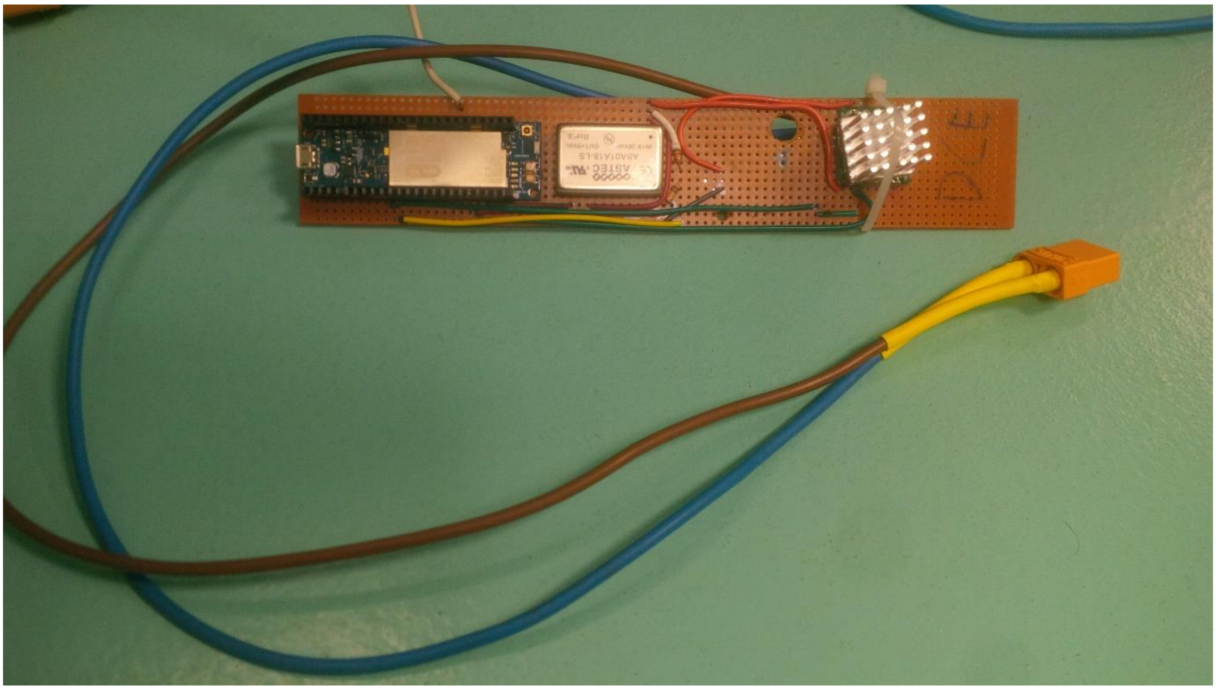


Figure 18. DC meter circuit

DC meter ratings:

- Polling time: 500 millsec.
- DC voltage range 0-20 V
- DC current range -75 +75 A

- Data transmission: WiFi / TCP/IP

AC smart meters and controllers

In order to control and monitor the AC power flow, custom made smart meters are employed. The computing/control platform used is an Arduino YUN IoT device. This device is TCP/IP capable and uses both wired and wireless Ethernet (Wi-Fi) for connectivity. The metering subsystem is based on a EmonTX Shield board plugged on top of the YUN. The control system is made of an Arduino 4 relay shield that control power flows. Relay one and two control the local loads, while relay 3 and 4 control the actual power exchange with the grid. Figure 19 shows the schematic of the actual configuration, while the complete device is visible in Figure 20 (in the top centre part of the electric panel).

Components:

- Arduino YUN[15]
- Arduino 4 relay shield[16]
- Open energy monitor EmonTx Arduino Shield[17]
- CT sensors[18]
- 9 V AC-AC transformer[19]

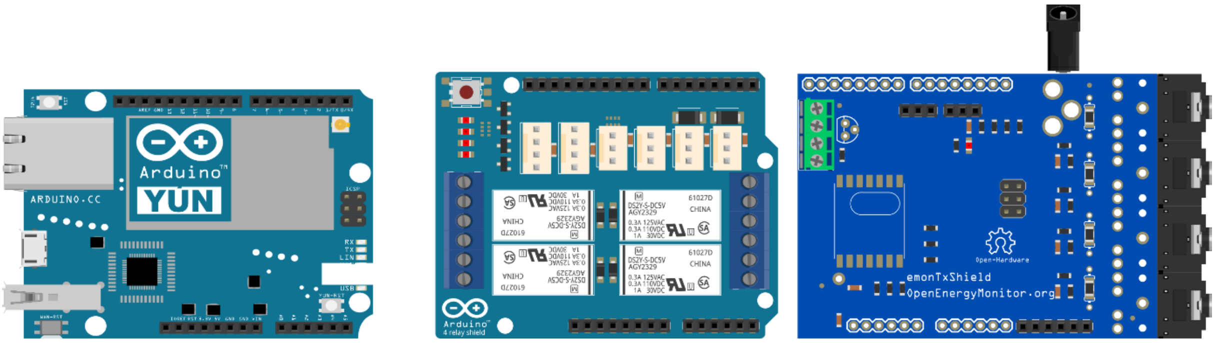


Figure 19. AC meter schematic

AC meter ratings:

- Polling time: 500 millsec.
- AC voltage range 100-300 V
- DC current range 0.1 - 90 A
- Data transmission: Wi-Fi / TCP/IP

UPS

The UPS, as stated before, simulates the mains where the nodes inject or withdraw energy and also other users can consume electricity. This allowed to have a safe and isolated grid instead of injecting directly to the mains of the lab (to which, of course, the UPS has been connected).

The device (model APC RT 2000) is able to provide a power capacity of 1.4 KWatts with a configurable output voltage of 220/230/240 Volts at a frequency of 50 or 60 Hz. Although the wattage is lower than what usually provided with a domestic subscription (3 KWatts), it still allows for the connection for several and quite powerful devices (e.g., the computers and dehumidifiers that were employed) that simulate external loads.

[15] http://www.linino.org/portfolio/yun/
[16] https://store.arduino.cc/arduino-4-relays-shield
[17] https://wiki.openenergymonitor.org/index.php/EmonTx_Arduino_Shield
[18] https://cdn2.bigcommerce.com/server4400/98a75/product_images/uploaded_images/sct013-000.jpg
[19] http://openenergymonitor.org/files/datasheet/EUR77DE-06-09-MI.pdf

Electric panel

Meters, interconnecting devices and cabling for every node were installed in an electricity panel like the one shown in Figure 20. The rack allows for the installation of switches and components on standard DIN rack and modules. In a real scenario, cables and interconnection can be simplified and switches and other controls made accessible through buttons and/or displays.

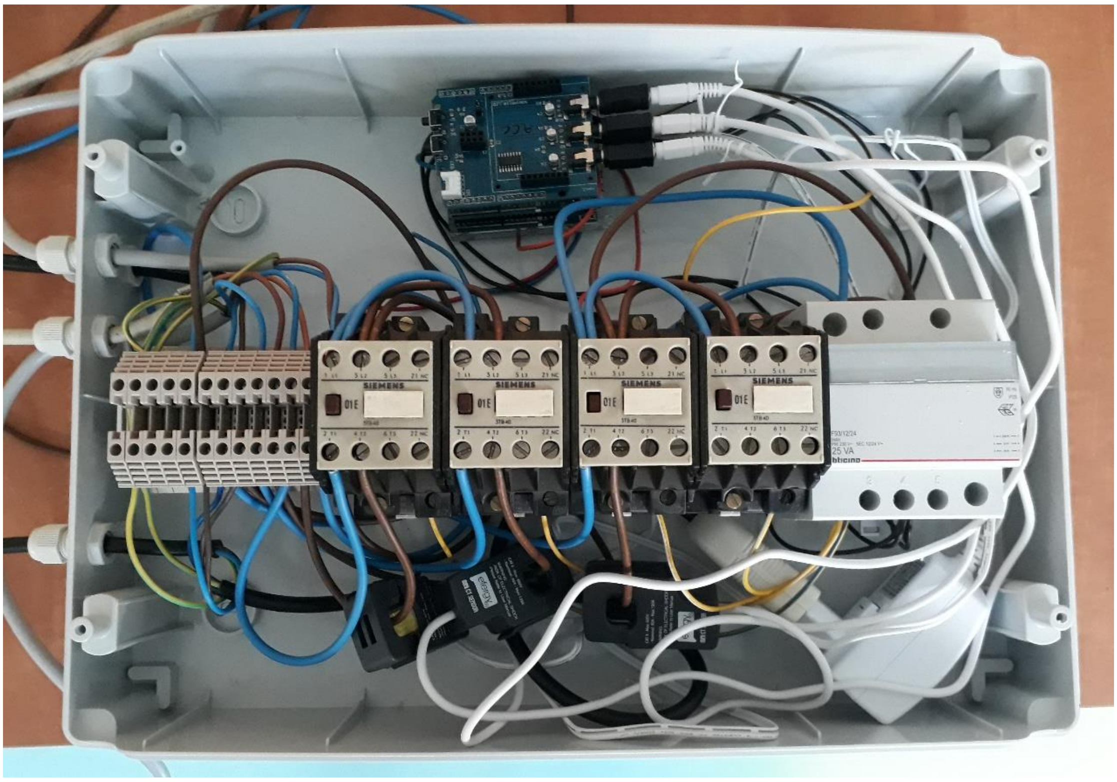


Figure 20. Electric panel with metering and interconnecting devices

Loads

Loads in the infrastructure were simulated using simple lights (e.g., for small consumptions inside the nodes) or more powerful devices such as computers or dehumidifiers (e.g., for bigger consumptions in the simulated mains). They were all connected to the AC source, so that there was no direct consumption of DC produced by the panels (except for a normal loss due to storage and conversion).

Annex 2. Coloured Coins

Coloured coins is a meta protocol that overlays information on small amounts of Bitcoin [43]. In particular, a small amount of Bitcoins is repurposed in order to express the possession of another asset. Extra labels are added to existing Bitcoins in order to indicate to what the coloured Bitcoin refers. This is done with the use of special wallets that add metadata to existing Bitcoins. An example of a coloured Bitcoin that contains a voucher redeemable for a cup of coffee is the following:

```
{
"source addresses": [
"1J2ZDBieMBiZm8cfRmh1sudzbZi6cbSxBB"
],
"contact_url": "https://www.kth.se/profile/kounelis/",
"name_short": "freeCoffee",
"name: "Free cup of coffee at the Angleria bar",
"issuer": "Ioannis Kounelis",
"description": "This voucher is redeemable for a free cup of coffee",
"description_mime": "text/x-markdown; charset=UTF-8",
"type": "Other",
"divisibility": 0,
"link_to_website": false,
"icon_url": null,
"image_url": null,
"version": "1.1"
}
```

Coloured Bitcoins can be transferred and exchanged as normal Bitcoins. Moreover, once used, the “colour” can be deleted. The actual term colour is a metaphor, since the coins do not actually have a real colour assigned to them. It is used in order to illustrate that an extra attribute has been added to these particular coins.

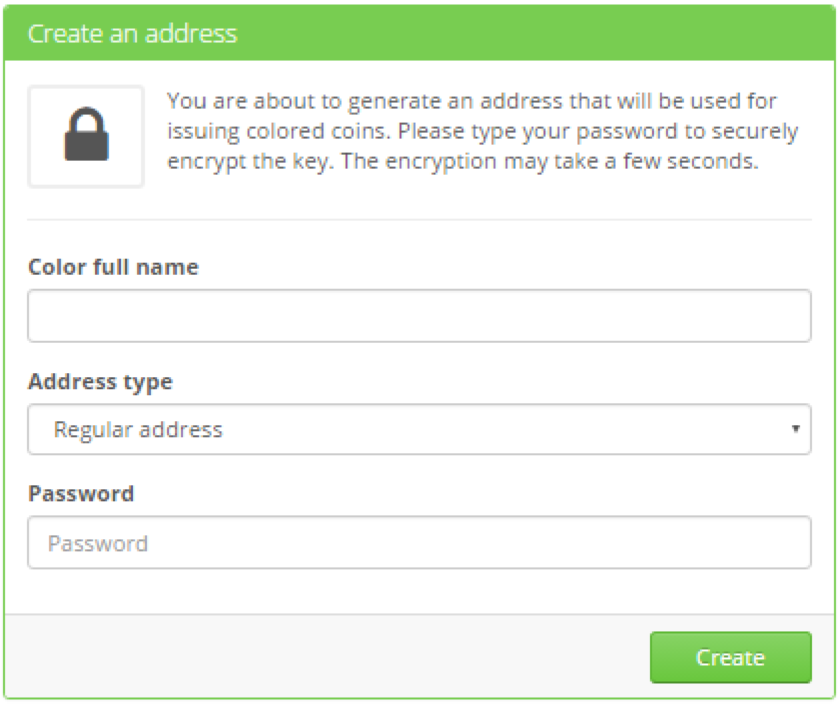
Coloured coins require special wallets in order to be handled. These wallets are Bitcoin wallets that in addition to Bitcoin support the metadata that coloured coins have. The most used coloured coins are analysed in the sections below.

CoinPrism

Coinprism[20] is probably the most detailed coloured wallet. After you register and create a wallet you are given the option to create your own currency (or colour as it is called in this wallet) by creating a bitcoin transaction and linking the new colour to it.

When creating a new colour, the first thing to do is to create an address that will be used for issuing coloured coins (Figure 21). The type of address is defined and the user's password is requested in order to proceed with the creation of the encryption keys.

[20] https://www.coinprism.com/



Create an address

You are about to generate an address that will be used for issuing colored coins. Please type your password to securely encrypt the key. The encryption may take a few seconds.

Color full name

Address type: Regular address

Password: Password

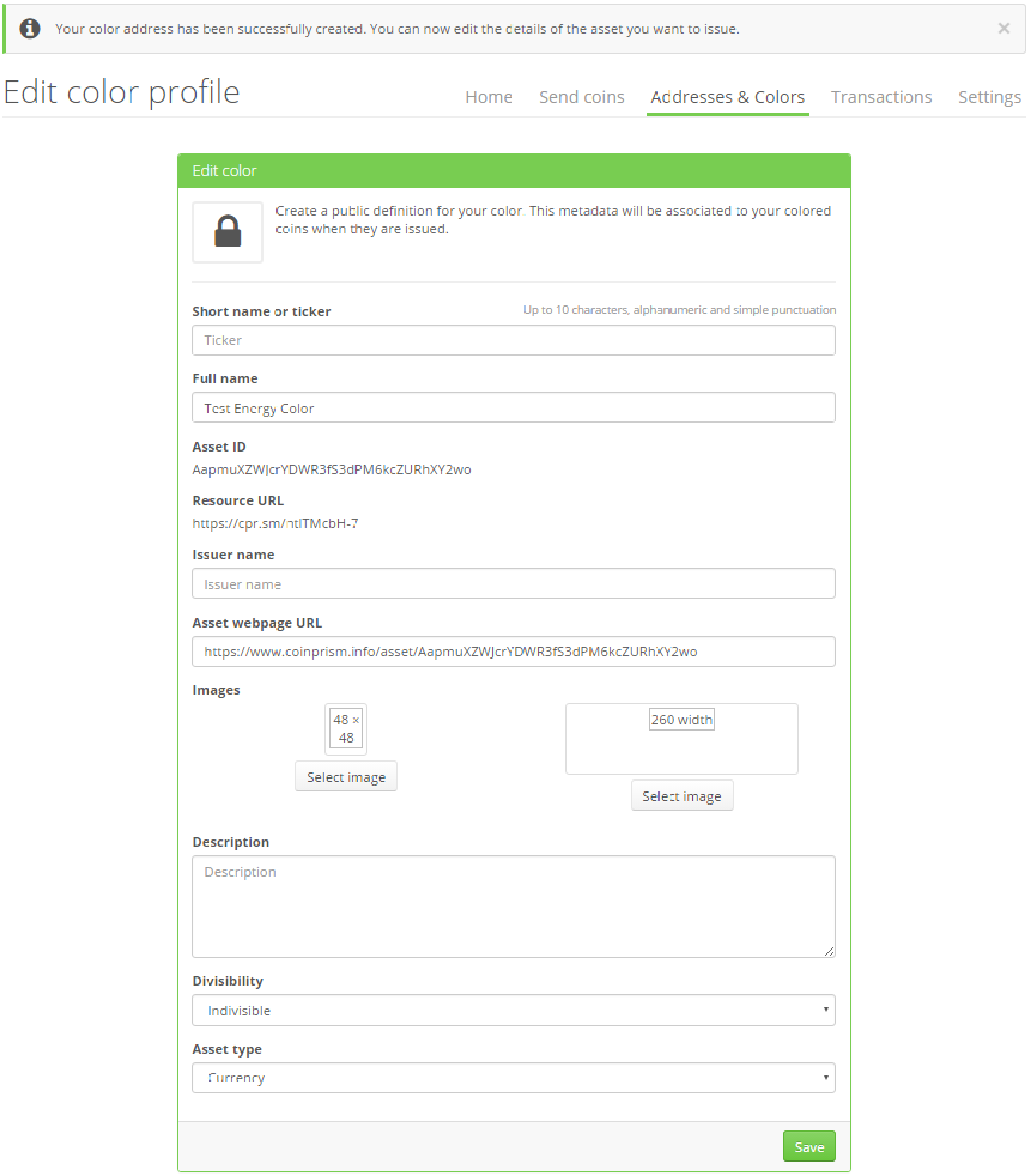
Figure 21. Creating an address with Coinprism

After having created the address, the user can edit the profile of the created colour (Figure 22). There are many parameters available in this step such as short, full name, and description of the colour, images that will be used as a logo, and issuer's name (which can be later verified).

One of the most important characteristics is the possibility to select the divisibility of the new colour. The user can select to make the new colour indivisible or to select up to 9 places of decimals for the division.

Another unique characteristic is that the asset type can be defined. There are several options to choose from, such as currency, stock, bond, commodity, points, collectible, smart property, and crypto-token.

Finally, the colour is automatically assigned a unique webpage URL that is publicly available so that all interesting parties can check its parameters as well as an Asset ID.



Your color address has been successfully created. You can now edit the details of the asset you want to issue.

Edit color profile

Edit color

Create a public definition for your color. This metadata will be associated to your colored coins when they are issued.

Short name or ticker — Up to 10 characters, alphanumeric and simple punctuation

Ticker

Full name

Test Energy Color

Asset ID

AapmuXZWJcrYDWR3fS3dPM6kcZURhXY2wo

Resource URL

https://cpr.sm/ntlTMcbH-7

Issuer name

Issuer name

Asset webpage URL

https://www.coinprism.info/asset/AapmuXZWJcrYDWR3fS3dPM6kcZURhXY2wo

Images

Description

Description

Divisibility

Indivisible

Asset type

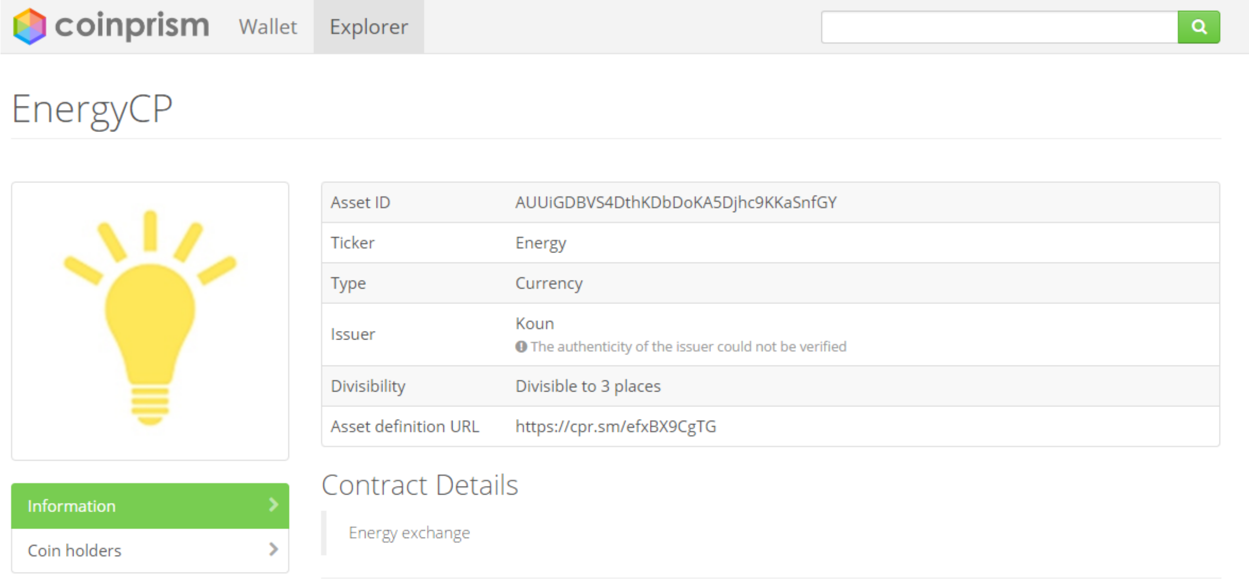
Currency

Figure 22. Editing the Color Profile

The resource URL (also called asset definition URL) is an array with all the colour's data:

```
{
  "asset_ids": [
    "AUUiGDBVS4DthKDbDoKA5Djhc9KKaSnfGY"
  ],
  "contract_url": "https://www.coinprism.info/asset/AUUiGDBVS4DthKDbDoKA5Djhc9KKaSnfGY",
  "name_short": "Energy",
  "name": "EnergyCP",
  "issuer": "Koun",
  "description": "Energy exchange",
  "description_mime": "text/x-markdown; charset=UTF-8",
  "type": "Currency",
  "divisibility": 3,
  "link_to_website": false,
  "icon_url":
"https://coinprism.blob.core.windows.net/profile/icon/AUUiGDBVS4DthKDbDoKA5Djhc9KKaSnfGY.jpg",
  "image_url":
"https://coinprism.blob.core.windows.net/profile/image/AUUiGDBVS4DthKDbDoKA5Djhc9KKaSnfGY.jpg"
,
  "version": "1.0"
}
```

The asset webpage URL provides graphical information on the colour (Figure 23) and also gives the possibility to see who are the coin holders and how many coins each one holds (Figure 24).



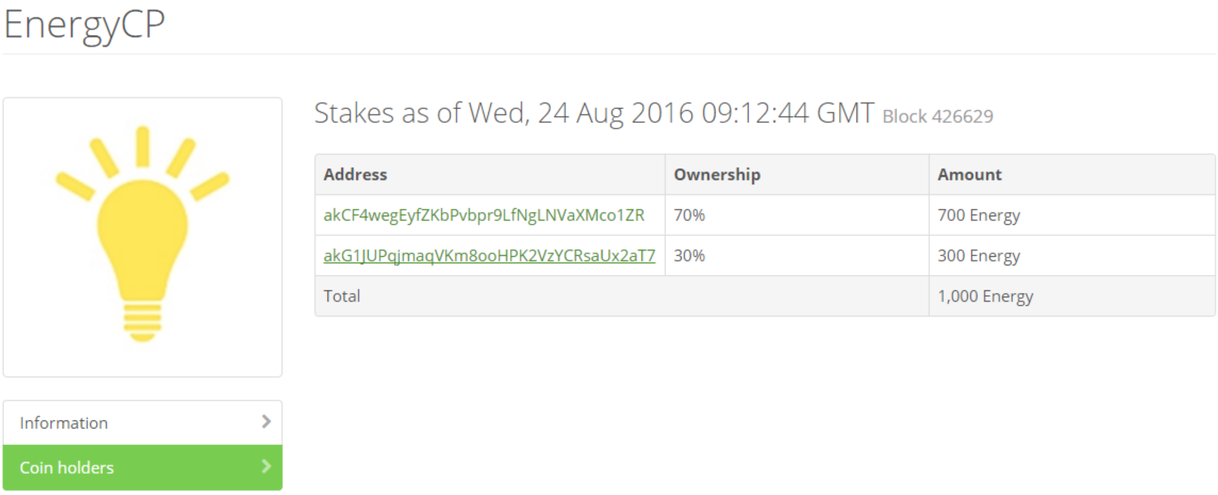
EnergyCP

Asset ID	AUUiGDBVS4DthKDbDoKA5Djhc9KKaSnfGY
Ticker	Energy
Type	Currency
Issuer	Koun ℹ The authenticity of the issuer could not be verified
Divisibility	Divisible to 3 places
Asset definition URL	https://cpr.sm/efxBX9CgTG

Contract Details

Energy exchange

Figure 23. Coin webpage



EnergyCP

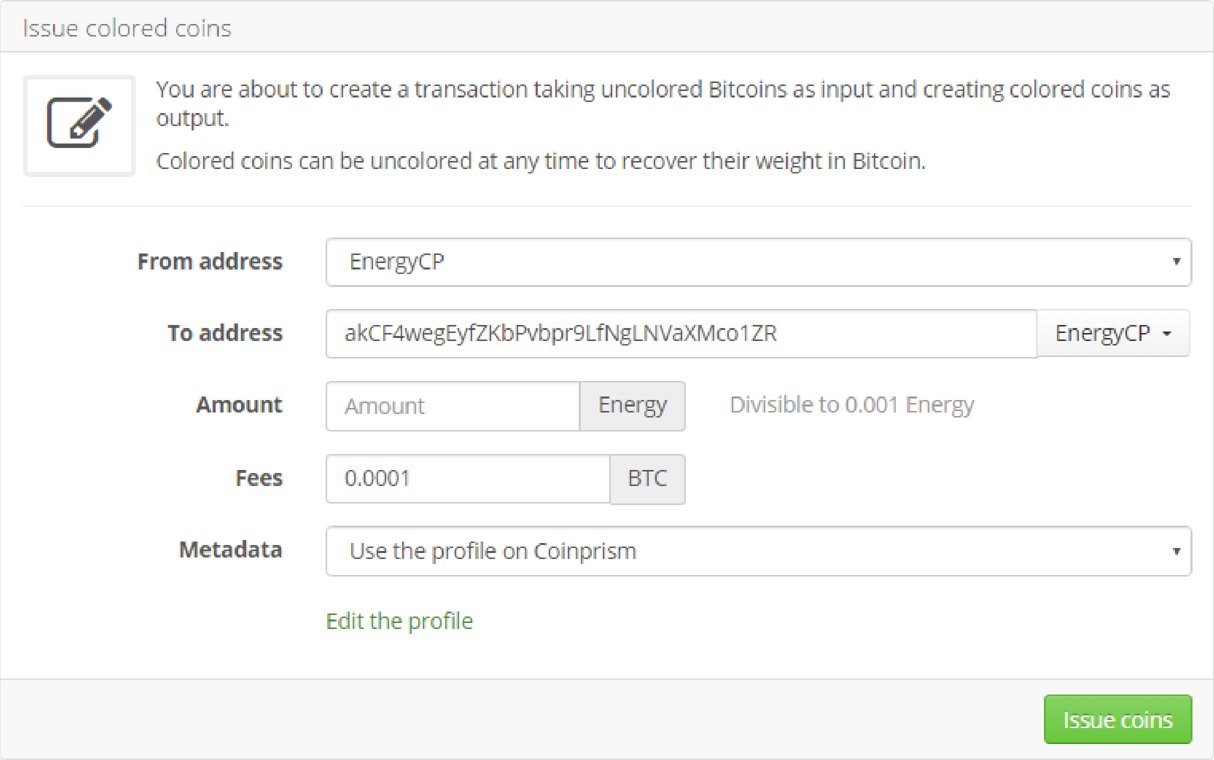
Stakes as of Wed, 24 Aug 2016 09:12:44 GMT Block 426629

Address	Ownership	Amount
akCF4wegEyfZKbPvbpr9LfNgLNVaXMco1ZR	70%	700 Energy
akG1JUPqjmaqVKm8ooHPK2VzYCRsaUx2aT7	30%	300 Energy
Total		1,000 Energy

Figure 24. Coil Holders

Once the colour has been created the next step is to issue coins. In order to do so the address that was generated at the beginning of the process needs to be funded with uncoloured Bitcoins (i.e. Bitcoins that have no other colours linked to them) in order to issue coins. As a results, Bitcoins need to be received in the associated Bitcoin address.

After having received Bitcoins, coloured coins can be issued (Figure 25). In order to do so, a transaction is made from the address that holds the Bitcoins towards the colour's address. The user decides how many coloured coins will be created with this transaction. The coins use the metadata of the colour that has previously been created.



Issue colored coins

You are about to create a transaction taking uncolored Bitcoins as input and creating colored coins as output.

Colored coins can be uncolored at any time to recover their weight in Bitcoin.

From address: EnergyCP

To address: akCF4wegEyfZKbPvbpr9LfNgLNVaXMco1ZR EnergyCP

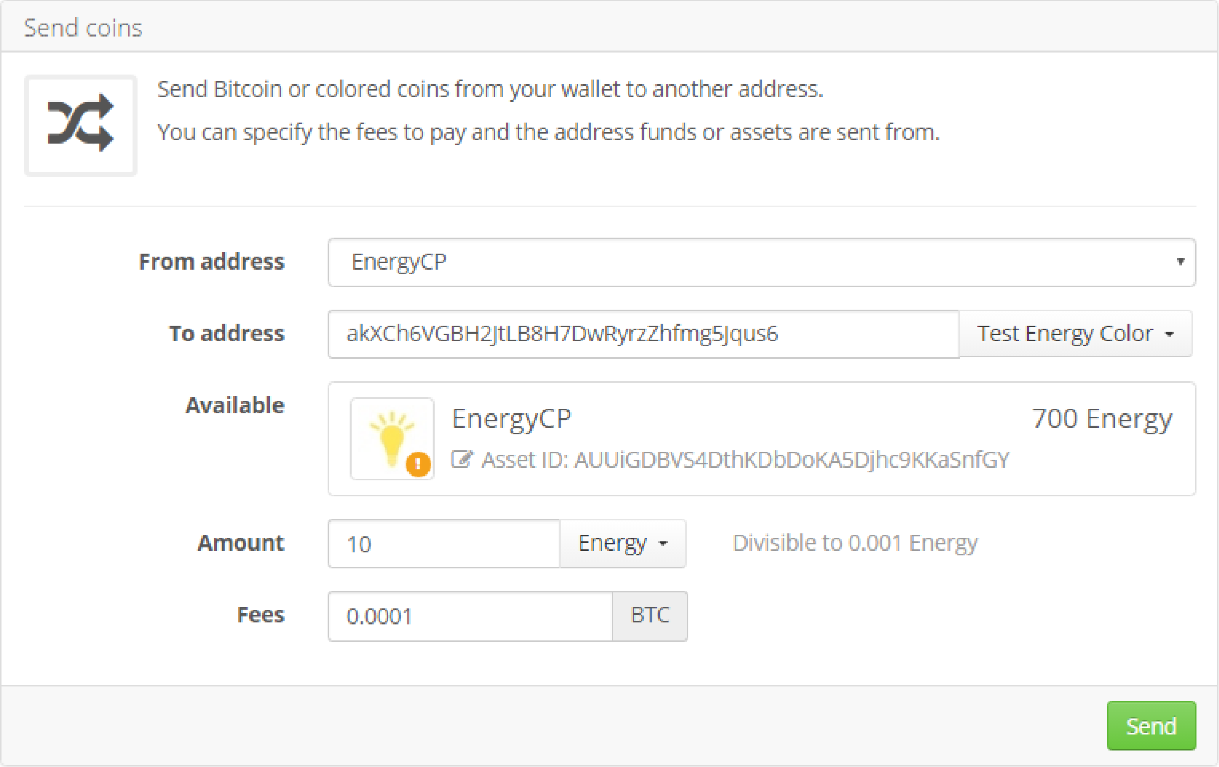
Amount: Amount Energy Divisible to 0.001 Energy

Fees: 0.0001 BTC

Metadata: Use the profile on Coinprism

Figure 25. Issuing coins

Once the coins have been created, they be sent to any other coloured address (Figure 26). The transaction is actually a bitcoin transaction that has linked to it the coloured coin transaction. Usually this transaction is of a very small amount of Bitcoins (a few hundred satoshi) but in such case the minimum suggested bitcoin transaction fee is of quite higher volume (usually 0.0001 BTC). In the example in Figure 27 in order to transfer 300 of EnergyCP coins a Bitcoin transaction of 0.000006 BTC was performed plus a transaction fee of 0.0001 BTC, in total 0.000106 BTC. For the current (i.e. 31/10/2017) BTC price of approx. 5450 Euro the total transaction cost is about 0.5 Euros.



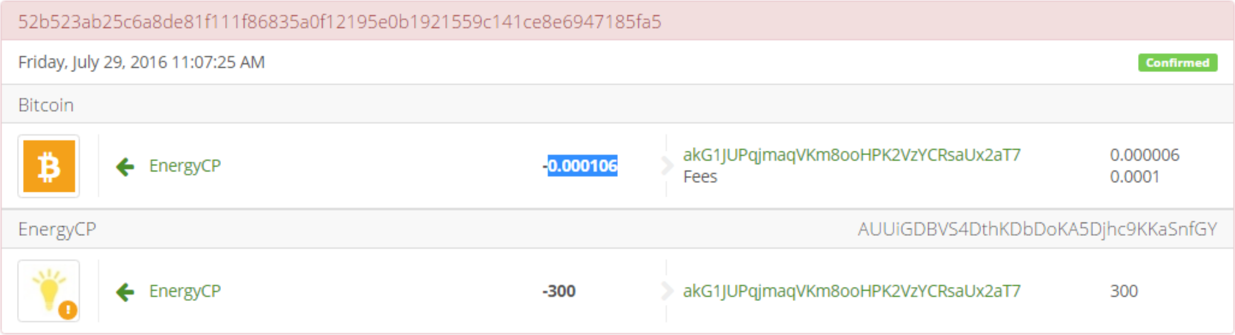
Send coins

Send Bitcoin or colored coins from your wallet to another address.

You can specify the fees to pay and the address funds or assets are sent from.

From address	EnergyCP
To address	akXCh6VGBH2JtLB8H7DwRyrzZhfmg5Jqus6 — Test Energy Color
Available	EnergyCP 700 Energy Asset ID: AUUiGDBVS4DthKDbDoKA5Djhc9KKaSnfGY
Amount	10 Energy — Divisible to 0.001 Energy
Fees	0.0001 BTC

Figure 26. Sending coins



52b523ab25c6a8de81f111f86835a0f12195e0b1921559c141ce8e6947185fa5

Friday, July 29, 2016 11:07:25 AM — Confirmed

Bitcoin

EnergyCP	-0.000106	akG1JUPqjmaqVKm8ooHPK2VzYCRsaUx2aT7 Fees	0.000006 0.0001

EnergyCP — AUUiGDBVS4DthKDbDoKA5Djhc9KKaSnfGY

EnergyCP	-300	akG1JUPqjmaqVKm8ooHPK2VzYCRsaUx2aT7	300

Figure 27. Colored coin transaction

Coinprism has also a mobile application. The application provides similar functionalities when it comes to receiving and sending both Bitcoins and coloured coins but does not support the creation of new colours and issuing new coins.

Colu

Colu[21] provides functionalities very similar to the ones of coinprism. Also on this platform you can create and use coloured coins with several options, control their use and transactions.

There are however some important differences. First of all, the interface of Colu[22] is, as its name suggests, a dashboard for creating coins rather that a pure wallet interface as in copay and coinprism. The user can easily create and distribute new coins but it is not clear

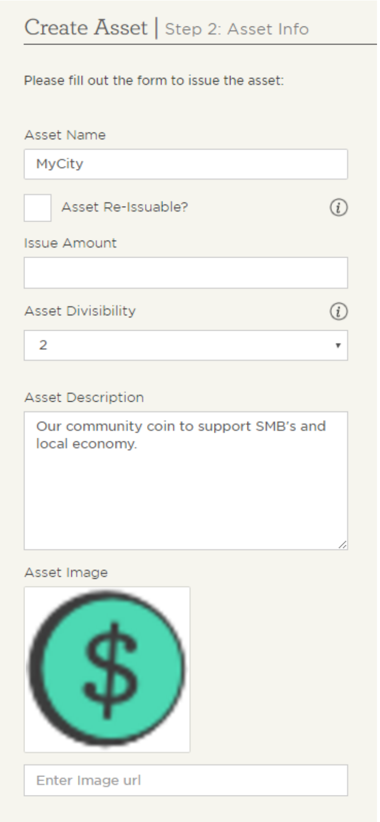
[21] https://www.colu.com/

[22] https://dashboard.colu.co/

if he/she can also receive other coins from other users. Moreover, no Bitcoin transactions are directly supported; i.e. Colu is not a Bitcoin wallet.

Another difference is that Colu does not require from the user any Bitcoin deposits. Even if the transactions performed are of course Bitcoin transactions, Colu provides the necessary satoshi themselves.

Creating an asset (the term asset is used in Colu instead of colour) is very similar to the procedure of Coinprism. The user can select one of the predefined types (currency, digital gold, coupon, hours, etc.) or create his/her own template. After that the divisibility, name, description and icon are set (Figure 28). There is also an option to select whether the asset is re-issuable, which means that the user can issue in the future more coins of this asset. The value of the new coin can also be set with any exchange (Figure 29).



Create Asset | Step 2: Asset Info

Please fill out the form to issue the asset:

Asset Name: MyCity

□ Asset Re-Issuable?

Issue Amount:

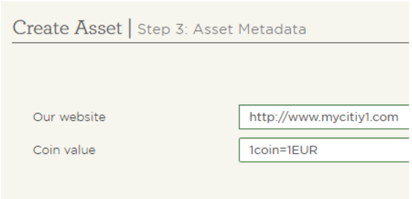
Asset Divisibility: 2

Asset Description: Our community coin to support SMB's and local economy.

Asset Image

Enter Image url

Figure 28. Colu. Creating an asset



Create Asset | Step 3: Asset Metadata

Our website: http://www.mycitiy1.com

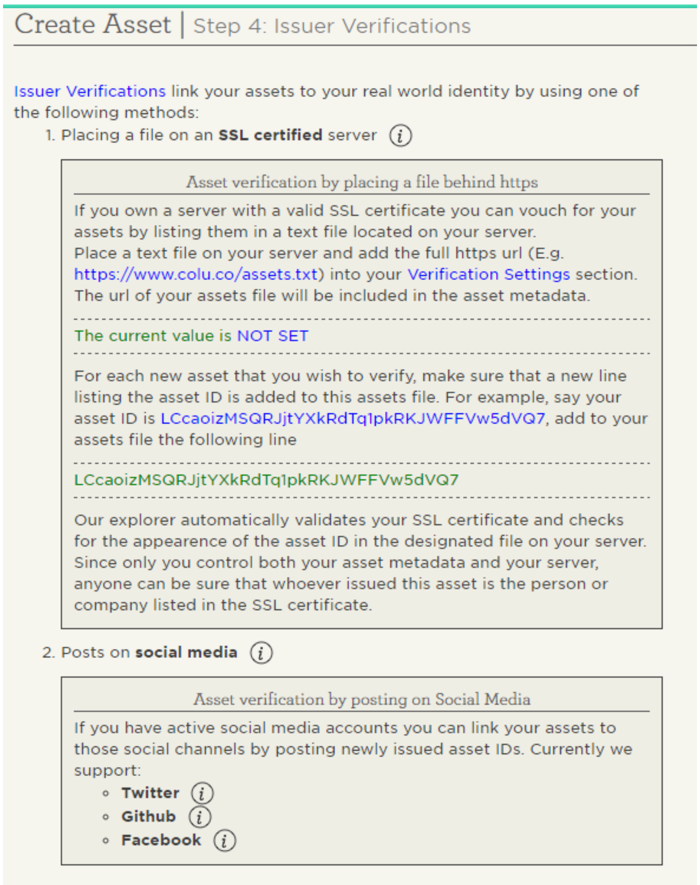
Coin value: 1coin=1EUR

Figure 29. Setting the website and coin value of the new asset

The final step is the process of verifying the issuer of the asset (Figure 30). There are two ways to do so:

i. To create a customized file under an SSL certified server.
ii. To link the asset to a social media account. Currently the accounts supported are Twitter, Github, and Facebook.

As mentioned also previously, transactions of assets can be sent without depositing Bitcoins. The transactions can performed towards another address, email or telephone. In the case of the email or telephone it is assumed that it corresponds to other already registered users and thus Colu is in the possession on their address in order to perform the transaction.



Create Asset | Step 4: Issuer Verifications

Issuer Verifications link your assets to your real world identity by using one of the following methods:

1. Placing a file on an **SSL certified** server ⓘ

Asset verification by placing a file behind https

If you own a server with a valid SSL certificate you can vouch for your assets by listing them in a text file located on your server.
Place a text file on your server and add the full https url (E.g. https://www.colu.co/assets.txt) into your Verification Settings section.
The url of your assets file will be included in the asset metadata.

The current value is NOT SET

For each new asset that you wish to verify, make sure that a new line listing the asset ID is added to this assets file. For example, say your asset ID is LCcaoizMSQRJjtYXkRdTq1pkRKJWFFVw5dVQ7, add to your assets file the following line

LCcaoizMSQRJjtYXkRdTq1pkRKJWFFVw5dVQ7

Our explorer automatically validates your SSL certificate and checks for the appearence of the asset ID in the designated file on your server. Since only you control both your asset metadata and your server, anyone can be sure that whoever issued this asset is the person or company listed in the SSL certificate.

2. Posts on **social media** ⓘ

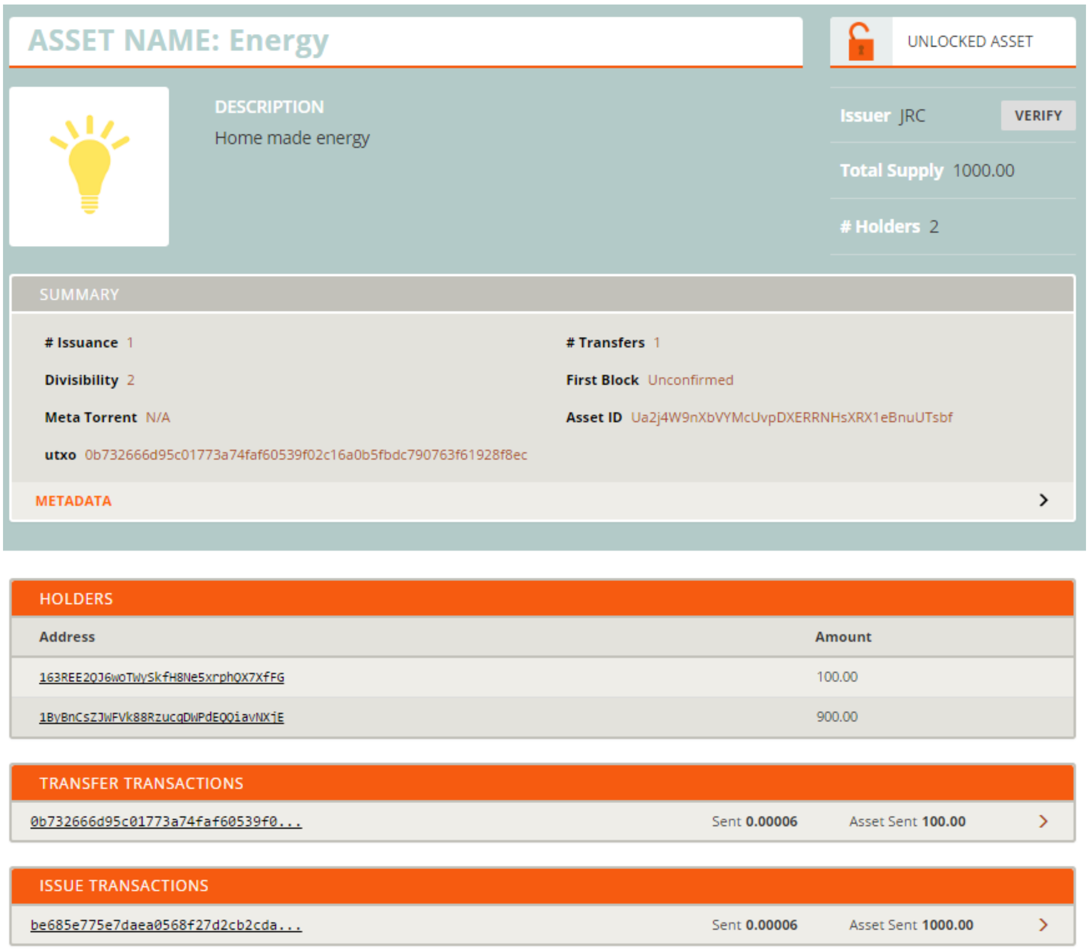
Asset verification by posting on Social Media

If you have active social media accounts you can link your assets to those social channels by posting newly issued asset IDs. Currently we support:

- **Twitter** ⓘ
- **Github** ⓘ
- **Facebook** ⓘ

Figure 30. Verifying the asset issuer’s ID

Each transaction performed, as well as the asset creation, is linked to the coloured blockchain explorer of coloured coins (Figure 31). On this page one can see all the information related to the asset as they were chosen during the creation phase. The issues can also be seen and if he/she had been verified, the verification will show as well.



ASSET NAME: Energy

UNLOCKED ASSET

DESCRIPTION
Home made energy

Issuer JRC VERIFY

Total Supply 1000.00

Holders 2

SUMMARY

Issuance 1

Divisibility 2

Meta Torrent N/A

utxo 0b732666d95c01773a74faf60539f02c16a0b5fbdc790763f61928f8ec

Transfers 1

First Block Unconfirmed

Asset ID Ua2j4W9nXbVYMcUvpDXERRNHsXRX1eBnuUTsbf

METADATA

HOLDERS

Address	Amount
163REE2QJ6woTWySkfH8Ne5xrphQX7XfFG	100.00
1ByBnCsZJWFVk88RzucqDWPdEQQiavNXjE	900.00

TRANSFER TRANSACTIONS

0b732666d95c01773a74faf60539f0...	Sent 0.00006	Asset Sent 100.00

ISSUE TRANSACTIONS

be685e775e7daea0568f27d2cb2cda...	Sent 0.00006	Asset Sent 1000.00

Figure 31. The Colu created asset on coloredcoins explorer

Coinprism cannot send an asset to Colu. Colu's address seems to be a Bitcoin address while Coinprism distinguished between Bitcoin and coloured addresses. Also the opposite is not possible, i.e. sending an asset from Colu to Coinprism. In the latter case the transaction is accepted on Colu's side as a valid transaction. However when it is received at Coinprism, it is only seen as a bitcoin transaction without having any colours/assets associated to it.

Annex 3. Helios Smart Contract

The following is the source code of the smart contract used for the Helios Coin. It is written in Solidity.

```
pragma solidity ^0.4.6;
contract owned {
    address public owner;

    function owned() {
        owner = msg.sender;
    }

    modifier onlyOwner {
        if (msg.sender != owner) throw;
        _;
    }

    //Probaly not needed for now
    function transferOwnership(address newOwner) onlyOwner {
        owner = newOwner;
    }
}

contract MyHeliosToken is owned {
  /* Public variables of the token */
  uint256 public totalSupply;     //Total supply of coins
  string public name;
  string public symbol;
  uint8 public decimals;

  uint8 private vote;

  /* This creates an array with all balances */
  mapping (address => uint256) public balanceOf;

  //events
  /* This generates a public event on the blockchain that will notify clients */
  event Transfer(address indexed from, address indexed to, uint256 value);

  //Constructor
  function MyHeliosToken(uint256 initialSupply, string tokenName, uint8 decimalUnits,
string tokenSymbol) onlyOwner(){
    totalSupply = initialSupply;
    balanceOf[msg.sender] = initialSupply;
    symbol = tokenSymbol;
    name = tokenName;
    decimals = decimalUnits;
  }

  //send measurements to node controller
  function sendMeasurements(address creator, uint256 measurement){
    //enum or struct?
    //prepei na apo8ikeuei prosorina tis metriseis pou erxontai sti dieu8insi tou creator
  }

  //Mint contract - @Owner, params: @addressCreator @numberOfCoinsCreated
  function mintToken(address target, uint256 mintedAmount) onlyOwner {
    balanceOf[target] += mintedAmount;
    totalSupply += mintedAmount;
    //Transfer(0, this, mintedAmount);//probably not needed
    Transfer(this, target, mintedAmount);
  }

  // Send coins
  function transfer(address _to, uint256 _value) {
    if (balanceOf[msg.sender] < _value) throw;            // Check if the sender has enough
    if (balanceOf[_to] + _value < balanceOf[_to]) throw; // Check for overflows
    balanceOf[msg.sender] -= _value;                      // Subtract from the sender
    balanceOf[_to] += _value;                             // Add the same to the recipient
    Transfer(msg.sender, _to, _value);                    // Notify anyone listening that this transfer took place
  }

  /* This unnamed function is called whenever someone tries to send ether to it */
  function () {
    throw;     // Prevents accidental sending of ether
  }

  // Function to recover the funds on the contract
  function kill() onlyOwner(){
     selfdestruct(owner);
   }

}//End of MySolarToken Contract
```

KJ-NA-29074-EN-N

JRC Mission

As the science and knowledge service of the European Commission, the Joint Research Centre's mission is to support EU policies with independent evidence throughout the whole policy cycle.

EU Science Hub
ec.europa.eu/jrc

@EU_ScienceHub

EU Science Hub - Joint Research Centre

Joint Research Centre

EU Science Hub

Publications Office

doi:10.2760/121912
ISBN 978-92-79-77773-8