SOFIE - Secure Open Federation for Internet Everywhere

779984

DELIVERABLE D6.7

Initial Report on Communication, Dissemination, and Exploitation

Project title	SOFIE – Secure Open Federation for Internet Everywhere
Contract Number	H2020-IOT-2017-3 – 779984
Duration	1.1.2018 – 31.12.2020
Date of preparation	19.12.2019
Author(s)	Dmitrij Lagutin (Aalto), Mikael Jaatinen (Ericsson), Priit Anton (GT), David Mason (Rovio), George Polyzos (AUEB-RC), Petri Laari (Ericsson), Mirjam Kert (GT), Liis Livin (GT)
Responsible person	Liis Livin (Guardtime), liis.livin@guardtime.com
Target Dissemination Level	Public
Status of the Document	Completed
Version	1.10
Project web-site	https://www.sofie-iot.eu/

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 779984.

Summary of changes compared to previous version

Version	Major changes
1.10	In the updated version of deliverable 6.7 “Initial Report on Communication, Dissemination, and Exploitation” IPR has been clearly defined in chapter 5.5 and components of commercial exploitation have been specified within the added chapter 5, through presenting the Business Model Canvas framework for the pilots. In addition, some slight changes were made throughout the deliverable’s text to facilitate the coherence of the primary changes listed above.

Table of Contents

1. Introduction

The present document, Deliverable 6.7 - Initial report on Communication, Dissemination and Exploitation, comprises communication, dissemination, and exploitation activities and results undertaken during the first 13 months on the project. It will be updated by D6.8 - Interim report on Communication, Dissemination, and Exploitation (M25) and D6.11 - Final report on Communication, Dissemination, and Exploitation (M36).

All consortium partners contributed to this deliverable, expressing their communication, dissemination and exploitation interests and results according to their own organizations' strategical interest.

The document begins in Section 1 that presents the results of communication activities, followed by Section 2 and 3 that re dedicated to the dissemination and exploitation activities of the project partners.

Deliverable D6.7 is part of the activities of WP6 “Communication, Dissemination, and Exploitation”. It is a public document which will be made available on the project website for those stakeholders interested in the SOFIE project.

2. Communication

This section provides an overview of the communication tools and activities conducted within the first 13 months of the project.

2.1 Communication tools

2.1.1 Logo

The SOFIE logo was created in the beginning of the project. As SOFIE stands for Secure Open Federation of Internet Everywhere, the circle in the logo is left open to symbolise the notion of openness of the SOFIE federation. The logo has been used on communication materials such as website, flyer, presentations, business card etc. The logo can be downloaded from the SOFIE website: http://www.sofie-iot.eu/assets/sofie-logo.svg.

2.1.2 Applications of the logo

Figure 1. The SOFIE logo.

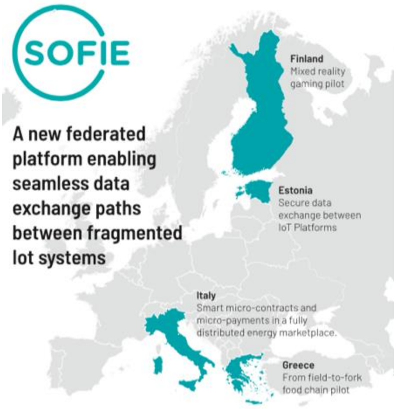

SOFIE
A new federated platform enabling seamless data exchange paths between fragmented Iot systems
Finland
Mixed reality gaming pilot
Estonia
Secure data exchange between IoT Platforms
Italy
Smart micro-contracts and micro-payments in a fully distributed energy marketplace.
Greece
From field-to-fork food chain pilot

Figure 2. The SOFIE flyer.

2.1.3 Flyer

The first SOFIE flyer was produced in March 2018, completing D6.3 on time. The flyer will be updated periodically throughout the project. It has been handed out at events like ICT2018, IoT Week 2018, and Junction hackaton. The flyer can be downloaded from SOFIE website: https://media.voog.com/0000/0042/0957/files/sofie-poster.pdf.

2.1.4 Business card

The SOFIE business card was created as an alternative for the flyer. The business card is something that the SOFIE project members can easily take with them and distribute at events they attend. The business contains the most relevant information such as the website address, social media contacts, and information e-mail.

2.2 Website

The SOFIE website was completed in in February 2018. The official home on the web is: https://www.sofie-iot.eu.

The goal of the website is to provide a visible presence on the internet and serve as a one stop shop for information about the project and to present its latest achievements. The site was created using the Voog platform. The website is regularly updated to assure that visitors get coherent and timely information about the project as it develops. The visitor numbers of the webpage keep growing having approximately 300-450 visitors per month.

The SOFIE website has been updated several times with the following “News” items:

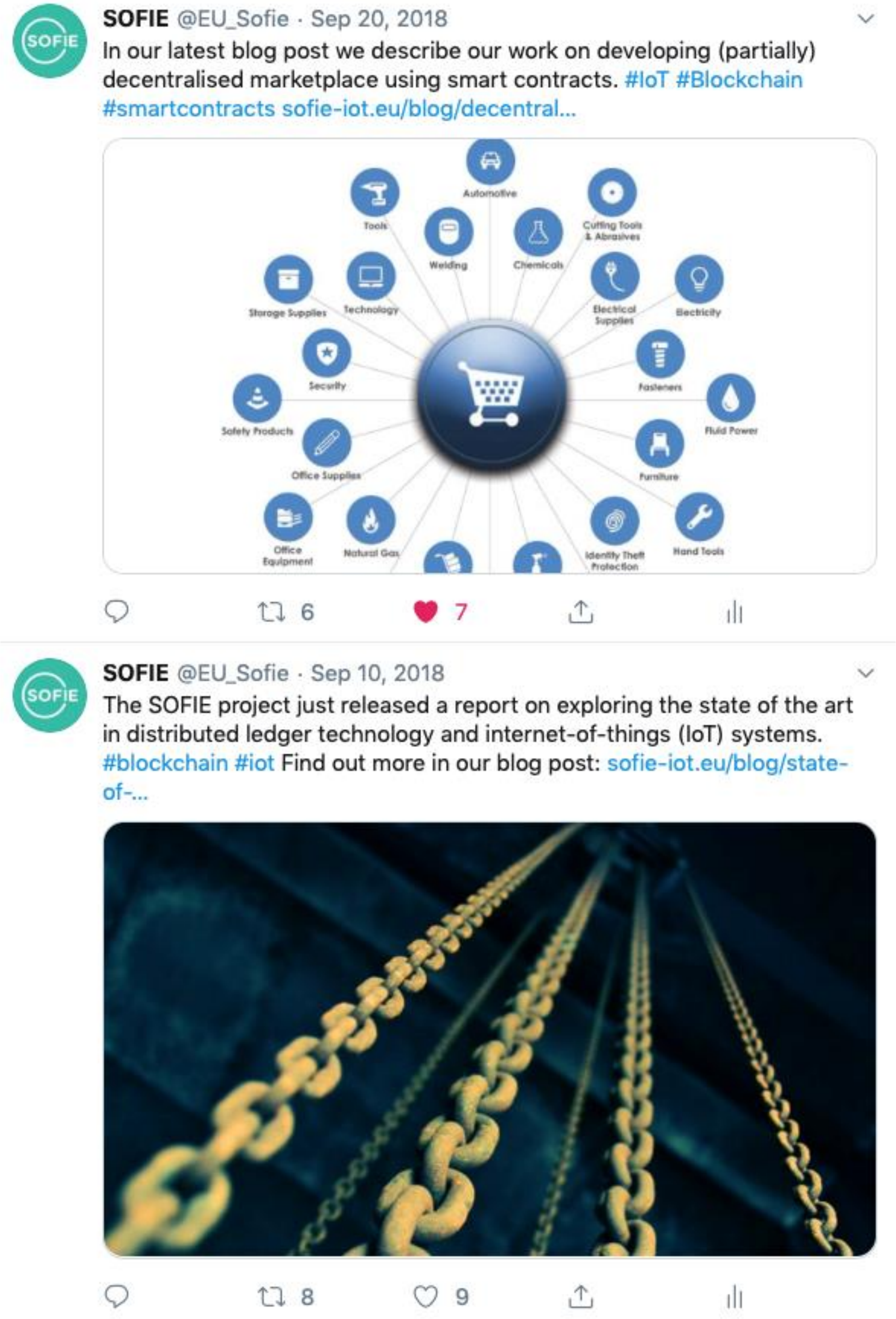
- Junction 2018 - Europe’s biggest hackathon
- Decentralized marketplace using smart contracts
- State of the Art in Blockchain Technology and IoT Systems
- A secure blockchain-based energy marketplace for load balancing in Low Voltage distribution grids
- Utilizing blockchain technology for providing product insights from-field-to-fork
- Blockchain technology to secure cross-border data exchange between smart meter platforms
- SOFIE presented at NDSS
- EU research looks into open federated IoT business platforms

2.3 Social networks

We have created accounts in two popular social networks in order to create a channel through which we can publicise our advances and our presence at marketing events and our project results.

- Twitter (@EU_Sofie), https://twitter.com/EU_Sofie.
- LinkedIn, https://www.linkedin.com/company/sofie-project.

The number of social media followers is increasing over time and the reach/impressions on these mediums are in correlation with other communication activities, e.g. when SOFIE is exhibited at an event the number of followers increases and the reach of the messages posted on the social media increases as well.



SOFIE @EU_Sofie · Sep 20, 2018

In our latest blog post we describe our work on developing (partially) decentralised marketplace using smart contracts. #IoT #Blockchain #smartcontracts sofie-iot.eu/blog/decentral...

6 7

SOFIE @EU_Sofie · Sep 10, 2018

The SOFIE project just released a report on exploring the state of the art in distributed ledger technology and internet-of-things (IoT) systems. #blockchain #iot Find out more in our blog post: sofie-iot.eu/blog/state-of-...

8 9

Figure 3. SOFIE Twitter page.

2.4 Liaisons

The SOFIE project in collaboration with 5 (ENACT, ARMOUR, SMESEC, IoT Crawler, CIPSEC) other IoT projects organised a joint exhibition area at ICT2018.

The SOFIE project also participated in the CHARIOT (EU H2020 project) workshop in October 2018, and established liaisons with H2020 projects GHOST, CHARIOT and SEMIoTICS. In addition, in January 2018 the SOFIE project in collaboration with the POINT project were part of organising the Iothon hackaton.

2.5 Exhibitions

During the first year the SOFIE project was exhibited at two conferences. The first exhibition was in IoT Week 2018 in Bilbao and the second one in ICT2018, Vienna. During both of the exhibitions the SOFIE flyers and business cards were distributed. In addition, the demos for the Estonian energy pilot and Greek from-field-to-fork were introduced.

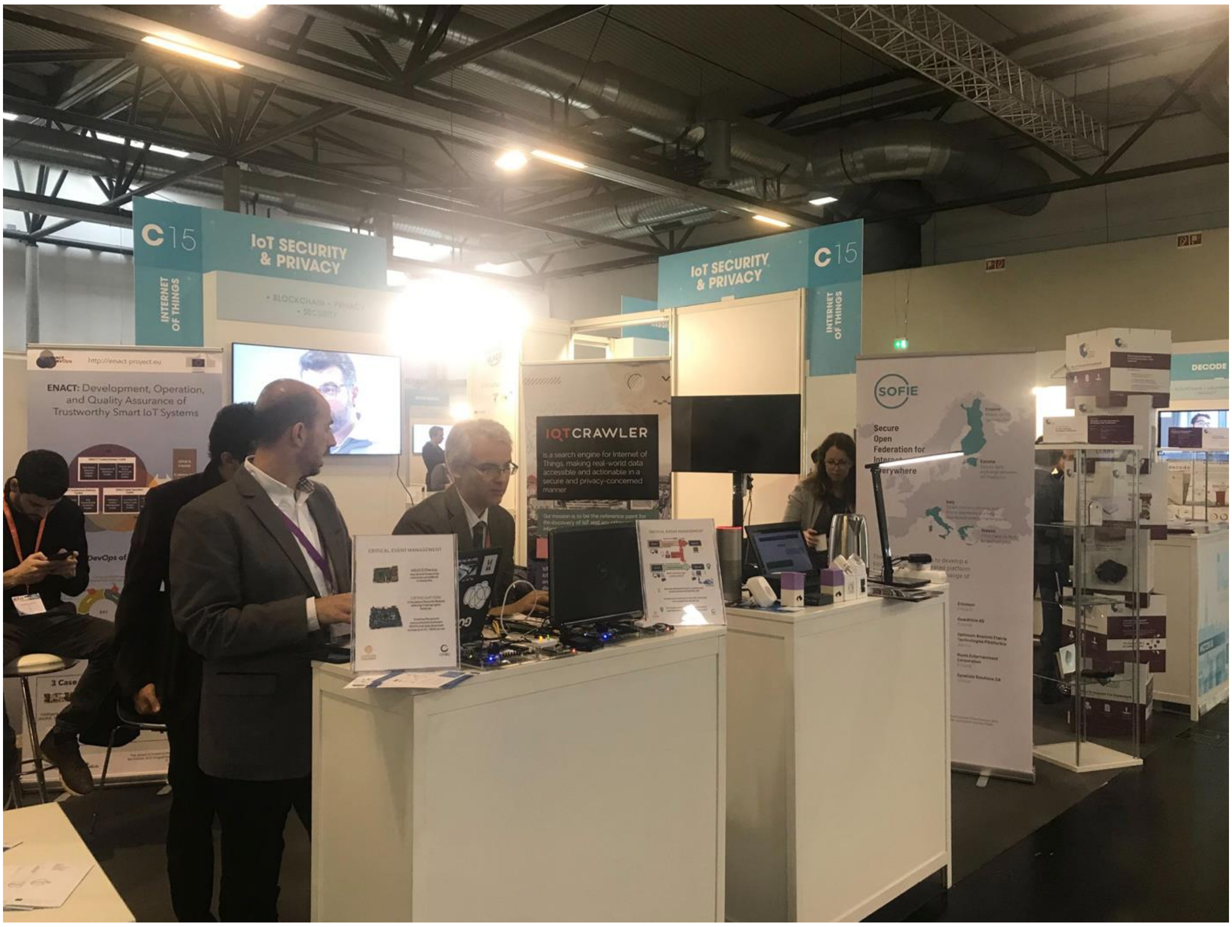

C15
IoT SECURITY & PRIVACY
INTERNET OF THINGS
ENACT: Development, Operation, and Quality Assurance of Trustworthy Smart IoT Systems
IOTCRAWLER
SOFIE
DECODE

Figure 4. SOFIE at ICT2018 in Vienna.

3. Dissemination

During the first 13 months of the project there were 6 publications published. In addition, 9 external presentations have been made.

3.1 Code Releases

SOFIE has planned for 3 main software releases. The first main release code has been made available in September 2018. The code is downloadable at GitHub: https://github.com/SOFIE-project.

Between main releases, the code base is improved through a continuous integration and deployment process.

3.2 Publications

During the first 13 months of the project there were 6 publications published. In addition, 9 external presentations have been made. All the scientific publications are also published on the project's website.

1. Secure Open Federation for Internet Everywhere. A. Karila, Y. Kortesniemi, D. Lagutin, P. Nikander, S. Paavolainen, N. Fotiou, G.C. Polyzos, V.A. Siris and T. Zahariadis. Workshop on "Decentralized IoT Security and Standards" (DISS) in conjunction with the 25th "Network and Distributed System Security Symposium" (NDSS 2018). Published 18.2.2018. https://dx.doi.org/10.14722/diss.2018.23001
2. Security and Privacy Challenges and Potential Solutions for DLT based IoT Systems. Santeri Paavolainen, Pekka Nikander. 2018 Global Internet of Things Summit (GioTS). Published 4.6.2018.
3. Smart Contracts for the Internet of Things: Opportunities and Challenges. N. Fotiou and G.C. Polyzos. European Conference on Networks and Communications (EuCNC). Published: 18.6.2018.
4. Interacting with the Internet of Things Using Smart Contracts and Blockchain Technologies. N. Fotiou, V. A. Siris, G.C. Polyzos. Proc. of Security, Privacy, and Anonymity in Computation, Communication, and Storage 2018 (SpaCCS 2018), Melbourne, Australia, 2018.
5. Turning the Trust Around: Smart contract-assisted Public Key Infrastructure. A. Ahmed, T. Aura. IEEE International Conference on Trust, Security and Privacy in Computing and Communications 2018.Published: 31.07.2018.
6. Risks from Spam Attacks on Blockchains for Internet-of-Things Devices. S. Paavolainen, T. Elo, P. Nikander. IEEE IEMCON 2018. Published: 02.11.2018.

3.3 Open data

As outlined in D6.5 - Data Management Plan, data that can compromise commercialization prospects or has inadequate protection of, e.g., personal information, shall not be published. The rest of the data will be deposited in an open access repository such as Zenodo (https://www.zenodo.org). When the data is related to a publication, it will be linked to it via OpenAIRE (https://www.openaire.eu).

Data available at Zenondo:

- Electric Vehicle (EV) data collected by Emotion. This data was collected using a particular OBD device connected to each EV. The dataset can be found here: https://www.zenodo.org/record/1410857#.XFBkLc8zau4 .

4. Exploitation

The exploitation of the project's results is the key element for the success of the SOFIE project. This chapter covers the knowledge advancement activities by academic partners, as well as the commercial exploitation and standardization efforts.

During the first year of the project it was identified that those SOFIE results that are closely related to the pilots, will have the strongest chance to survive and move to the pipeline for commercialization.

The following chapter starts with giving an overview of the general exploitation foreground, followed by the academic exploitation efforts. The second part of this chapter is dedicated to commercial exploitation (section 4.3) followed pilot exploitation plans in chapter 5.

4.1 Exploitable Foreground

Interledger

There exists a large number of DLTs each offering different tradeoffs in terms of latency, throughput, consensus algorithm, etc. Therefore, in complex systems it is not feasible to use a single DLT, hence the *interledger* approach that allows different DLTs to exchange data with each other is necessary in most situations. Using multiple ledgers is also necessary for privacy reasons, which affect both individuals and companies. By default, all participants within a DLT can access all the data stored in the DLT, therefore the participant may use private ledger, and store only a subset of his data to main ledger used for collaboration with others. Multiple ledgers are also necessary to enable crypto-agility, cryptographic algorithms used by DLTs such as SHA-256 will not stay safe forever, therefore it is necessary to have a mechanism to transfer data from one ledger to another.

Decentralized identifiers and Verifiable Credentials

Decentralized identifiers (DIDs) are a privacy-promoting self-sovereign type of identifier, where the owner of the identifier is free to create, use, modify or revoke the identifier at will and free of any controlling central entity. A related technology, verifiable credentials (VCs), allows one to make reliable attestations about the owner of the identifier. In SOFIE, DIDs will be used in co-operation with legacy identifiers to support privacy-preserving cross-ledger operations, and VCs will be used to authenticate and authorise the users of the services.

System dynamics models of business platform network effects

System dynamics models are causal loop diagrams, which include simulation equations and real-world data as inputs to the model. Simulation results and scenarios can thus be produced by using standard tools such as Vensim[1]. In the future, we plan to model SOFIE IoT platforms with System Dynamics. These models can be used to simulate the data markets, the economic sensitivity, and economic sustainability of the platform businesses.

IoT federation adapters for open and commercial IoT platforms

IoT federation adapters enable interoperability of legacy IoT platforms with SOFIE business platforms and interledger operations. Each IoT federation adapter should be able to proactively adapt and reconfigure data from devices to align with semantics, service discovery, access control, security and privacy specifications dictated by SOFIE architecture. In SOFIE, a common

[1] https://vensim.com/

framework for secure adaptation of IoT platforms and devices will be released on top of which specific implementations will be implemented for each integrated IoT platform.

Decentralized marketplace, DSO congestion detection and EV flexibility provision

The *decentralized marketplace* will be applied in the Italian Energy pilot in conjunction with the *DSO congestion detection dashboard* used by the DSO to detect potential congestion points and the *EV flexibility provision dashboard* used by the Fleet Manager to monitor and manage the electric vehicles and the charging stations and to provide flexibility to DSO.

The components will be used to create specific Demand Response (DR) campaigns leveraging distributed ledger technologies and smart contracts capabilities.

Blockchain federation

The SOFIE project is relevant to ASM in terms of new tools and services to make the distribution power network stable and secure. The high penetration of DR in the Terni's area has led to a significant increase of the reverse power flow in the substations and number of congestions. Matching consumption with production through secure and efficient DR strategies using blockchain technology represents nowadays one of the most promising approach for the DSO's grid management. Thanks to the blockchain driven federated IoT business platform developed under the SOFIE project, smart micro-contracts and micro-payments will enable the emerging neighbourhood market of energy and energy services.

4.2 Academic Knowledge Advancement

4.2.1 Aalto University

Foreground to be exploited: interledger, decentralized identifiers, system dynamic models of business platform network effects, decentralized marketplace.

Measures taken so far: Two PhD students are working on the SOFIE project. A graduate course "Postgraduate Seminar in Communications Engineering on Data Economics" was held in Autumn 2018 at Aalto university.

Future work: SOFIE results will be utilized in several EU- and national-level research projects, accepted projects include H2020 PHOENIX, EMPIR SmartCom, and EIT Climate-KIC GOWOOD (provisionally accepted).

Aalto will also offer master thesis topics, guest lectures, seminars, and/or special courses related to the SOFIE project. A course related to SOFIE, "Microservice architectures and serverless computing", will be held in Spring 2019.

4.2.2 Athens University of Economics and Business

Foreground to be exploited: Interledger mechanisms, design of smart contracts encoding payment and authorization policies.

Measures taken so far: One PhD student is working on topics related to SOFIE. Furthermore, two master students are working on master theses related to SOFIE, entitled "Creating a 'Store of Value' platform for cryptocurrencies" and "Interacting with Web of Things gateways using blockchains". Finally, laboratory seminars on distributed ledger technology, programming of smart contracts, and blockchain security have been offered.

Future work: AUEB will offer master thesis topics and seminars related to the SOFIE project. A graduate course on 'Blockchains and Smart Contracts' is scheduled for the Spring 2019 semester. Two additional PhD dissertations related to IoT, WoT and blockchains are expected to start during the Spring 2019 semester.

4.3 Commercial Exploitation

Commercial exploitation of SOFIE started with identifying what resources will be utilized. This includes the foreground to be exploited as well as partners' experience and networks to be used for exploitation.

4.3.1 ASM Terni SPA

Foreground to be exploited: ASM Terni is a municipal undertaking, aiming at offering specialized and public services to citizens, including water and electricity grid management through cutting-edge technologies such as a potential federation composed of different platforms connected to each other. ASM Terni as responsible for the power distribution network has the potential to offer a significant change in terms of energy availability by providing safe and secure operation and management of the Distribution Network. In this case, renewable energy has the paramount benefit to meet the local green economy.

Moreover, the knowledge acquired in SOFIE will be exploited in other projects ASM Terni is already part of, such as: NRG-5 (http://www.nrg5.eu/), eDREAM (https://edream-h2020.eu/), Defender (http://defender-project.eu/) and Phoenix that will be granted in 2019. Thanks to the exploitation of SOFIE there will be many ways to use energy and the ASM Terni Smart Grid will allow to upgrade European platforms.

What is more, ASM Terni is interested in exploiting the blockchain technology, smart micro-contracts and micro-payments, as well as in the P2P approach considering an end-to-end scenario from electricity production to distribution, storage and consumption. However, since legal barriers currently exist in Italy, the exploitation of SOFIE results will be strongly affected by the decisions of the national government.

Measures taken so far:

1. Evaluation of flexibility focusing on renewable energy production (e.g. PV arrays) and electric mobility in the city of Terni,

Future work:

- Electric Infrastructure improvement for real-time measurements,
- Block Chain installation for Smart contracts, if legally applicable, at ASM headquarters

4.3.2 Emotion SRL

Foreground to be exploited: Emotion will be part of the Italian Energy pilot providing monitoring and management services for electric vehicles and charging stations. Collaboration with the other partners of the SOFIE project for the development of the demand response campaigns based on micro contracts and micro payments and the implementation of a monitoring and management service for electric vehicles and charging stations using blockchain technology will allow Emotion to refine their skills and enrich their knowledge, allowing it to take advantage of this knowledge after the end of the project. Furthermore, Emotion will use the involvement in the SOFIE project to improve the ability of its employees and to increase the ability to provide contribution to the European projects in which it participates, such as WiseGRID (http://www.wisegrid.eu/), NRG-5 (http://www.nrg5.eu/), eDREAM (http://edream-h2020.eu/), and those to which it will participate. In addition, the acquired knowledge will be exploited to increase its business, offering to the market products and services enhanced during the project, with the aim of giving strength to electric mobility, for a cleaner mobility, allowing an increasingly massive deployment of electric vehicles and charging stations and an increasingly intense use of renewable photovoltaic energy that is mainly produced at lunchtime, when consumption is lower and when the vehicle could be parked in charge.

Measures taken so far: An EV fleet dashboard was developed and a DR campaign based on micro contract and micro payment was performed at the laboratory level.

Future work: The following actions are being planned for in relation to SOFIE:

- Improving Emotion platform of car sharing;
- Improving Emotion services by exploiting blockchain technology.

4.3.3 Engineering Ingegneria Informatica SPA

Foreground to be exploited: Engineering is involved in the Italian Energy pilot, implementing the Decentralized Marketplace that enables the demand response campaigns via smart contracts.

The results of the project, in particular the components related to the Decentralized Marketplace and the DSO forecast and congestions detection dashboard, will be exploited in several European research projects exploring the usage of distributed ledger solutions in the Energy field; moreover these technologies will be made available to the related ENG business unit.

In fact Engineering addresses the specific market with its Business unit Energy & Utility to provide its own value proposition as complete solution for its customers.

In the Engineering innovation model, the R&I activity goal is to contribute to the change in markets and companies via solutions that can create innovative experiences for the users, in order to encourage a safe and aware use of information technology. The process is composed by three macros steps:

1. Develop and consolidate the results of research projects
2. Define and execute experimental checks of developed solutions –or components- including the activity to assure the replicability of processes.
3. Capitalize the investment providing -via ENG Business Unit- Business Offer to the clients according to a specific business plan. Part of this step is the actual commercialization process, including the work of the business unit to extend the company offer portfolio and address the worldwide market with a proper marketing strategy.

Measures taken so far: Involvement of Energy & Utility Business Unit for the scenarios identification, preliminary pilot use cases design and first requirement analysis.

Future work: After the prototype realization:

- Business Unit involvement to evaluate the SOFIE platform to identify potential extensions of the company solutions offer;
- Preparation of a potential technology transfer preparatory for engineering phases to address a product.

4.3.4 LMF Ericsson

Foreground to be exploited: Ericsson is very interested in the federated approach overall, as well as the offer marketplace, distributed identifiers and interledger models that are being researched and developed in SOFIE. We have already identified opportunities to exploit these capabilities as part of Ericsson's product/concept development.

Measures taken so far: SOFIE approach for distributed identifiers has been adopted so far in one completed research project. One Master's Thesis completed in the areas of Distributed Identifiers.

Future work:

- Development of an IoT marketplace use case that builds on top of the SOFIE framework code. Our intent is to leverage on the IoT marketplace work for an internal project that we aim to be able to demonstrate at the Mobile World Congress in 2021.
- Research on transparency for centralized identity system. Centralized system including identity e.g, PKI, Remote SIM provisioning (RSP) system are centralized in nature. Recent state nation attack shows transparency for such systems are critical. SOFIE uses decentralized and immutable structure of ledger and smart contract for transparency of identity data.
- Security analysis of identity systems. Security analysis of blockchain and non-blockchain identity systems, considering e.g. PKI, Remote SIM provisioning and Ethereum name service.Research to evaluate automated device provisioning with use of blockchain.

4.3.5 Guardtime AS

Foreground to be exploited: During the first year of SOFIE, Guardtime has defined the use-cases on how data exchange between Transmission System Operators (TSO) and smart meter platforms could be handled. These use-cases can be exploited in a horizontal way to support the business case of a TSO and to protect them from legal problems when opening up the data to third parties. From a technical perspective the foreground component to be used is divided into four main pillars:

1) The authorisation and access between systems;

2) The hardware, mainly smart meters, opt in to the existing platform;

3) Data exchange and sharing;

4) Security module.

The foreground component is using the Guardtime KSI API and combining this with the SOFIE federated framework. In Addition to SOFIE’s components the methodology how to evaluate existing TSO legacy platforms is developed and will be used for future exploitation of the SOFIE federated platform.

Measures taken so far: The structure of Guardtime’s exploitation plan is divided into two main blocks: the activities related to the industry side and the work towards the EU legislation, regulatory side with organisations that group together different interest groups. Guardtime’s interest is to bring novel technologies to the market that would directly affect the challenges that Energy sector (TSOs, DSOs, flexibility service providers) have. For this purpose, there is direct connection to Guardtime’s energy sector marketing and sales force and results and exploitation plan in SOFIE. In the industry side the starting point for Guardtime, is to have synergy between our existing networks, customers and projects in Energy sector. We see that there is much benefit to use the existing customers like the TSOs (TenneT, Elering, AKKA, ESO) to discuss and evaluate the value that could be brought through the SOFIE Estonian Energy project as well as technology components described in previous section in exploitation plan. In EU and policy maker level Guardtime has approached Entso-E and attended in a couple of workshops to map the existing challenges with the tasks defined in SOFIE. Additionally, Guardtime presented the key components of the SOFIE federated framework related to using distributed ledger and KSI Blockchain combination. The results of the EU energy policy indicate that the stand-alone data hubs and legacy systems that the current TSOs and DSOs are operating cannot achieve the overall goals of reaching 50% of Renewable energy production by 2030. This is a clear indication that the technology developed in SOFIE is needed and should be supported by exploitation activities. In parallel to enabling the technology in business perspective there has also been activities related to comply with GDPR in regards to existing and new energy services. Exploitation activities so far have been to define the key points where SOFIE federated architecture could help the industry side comply with GDPR and handle personal identifiable information accordingly.

Future work: The exploitation plan is to carry on with the three main topics.

- Work related to legal and regulatory side. Both GDPR and flexible open energy market activities, with Entso-E and EU commission bodies related to Energy sector.
- The future use of Guardtime's business network in energy sector (information exchange, joint events, cross usage of sales/marketing force), thus making sure that the approach towards industry is constantly and widely targeted.
- Efforts to combine the different components, developed in SOFIE federated platform, and matching them to the legal and business-related challenges to find best steps forward for long term exploitation of the results.

4.3.6 Optimum Anonimi Etairia Technologies Pliroforikis

Foreground to be exploited: IoT service/device description, data description.

Measures taken so far: Presentation of the SOFIE business platform to partners and commercial customers to inform them about new business opportunities towards integrating end-to-end secure traceability in logistics and warehouse management.

Future work: the following actions are planned in relation to SOFIE

- Improving IoT semantics of Aberon IoT platform
- Improving Aberon services tailored to the needs of logistic chain with blockchain technology

4.3.7 Rovio Entertainment Corporation

Foreground to be exploited: Rovio leads the Mobile Gaming Pilot in the project. We aim to seek and identify where data platforms using DLTs can have significant impact in gaming industry. We will also build prototypes for leading use cases and validate game experience and business potential for DLTs and IoT in gaming.

Measures taken so far: One Blockchain research developer (PhD student) working on to identify use cases, current challenges to implement those use cases and their possible solutions. A publication is being prepared for this purpose.

A wider team is involved in prototype development. To date, we have developed one prototype to understand the use of DLTs for content ownership by players in games enabling buying and selling of in-game assets. Furthermore, system requirement and architecture of a scavenger hunt game is also being prepared which will seek to understand the potential for DLT and IoT in a gaming context.

Future work:

- Paper submission for review "SOFIE Gaming - Use Cases, Challenges and Solutions" - planned for first week of March (IEEE TrustCom '19).
- Implementation of the scavenger hunt game testing DLT and IoT gaming use case.
- Play testing and business requirement assessments for use case for the gaming pilot.Define requirements for SOFIE platform integration with the gaming pilot use cases.

4.3.8 Synelixis Solutions SA

Foreground to be exploited: Synelixis is interested in the semantics schema developed in the scope of SOFIE to support supply chain management, especially that part that matches processing of data from farming system (as it is managed by SynField IoT platform) to the other segments of the chain. Also, we are planning to evaluate SOFIE IoT Federation adaptations as an extension of our SynField platform that enhances its secure integration capabilities in Smart City applications

Measures taken so far: Within the food supply business environment, the first measure taken by Synelixis was to present SOFIE technological and business views to 7GRAPES- Pegasus (http://www.7grapes.gr/) in order to use this entity with employees and facilities in the food-chain pilot.

Future work: Future exploitation will result through main research, development and dissemination activities of SOFIE in which Synelixis is actively involved and interested. In this scope, the following priorities are planned for the next period:

- Security analysis of IoT platforms deployed in the segments of the food chain pilot.
- Evaluation and development of the semantics reference model for web services discovery and provision in the food-chain supply system.
- Investigation and determination of the social/business context (e.g. structural properties of collaboration, business routines, governance issues etc.) in which the food-chain pilot will be deployed and operate.
- Exploitation of SOFIE advances within other EU H2020 research and development projects, e.g. PHOENIX.

5. Business Models for pilots

This chapter presents the business models best suited to SOFIE's pilots, through which the generated innovation (commercially exploitable components) will be brought to the market. The Business Model Canvas approach is used to generate, present and develop the planning of exploitation through the pilots.

The Business Model Canvas (BMC) is a strategic management template for developing new or documenting existing business models. It is a visual chart with elements describing a product's value proposition, infrastructure, customers, and finances[2]. The underlying BMC is slightly adjusted to fit better for an innovation action/project.

The Business Model Canvases will present the exploitation strategy of each pilot, as well as the benefits for the stakeholders, enabling technologies and also an overview of market trends. The workflow and interaction between SOFIE work packages of Business Model Canvases are described in chapter 3.4 "Business outreach" in the updated version of deliverable 6.6.

5.1 Energy data exchange pilot (Guardtime)

The Problem

Currently, the possibility to provide next-generation energy flexibility services is limited by the lack of access to energy consumption data. People would be choosing a better deal from energy service providers, but the use of centralized data management, with complicated and high integration cost data exchange between datahubs and related systems, is preventing this from happening worldwide.

The Energy Data Exchange Pilot

The pilot furthers the liberation of energy sector data, by providing currently missing building blocks for a future where the energy service providers and consumers have more control, freedom and flexibility over their data. The pilot establishes seamless access to the data with a few clicks done by the data owner (the citizen), regardless of where the person lives or what existing energy networks are in place.

The pilot and the following exploitation activities are directed towards smart meter data operators (TSOs/DSOs). We will create a novel digital infrastructure available that will allow the targeted TSO-s/DSOs to grant access to data, track the process of who gives/receives data through their platform and creates immutable evidence for auditing and security purposes. The pilot is taking advantage of the recent cutting-edge breakthroughs in blockchain technologies, which enable to increase trust among companies and transparency in data management.

The pilot is led by Guardtime throughout the project 2018-2020. The data exchange pilot is held in close cooperation with the targeted users' groups, which will ensure the product-market-fit from the early stage of the development, allows to validate the feasibility in real-life environment, on real on-sites and thereby lay the foundation for scaling and commercial uptake.

The Pilot Objective

The Energy Data Exchange Pilot will deliver:

- Means to manage DSO/TSO datahub access to data with the data owners' consent and GDPR compliant evidence/audit trail;

[2] https://en.wikipedia.org/wiki/Business_Model_Canvas

- SOFIE adapters placement in data input and on each participant side;
- Secure authentication and control in a mobile device for each data owner;
- Dashboards for the data owner, national data hub manager and service providers' premises;
- GDPR compliant data access to pilot specific test sites.

The Exploitation Strategy

We plan to execute a two-tiered exploitation strategy:

- **Tier 1** - we approach the DSO/TSO's operating the access control of energy consumption data. We provide them with the digital infrastructure based on SOFIE adapters on an annual license fee. The solution adds value to the existing and running platforms, so DSO/TSO can make a shortcut into sharing data and skip the planning/development phase on their existing platform.
- **Tier 2** - we aim to get service providers to start using SOFIE solution to be able to get data and sell flexibility services. Also providing evidence to DSO/TSO as well as regulators and other supervisory boards in the energy network is delivered to the service providers. The business model with service providers is sharing a revenue stream based on the new customer base that they get by new data access through the digital infrastructure.

Key markets to be targeted - we have mapped the key customer segments based on our value proposition and the target market selection is done in parallel with smart grid infrastructure development. The exploitation, and market entry strategy will focus on mature countries where smart meters and national/regional data hubs are in place (Denmark, Norway, Finland, the Netherlands etc.)

Potential customer segment - smart meter datahub managers, the industry responsible for energy data consumption/production distribution, energy flexibility service providers.

Strategic exploitation stakeholders - energy sector regulators, GSPR related data protection agencies.

Benefits for targeted end-users

- Traceability of products and ensuring the integrity of critical data without the need for centralized authority;
- Reducing the chances of fraud and data manipulation, cutting out corresponding mediation expenses and transaction costs;
- Transparent data adaptation layer for IoT platforms and easy to deploy solution to federate heterogeneous IoT environments;
- Immutable blockchain-backed energy consumption readings which are correct beyond dispute;
- Provenance chain throughout the whole infrastructure.

Enabling technologies

- Guardtime's KSI Blockchain® API provides technology for massive scale integrity verification and immutable audit trail generation;
- Hyperledger Indy-based decentralised identifiers provide a mechanism to link the data owners and service providers together (automated matchmaking functionality) and create a novel trusted way to authorize the access of data between the parties;

Market Trends

- There is an industry-wide agreement to make the make energy consumption, as well as production data available and more usable. This has been also agreed in the Clean energy package. There is an organic demand and expanding the market need for technical solutions which make this industry disruptive trend possible.

- SOFIE adapters to collect energy consumption data

Pilot outputs

- The solution validated with key stakeholders;
- The technology demonstrated in relevant environment (TRL-6);
- The pilot will set us ready for engaging business stakeholders and start with exploitation activities;
- The primary input for detailed business strategy formulation.

5.2 Energy Flexibility pilot (Engineering)

The Problem

Following the advent of distributed electricity generation, the electric grid underwent an impressive change in power flows. The grid was designed with an assumption that energy had a unidirectional power flow, but today we have many renewable generation sources (solar and wind), distributed in the network and, sometimes the energy produced is higher than the energy consumed by the end users present in the same local network. The reversed power flow causes stability and safety problems in the electricity grid, which the DSO has to solve to guarantee the continuity of the energy service. To understand the complexity of this phenomenon, we must consider that it is generated mainly by intermittent and non-programmable generation plants, strongly influenced by atmospheric conditions, making it very difficult to predict its progression.

The Energy Flexibility Marketplace Pilot

Thanks to the network equipped with devices that allow remote monitoring and management in real time, is possible to obtain useful information to obtain accurate forecasts and avoid the emerging of reverse power flow. Thanks to the SOFIE project, we want to use blockchain technology and, smart contracts to enable a secure and transparent mechanism to time-shift the end users' consumption according to the needs of the network (Demand-Response) involving the DSO, which needs energy flexibility, the EV Fleet Managers, which provide energy flexibility by directing the electric vehicles in the areas of interest to charge and, finally, the Energy Retailers, which supply electricity.

The Pilot Objective

The goal is to build a new decentralized, fair, transparent, and secure marketplace powered by the blockchain in which market operators can be sure that the best offers will be selected without any kind of bias, and, by interfacing directly with the smart meters on the grid, the payments can be settled in near real time, without the need for longer verification times.

The Exploitation Strategy

Different paths will be followed for the exploitation strategy. As for the DSO point of view, flexibility can be used for obtaining technical data. As for the Fleet Manager point of view, SOFIE outcomes could be exploited to improve electric mobility services, achieving money savings and reduced environmental impact: the use of energy produced from renewable sources for electric mobility entails a double benefit, on the one hand harmful emissions are removed from the places where vehicles circulate, making the streets healthier, on the other hand, avoiding to produce such energy from fossil fuel power plants, dangerous emissions that contribute to sickening our planet are not released.

We aim to get service providers to start using SOFIE platform to be able to get data and sell flexibility services. Also providing evidence to DSO/TSO as well as regulators and other supervisory boards in the energy network is delivered to the service providers. The business model with service providers is sharing a revenue stream based on the new customer base that they get by new data access through the digital infrastructure.

Key markets to be targeted - we have mapped the key customer segments based on our value proposition and the target market selection is done in parallel with smart grid infrastructure development.

Potential customer segment - smart meter datahub managers, the industry responsible for energy data consumption/production distribution, energy flexibility service providers.

Strategic exploitation stakeholders - energy sector regulators, GDPR related data protection agencies.

Benefits for targeted end-users and stakeholders

- Use real time and historical data to forecast the occurrence of reverse power flow
- Create flexibility requests on the marketplace to balance the local energy supply
- Help to recharge the batteries of its fleet of electric vehicles at advantageous price.
- The incentive provided by the DSO can cover part of the electrical supply
- Thanks to the marketplace, the most convenient energy retailer can be selected any time a recharge is needed
- Provides a rapid user-friendly mechanism to negotiate micro-contracts
- Grants security, transparency and auditability of the operations.
- Enable the interoperability among different siloed IoT systems.

Enabling technologies

- SOFIE decentralized blockchain-based marketplace
- SOFIE adapters to collect data from DSO’s smart meters and fleet managers’ EVs and EVSEs

Market Trends

- There is an industry-wide agreement to make the make energy consumption, as well as production data available and more usable. This has been also agreed in the Clean energy package. There is an organic demand and expanding the market need for technical solutions which make this industry disruptive trend possible.
- Increase of distributed generation from renewable sources (solar and wind)

Pilot outputs

- The solution designed and validated with key stakeholders;
- The solution deployed in an operational environment (TRL-6);
- The solution replicable and scalable in any microgrid.

5.3 Food Supply Chain pilot (Synelixis)

The Problem

Producers, distributors, logistics and retailers want to get their products to the market quickly, safely, and in the best possible condition. Consumers want to buy high-quality products and know how these were produced, where they came from and what is their ingredients. They also have increased expectations about the environmental sustainability or health-related issues in the production cycle, not rarely preferring brands which promote the same social and environmental values as their own.

The Food Supply Chain Pilot

The food supply chain (FSC) pilot considers the field-to-fork grapes supply chain system covering the farming, storage, distribution (logistics), and retail subdomains, and serves as a proof-of-concept for the validation and demonstration of the capabilities of the SOFIE platform to combine and interconnect, in a secure way, different IoT platforms that are involved in the food supply chain sector.

The pilot demonstrates a provenance chain Business Platform (BP) to ensure wide visibility of supply chain information, traceability of assets, and secure data exchange among heterogeneous, federated IoT environments, without forcing additional changes to their infrastructures, equipment and security policies. The pilot leverages a hierarchical topology of DLTs to improve transparency and traceability of assets and build a robust and secure data management framework that verifies integrity of exchanged data and ensures identity and authenticity control of involved entities.

The pilot is organized by Synelixis and Optimum with strong involvement of 7Grapes product association which as end-user and early adopter participates in the definition of end-user requirements and the evaluation of pilot services. On-site testing and demonstration activities are taking place in Kiato area, Greece, mainly during grapes harvesting periods.

The Pilot Objective

The objective is to demonstrate a provenance chain BP that secures information sharing and value exchange between organizations which participate in the food supply chain without the need of a third-party intermediary to establish trust, coordinate interaction and supervise products flow over the chain. The BP will provide end-to-end product traceability services to all involved companies as well as food consumers.

The Exploitation Strategy

FSC traceability services could be released as a mixed Platform as a Service (PaaS) and Software as a Service (SaaS) model. This model will maximize the scalability and flexibility of the platform allowing customers to access more or fewer services or features on-demand. Different releases of the platform and provided services could be possible:

- Open platform access with limited functionality and service provision on top of a basic schema to adapt existing IoT services and systems.
- Full platform access and customizable services with provision of federation adapters for existing IoT systems.

The commercial usage of the pilot platform and its services could combine a double revenue model: On the one hand, the companies which participate in the supply chain could pay a periodical fee (subscription model) to get federation adapters for their IoT platforms and share data through the SOFIE FSC platform. This is applicable to all identified chain segments (e.g.

producers, logistics, etc.), under the appropriate adaptations tailored to the specific interests and activities per domain. On the other hand, retailers and/or customers which want secure traceability information and food safety assurance could pay directly a small amount per SOFIE-traceable product purchase.

Potential customer segments - suppliers in agri-food domain, logistics and transportation companies.

Strategic exploitation stakeholders - retailers, supermarkets, consumers associations.

Benefits for targeted end-users and stakeholders

For suppliers:

- secure information sharing without the need of a centralized authority to supervise and control data exchange,
- easy to use and non-disruptive solution to federate local IoT business environments,
- verify goods ownership and authenticity, as well as on-time and in-full transactions and deliveries,
- cut out mediation expenses, reduce transaction costs and improve quality management of products distribution

For retailers:

- increase visibility in goods transfer from the field to the market shelf,
- improve efficiency in audits and disputes resolution when quality conditions are not met,
- enable immediate identification and recall of potential contaminated goods in cases where product quality and/or safety events are detected

For food consumers:

- increase consumers' visibility about goods production, transportation and processing practices over the whole food supply chain.

Enabling technologies

- DLT-based identity authentication and role-based control management.
- SOFIE adapters to enable a common interface specification upon federation of heterogeneous IoT systems.
- SOFIE interledger protocol to bridge different DLTs.

Market Trends

- Immutable, real-time keeping of transactions among supply chain companies improves product and inventory mgmt., minimizes errors in their communication and increases trust among them.
- Companies want to protect their brands and product labels against negative publicity, potential frauds and counterfeits as well as to highlight their sustainable supply chain and market practices.
- Customers and customer associations push for extended visibility and traceability of products' history to ensure high standards for their quality and safety.

Pilot outputs

- A validated platform with key stakeholders that offers two main services: i) secure product traceability for final customers, and ii) audit process allowing supply chain companies to detect product quality issues.
- The solution deployed in an operational environment (TRL-6).

5.4 Mobile gaming pilot (Rovio)

The Problem

New location-based mobile games require access to infrastructure in order to be attractive and to offer new exciting gaming experiences. There is a high cost to invest into new sensors, thus making it more reasonable to use existing devices and sensors while developing new location-based games. In this process, involving the stakeholders of IoT devices is challenging. The hurdle how to motivate them to be a part of the game and get the fair share of the money coming in from the game and cover the costs of integration and implementation, needs to be tackled. There is a need for new solutions and tools to cope with these obstacles.

From technical perspective we are solving these two problems:

- Could the existing base of fixed-location IoT devices also be used for location-based mobile gaming?
- Could DLT bring benefits to players or other stakeholders in mobile gaming?

The Context-aware Mobile Gaming Pilot

We identify and test use cases of DLT and IoT in mobile gaming in an iterative fashion. We are not working on a commercial product but experimenting with new technologies.

The Pilot Objective

Through tests and calculations, we evaluate the technical fit, performance, and business potential of the use cases that we identify. At the end of this project we will have a clearer answer of whether we should pursue DLT/IoT in gaming commercially or not.

The Exploitation Strategy

We have a working architecture, and we receive feedback and insight from dissemination activities and contacts from the game industry. We don't want to limit our target audience to blockchain enthusiasts but are keen on discovering whether these technologies do not stand in the way of sustaining a game with one million daily active users and means of generating more than $100k revenue, while bringing benefits to consumers and/or other stakeholders.

Benefits for targeted end-users and stakeholders

- By using ephemeral identifiers, beacons can be harder to spoof than GPS. Player locations can be verified, reducing the number of cheaters in competitive games.
- Indoor positions, especially altitude information, can be more accurate
- DLTs can bring transparency and automation to companies participating in an ecosystem for location-based games

Market Trends

- The global number of fixed-location IoT devices is increasing.

Enabling technologies

- In the prototype we’re using Hyperledger Fabric for a permissioned blockchain, but we’re not locking into it.
- Bluetooth low-energy beacons

Pilot outputs

- Results from testing the technical fit and performance of DLT and IoT technologies in mobile gaming. Learning which benefits of DLT outweigh the technology’s shortcomings, and which functionalities are better left off on a traditional game server.

A non-commercial scavenger hunt game prototype: an example of a real location-based game that uses beacons for positioning.

In conclusion, during the first exploitation year in the project, exploitable components were identified, and a basic workflow was planned and executed accordingly. This resulted in four Business Model Canvases that remain to be actively updated in relation to the planned communication and dissemination activities, as well as development and testing advancements, that are running in parallel throughout the project.

5.5 Intellectual Property Rights

IPR & future exploitation of results is treated according principles agreed in the Consortium Agreement.

SOFIE open source framework components are released under the Apache License Version 2.0. Licensing of pilot components is up to the pilots. Terms of licensing will be agreed between the owner of the IPR (e.g. pilot lead) and the potential user. This means that IPRs are owned by the consortium partners that generate them. Most of the results of the SOFIE project, such as the SOFIE federation framework, will be released under open source license and/or described in scientific publications, allowing also other parties to utilize and exploit them.

6. Conclusion

We foresee that the communication and exploitation activities advance and grow as the project evolves. The SOFIE project has already made some good progress in the first year.

In communication all the necessary materials have been completed, the website has been built and updated. The project has set up social networks and is actively using Twitter. We also have been actively building liaisons with other projects as well as exhibiting at conferences.

As for dissemination, two open-source codes were released in the end of 2018 and the codes are publicly downloadable at GitHub. During the first 13 months of the project already 6 papers have been published. SOFIE is also participating in the Horizon 2020 Pilot on Open Research Data and the data related to publications and deliverables has been made available via the project’s website.

In the area of exploitation, the academic partners have already been providing education related to the SOFIE project and the industrial partners are taking first steps towards commercial exploitation.