# ISO/IEC TR 30176

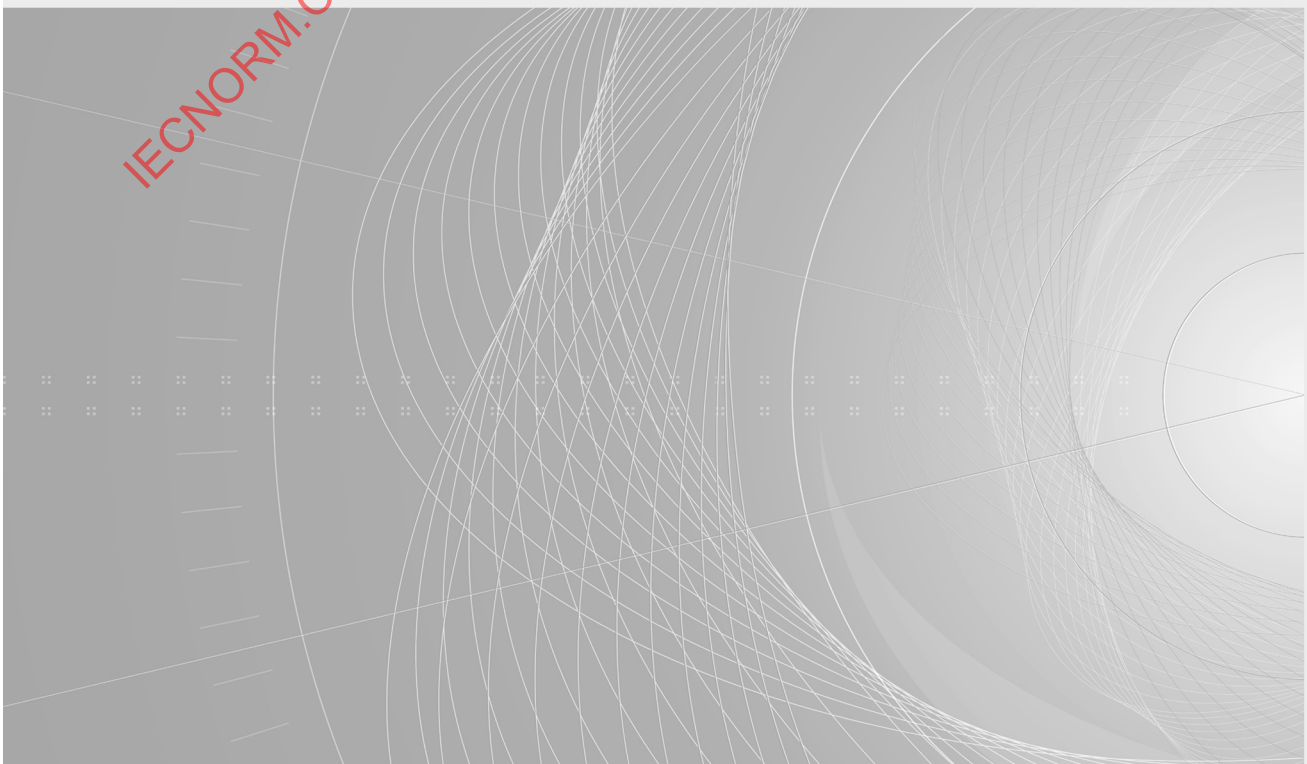
Edition 1.0 2021-11

# TECHNICAL REPORT

colour inside

## Internet of things (IoT) – Integration of IoT and DLT/blockchain: Use cases





ISO/IEC TR 30176:2021-11(en)

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

**About the IEC**
The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

**About IEC publications**
The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigendum or an amendment might have been published.

**IEC publications search - webstore.iec.ch/advsearchform**
The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee, …). It also gives information on projects, replaced and withdrawn publications.

**IEC Just Published - webstore.iec.ch/justpublished**
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

**IEC Customer Service Centre - webstore.iec.ch/csc**
If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: sales@iec.ch.

**IEC online collection - oc.iec.ch**
Discover our powerful search engine and read freely all the publications previews. With a subscription you will always have access to up to date content tailored to your needs.

**Electropedia - www.electropedia.org**
The world's leading online dictionary on electrotechnology, containing more than 22 000 terminological entries in English and French, with equivalent terms in 18 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

# ISO/IEC TR 30176

Edition 1.0 2021-11

# TECHNICAL REPORT





## Internet of things (IoT) – Integration of IoT and DLT/blockchain: Use cases

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 33.020

ISBN 978-2-8322-1037-5

# CONTENTS

# INTERNET OF THINGS (IoT) – INTEGRATION OF IoT AND DLT/BLOCKCHAIN: USE CASES

## FOREWORD

1) ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.
2) The formal decisions or agreements of IEC and ISO on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC and ISO National bodies.
3) IEC and ISO documents have the form of recommendations for international use and are accepted by IEC and ISO National bodies in that sense. While all reasonable efforts are made to ensure that the technical content of IEC and ISO documents is accurate, IEC and ISO cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC and ISO National bodies undertake to apply IEC and ISO documents transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC and ISO document and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC and ISO do not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC and ISO marks of conformity. IEC and ISO are not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this document.
7) No liability shall attach to IEC and ISO or their directors, employees, servants or agents including individual experts and members of its technical committees and IEC and ISO National bodies for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this ISO/IEC document or any other IEC and ISO documents.
8) Attention is drawn to the Normative references cited in this document. Use of the referenced publications is indispensable for the correct application of this document.
9) Attention is drawn to the possibility that some of the elements of this ISO/IEC document may be the subject of patent rights. IEC and ISO shall not be held responsible for identifying any or all such patent rights.

IEC TR 30176 has been prepared by subcommittee 41: Internet of Things and Digital Twin, of ISO/IEC joint technical committee 1: Information technology. It is a Technical Report.

The text of this Technical Report is based on the following documents:

| Draft | Report on voting |
|---|---|
| JTC1-SC41/220A/DTR | JTC1-SC41/241A/RVDTR |

Full information on the voting for its approval can be found in the report on voting indicated in the above table.

The language used for the development of this Technical Report is English.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1, available at www.iec.ch/members_experts/refdocs and www.iso.org/directives.

**IMPORTANT – The "colour inside" logo on the cover page of this document indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.**

# INTRODUCTION

Distributed ledger technology (DLT) provides the capability of a distributed ledger, which is shared across a set of DLT nodes and synchronized among DLT nodes using a consensus mechanism. Blockchain is a kind of DLT, which uses confirmed blocks organized in an append-only, sequential chain using cryptographic links. Blockchain is designed to be tamper resistant and to create final, definitive and immutable ledger records. Either DLT or blockchain can be quoted and used in terms of technology realization for application scenarios. Each participant in a blockchain and DLT network has their own tamper-resistant replica of transaction records associated with the participants who are individuals or organizations. Blockchain and DLT can be applied to solutions involving IoT systems which contain sensors, actuators, tags and readers, wearable devices, and service platforms, all of which are networked.

Through the analysis of the IoT involving the DLT and blockchain technology, the DLT and blockchain technology can help in solving the problems of IoT, especially those existing in the physical system, such as device digital identity, data source trustworthiness, key data forensics, data rights and interests, data assets and value exchange, etc. At the same time, the IoT also provides an important commercial application scenario for DLT and blockchain, and promotes entity and virtual economy combination. The integration of the IoT system with the DLT and blockchain technology can achieve complementary advantages and bring new business opportunities.

In fact, the integration of IoT system with DLT and blockchain can enable the creation of better solutions for many business sectors, particularly where those solutions involve information associated with physical entities, and where the solution spans many organizations with the need for trusted information to be shared by those organizations.

The solutions that can be provided by the integration are important for the business sectors such as agriculture, industry, healthcare, pharmaceuticals, environmental protection, transportation, security, finance, insurance, object tracing, supply chain, smart grid, and smart cities. This document is focused on collecting use cases in some of these sectors.

This document has been prepared based on the applications of IoT and DLT/blockchain technology with the template of IoT use cases.

# INTERNET OF THINGS (IoT) – INTEGRATION OF IoT AND DLT/BLOCKCHAIN: USE CASES

## 1 Scope

This document identifies and collects use cases for the integration of the DLT/blockchain within IoT systems, applications, and/or services.

The use cases presented in this document use the IoT use case template.

## 2 Normative references

There are no normative references in this document.

## 3 Terms and definitions

No terms and definitions are listed in this document.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at http://www.electropedia.org/
- ISO Online browsing platform: available at http://www.iso.org/obp

## 4 Symbols and abbreviated terms

APP application
DLT distributed ledger technology
HMI human–machine interface

## 5 Use case scenarios

### 5.1 General

Use cases presented in this document depict typical use cases involving blockchain/DLT and IoT systems, applications, and/or services; however, this document is not intended to be an exhaustive list of all realizations.

### 5.2 Use cases

Table 1 summarizes the use case scenarios in this document along with the key actors in each scenario.

**Table 1 – Summary of use case scenarios**

| Use case number | Name of use case scenario | Short description | Actors |
|---|---|---|---|
| 1 | Agricultural product tracing | The agricultural product tracing provides the digital capability of recording and tracing the entire process of the agricultural product, from sowing, cultivating and growing, harvesting, storage, transportation, and so on, to the end users. All the data associated with the entire process are collected and stored by the IoT and blockchain technologies to protect from and prevent any tampering of the data, which ensures the brand name, quality, and more importantly the tracing of the agricultural products. | Various sensor nodes, IoT gateways, agricultural product monitoring platform, APP, product testing agency, sellers, logistics service provider, and agricultural product consumers. |
| 2 | Financial services for fish farming | Financial services, such as insurance services and loans, are provided to fish farmers by collaboration between financial institutions and high-tech companies. The business collaboration model initiates the innovative way of financial services for fish farming, which is enabled by the IoT and blockchain technology. | Sensor nodes for fish farm monitoring, oxygen controllers, IoT gateways, aquaculture monitoring platform with blockchain, APP, financial service portal, banks, insurance companies, fish farmers. |
| 3 | Chattel mortgage services | This use case describes how to integrate IoT system with authorized device and platform integrated with blockchain to monitor the real-time status of chattel asset in the warehouse and during transportation, and provide the authorized data to the relevant stakeholders such as banks, chattel asset owners, chattel asset monitoring organizations, etc., so as to prevent fraudulent activities and reduce unnecessary high risks in providing chattel mortgage services. | Sensor nodes for the chattel asset monitoring, IoT gateway, chattel mortgage monitoring platform with blockchain, APP, financial service portal, banks. |
| 4 | Distributed energy trading | A blockchain-based trading infrastructure offers a distributed platform that enables peer-to-peer trading of energy between consumers and prosumers in a secure manner. The identity privacy and security of transaction is higher in the distributed platform compared to the traditional system, in which the energy transaction is usually performed through the central platform which is vulnerable to security threats. | Smart meter, aggregator (EAG) with blockchain, wallet, energy seller, energy buyer. |
| 5 | Automated parking payment service | Automated parking payment is a new way for users to pay a parking toll without manual payment and without use of a smart phone. This use case will give the main idea of what the seamless payment is and how to realize the seamless parking payment by automatically calculating and paying parking fees. The entire process is automatically realized by authorized devices, platform integrated with blockchain, wallet, and smart contracts. | Smart devices for the parking vehicles, IoT gateway, parking management platform with blockchain, wallet, parking manager, parking user. |

# 6 Description of use case

## 6.1 Agricultural product tracing

### 6.1.1 Scope and objectives of use case

The main scope of this use case includes:

- the advantages gained over the traditional agricultural product when the IoT and blockchain technologies are applied; and
- how the IoT and blockchain technologies are used in the agricultural product's tracing system.

The objectives of this use case are to:

- clarify the requirements for tracing the agricultural products;
- provide the general descriptions of an IoT system integrated with blockchain technology; and
- improve the online functionality, the end-to-end processes, and the reliability of the management of agricultural products.

### 6.1.2 Narrative of use case

#### 6.1.2.1 Short description

The agricultural product tracing provides the digital capability of recording and tracing the entire process of the agricultural product, from sowing, cultivating and growing, harvesting, storage, transportation, and so on, to the end users. All the data associated with the entire process are collected and stored by the IoT and blockchain technologies to protect from and prevent any tampering of the data, which ensures the brand name, quality, and more importantly the tracing of the agricultural products.

#### 6.1.2.2 Complete description

The agricultural product tracing lowers food safety risks and protects the reputation of the agricultural product's brand name and quality. A service for securely tracing the entire end-to-end process can be provided by an IoT system integrated with the blockchain technology. The IoT system is used to collect the data from the entire process, i.e. from sowing in the farmland to the consumer market, and the collected data can be stored in the blockchain preventing any potential data tampering.

Various types of sensor nodes can be deployed to measure and collect data on seed conditions, soil quality, lighting condition, weather, crop height, etc. in the agricultural product growth environment. Additionally, other types of sensor nodes can also be deployed to provide location and image/video (cameras) to collect key data on the growth, fertilization, watering, and harvesting time.

The data are transmitted automatically at the scheduled time intervals (e.g. sampling rates) to the agricultural product service platform, encrypted, and recorded in the blockchain along with the time stamp. The encryption key pairs are generated based on the ID of sensor nodes or devices.

After harvesting the agricultural products, the data from the harvested product, e.g. pick-up time, weight of the package, product code of the agricultural products, are uploaded to the agricultural product monitoring platform and stored in blockchain. When the product's test reports from a testing agency are available, the test reports are also stored in blockchain along with the data. The information provided by the logistics service providers, such as product packing information and transportation condition, can also be recorded in the blockchain.

Meanwhile, all the participants in the entire end-to-end process are authenticated and their information is stored in the blockchain. Furthermore, the consumers will be able to trace all the data by the product codes from the product monitoring platform, providing the transparency between those who are in the entire end-to-end process and the consumers and also ensuring the product quality and reputation of the producer's brand.

### 6.1.3 Actors: people, components, systems, integrated systems, applications and organizations

Table 2 shows various actors involved in the agricultural product tracing. It also provides the description of each actor and its interactions with physical and virtual entities or other actors.

**Table 2 – Actors for agricultural product tracing**

| Actor Name | Actor role | Actor description | Actor interactions (transactions between actors) |
|---|---|---|---|
| Sensor nodes | IoT devices for monitoring the crop growth | Various devices which acquire the data/information relevant to the crop growth, such as soil nutrition, water, light, temperature, humidity, etc. | IoT gateway |
| Tags | Physical entities | Physical entities that are attached to other physical entities providing information of the physical entities. | Tag readers |
| Tag readers | IoT devices | Devices read the associated information from the tags, such as the product code and entire process data of the agricultural products. | IoT gateway |
| IoT gateway | IoT gateway | A device which communicates with the sensor nodes in the proximity network and aggregates the data/information from the sensor nodes, and transmits the aggregated data/information to the agricultural product monitoring platform by which it is authenticated first. | Sensor nodes and the agricultural product monitoring platform |
| Agricultural product monitoring platform with blockchain | Application and service sub-system | A platform to provide the monitoring and tracing services of the agricultural products, supported by blockchain where the product data is stored. The smart contract on the product code within the validity period or on other transaction is operated in this platform involved with the participants. | IoT gateways, APP, agricultural product testing agencies, and logistics service providers |
| APP | IoT user / digital user | An application software through the human–machine interface (HMI) for the users to access the service of the agricultural product monitoring platform. | Agricultural product monitoring platform |
| Product testing agency | IoT user / human user | An organization qualified to test and certify the quality of the agricultural product and publish the test results to the agricultural product monitoring platform to be stored in the blockchain. | Agricultural product monitoring platform |
| Logistics service provider | IoT user / human user | A service organization that provides the logistics service and ensures the appropriate transportation conditions for agricultural products, and publishes the logistical information to the agricultural product monitoring platform to be stored in the blockchain. | Agricultural product monitoring platform |
| Sellers | IoT user / human user | Participants who sell the agricultural products to the consumers. | APP |
| Agricultural product consumers | IoT user / human user | Individuals who trace the agricultural product quality, buy, and consume the agricultural products. | APP |

### 6.1.4 Issues: legal contracts, legal regulations, and constraints

Individuals, organizations, companies or institutions will comply with the legal contract's terms and conditions, legal regulations and constraints in international, national, regional, or local area relating to the information security of agricultural product data from planting, testing, packing, to transportation, and relating to the personal privacy of the participants.

### 6.1.5 Reference standards and/or standardization committees

None.

### 6.1.6 Relation with other known use cases

None.

### 6.1.7 General remarks

None.

### 6.1.8 Data security, privacy and trustworthiness

Table 3 describes the security, privacy and trustworthiness associated with the data and information collected and stored in the agricultural product monitoring platform.

**Table 3 – Data security, privacy and trustworthiness for agricultural product tracing**

| **Data security requirements and implications for applications, systems, etc.** |
|---|
| The data security requirements are essential for the service providers, participants and users. For example, the data from the agricultural product has not been tampered with, and the data are encrypted and stored in a distributed fashion. All participants who publish their data/information to the agricultural product monitoring platform are authenticated. |
| **Privacy requirements and implications for applications, systems, etc.** |
| The privacy requirements are important for every stakeholder, participant, and user. The data/information of stakeholders, participants and users are not obtained by unauthenticated users. Encryption or technologies with anonymous characteristics can be used to protect the data/information privacy. |
| **Trustworthiness requirements and implications for applications, systems, etc.** |
| The trustworthiness requirements for the agricultural product tracing are fundamental and essential. The agricultural product monitoring platform provides reliable and tamper-proof product data and information to the users. More importantly, the participants providing their data/information are the only ones who can be trusted and authenticated. |



### 6.1.9 Conformity aspects

None.

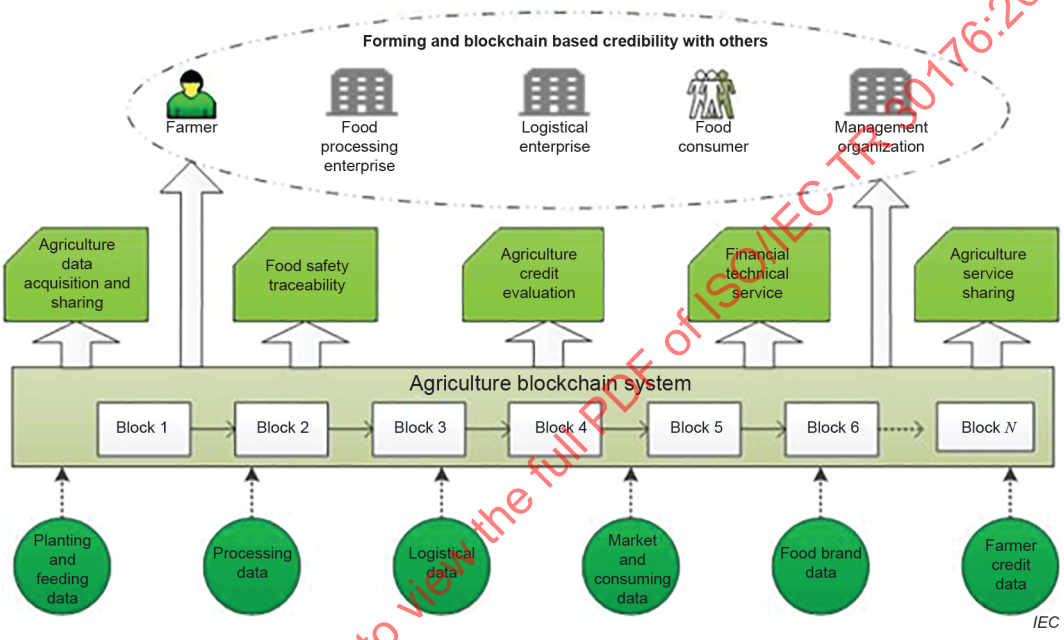
### 6.1.10 User requirements and interactions with other actors

The users request and obtain the entire end-to-end process data of agricultural products provided by the service providers, such as sowing crops, growing process, harvesting, testing, storage, logistics, and sales.

The participants are authenticated by third parties to ensure that their identities are credible, and then the data of the agricultural products is provided by the authenticated participants, for example, farm managers, testing agencies, logistics service providers and sellers. The agricultural products have their own identifiers associated with the data provided by the participants.

### 6.1.11 Drawing of use case

Figure 1 describes the use case of smart agriculture with an IoT system and blockchain technology. Agricultural product tracing is an essential part of the smart agriculture. The IoT systems and other third-party systems collect the data on planting, processing, logistics, marketing, food brand, and the participant's credit data. The third parties are also authenticated to access the system. All the data associated with the products are stored in the blockchain integrated in the agricultural product monitoring platform. The monitoring platform integrates the data from all the participants and provides the data sharing, food safety tracing, credit evaluation, and other financial services for various users. For example, the consumers can get a food safety tracing service, and a management organization can get shared data service. Blockchain helps to construct a peer-to-peer platform for the users and participants.




SOURCE: Figure 2 of Study report of JTC 1 /SC 41 AHG 18 [SC41N1089]

**Figure 1 – General overview of smart agriculture**

### 6.1.12 Data flow diagram of use case

The agricultural product tracing use case includes the following types of data flows:

1) Agricultural product data flow generated by IoT system and participants

   The agricultural product data are stored in the platform supported by blockchain. For example, the data associated with the operations for the product include the operation result, the participants and the time stamp. The data associated with testing include test reports, testing agency, and time stamp.

   The IoT systems collect the data associated with the agricultural product's growing, storage, logistics, and sales. For example, the data associated with the crop growing include temperature, humidity, the PH value of the soil, and pictures of the product appearance.

   Other participants provide their process data to agricultural product monitoring platform. For example, the testing agency provides the testing service for the agricultural products and generates the test reports.

All end-to-end process data of the agricultural product are collected, transferred and stored in blockchain to ensure that the data recorded and traced are tamper-proof. When the agricultural products are packed in boxes for transportation, the agricultural product monitoring platform associates a unique product code for each box with the entire process data, and the tag with the product code is affixed on each box.

If the products are expired due to passing the expiration date, the smart contract implemented in blockchain will either delete the product codes or enter a code for the expired product. No product code or an expired product code will remind the consumers of any products that are out of date. The product code is deleted when the product is sold out. The product code can't be reused for other agricultural products.

2) Identification data flow for the participants

The participants have their own identifications, and each participant has a unique and private encryption and decryption key pair for accessing the blockchain in the monitoring platform to ensure the authenticated access to the blockchain. The participants use their unique private key to write the records or operations relevant to the agricultural product in the blockchain.

3) Inquiry data flow for the consumers and participants

The consumers and participants can request, check and trace the agricultural products using the tracing service by the product code. The participants include logistics service providers, storage managers, sellers, etc.

The data flow diagram for the use case of agricultural product traceabiltiy is shown in Figure 2.

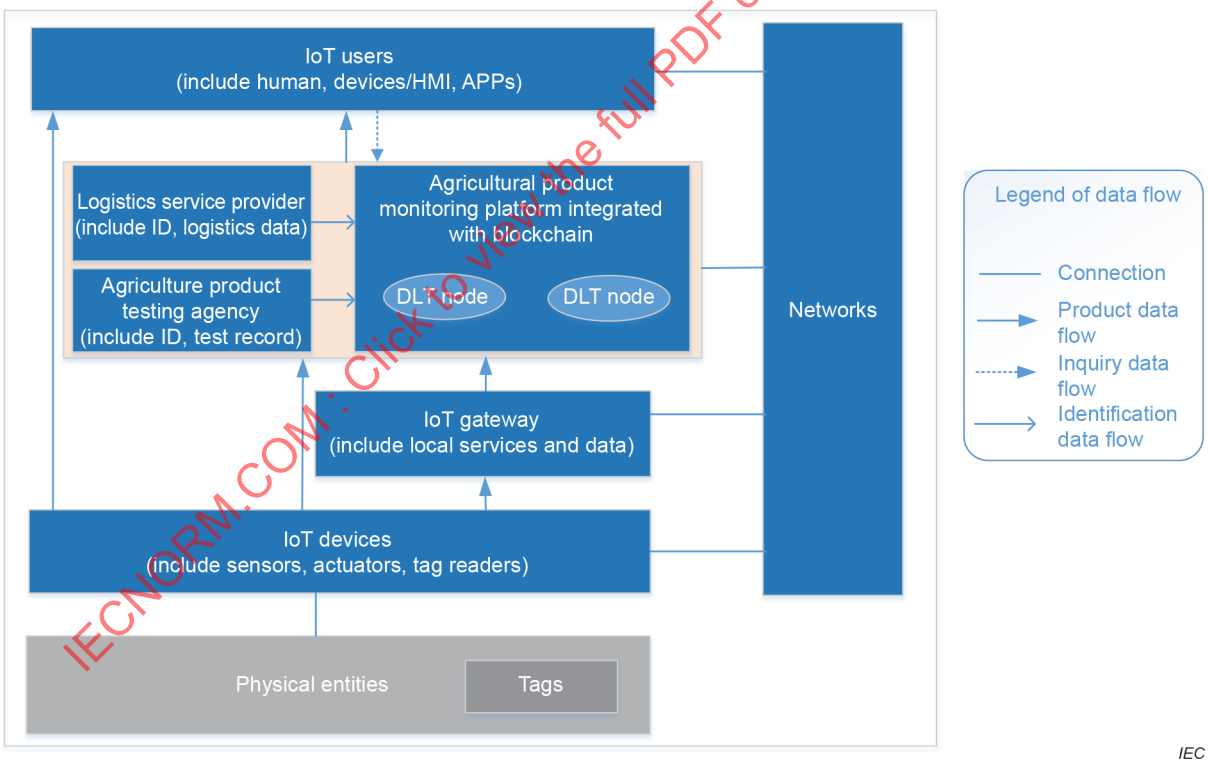



**Figure 2 – Data flow diagram of agricultural product tracing**

### 6.1.13 Sequence diagram of use case

The sequence diagram shown in Figure 3 describes the steps to set up the interactions for all the actors in the IoT system integrated with blockchain. Table 4 provides additional details of the steps shown in Figure 3.

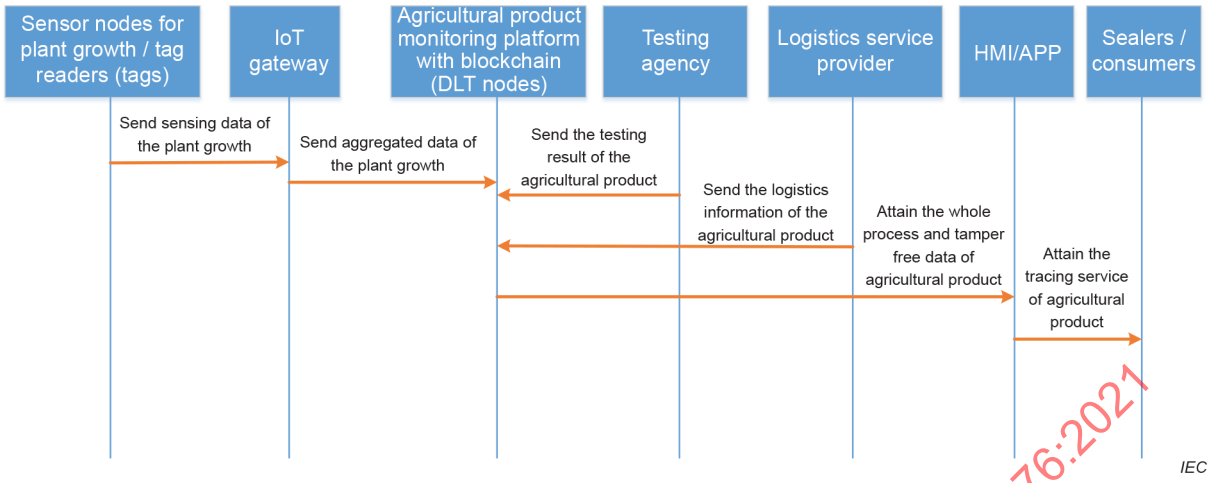



**Figure 3 – Sequence diagram of agricultural product tracing**

**Table 4 – Steps of the agricultural product tracing**

| Scenario | | | | |
|---|---|---|---|---|
| **Scenario name:** | Realizing both the tracing services of the whole process and the generation of the tamper-free data for the agricultural products | | | |
| **Step No.** | **Event** | **Information producer (actor)** | **Information receiver (actor)** | **Information exchanged (IDs)** |
| 1 | Get the original sensing data and whole procedure data of the agricultural products | Sensor nodes / Tag readers (Tags) | IoT gateway | Sensing data of the plant growth and the whole procedure data of the agricultural products |
| 2 | Send the aggregated data | IoT gateway | Agricultural product monitoring platform with blockchain | Aggregated data of the agricultural products |
| 3 | Send the test results of the agricultural products | Testing agency | Agricultural product monitoring platform with blockchain | The test data and result of agricultural products |
| 4 | Send the logistics information of the agricultural products | Logistics service provider | Agricultural product monitoring platform with blockchain | The logistics information of the agricultural products |
| 5 | Attain the whole process and tamper-proof data of agricultural products | Agricultural product monitoring platform with blockchain | HMI / APP | The entire process and tamper-proof data of agricultural products |
| 6 | Attain the tracing service of agricultural products | HMI / APP | Sellers or consumers | The tracing service of agricultural products, such as seeding to growth, the logistics, testing results, etc. |



## 6.2 Financial services for fish farming

### 6.2.1 Scope and objectives of use case

This use case describes how financial institutions (e.g. banks) and IoT service companies for fish farming collaborate to provide fish farmers with financial services. An IoT service company for fish farming is a high-tech company providing the aquaculture service with the IoT system and blockchain technology.

The objective of this use case is to analyse a business collaboration model of the IoT service companies for fish farming, insurance institutions, and banks to provide the financial services to fish farmers, and also to explore potential markets for financial services.

### 6.2.2 Narrative of use case

#### 6.2.2.1 Short description

Financial services, such as insurance services and loans, are provided to fish farmers by collaboration between financial institutions and high-tech companies. The business collaboration model initiates the innovative way of financial services for fish farming, which is enabled by the IoT and blockchain technology.

#### 6.2.2.2 Complete description

1) In the traditional way, fish farmers can't easily get financial services in some regions.

   Banks and insurance companies need to control the risks. The banks in some regions are unwilling to provide financial services to fish farmers because they can't provide sufficient assets (i.e. collateral) and lack historical financial records (i.e. credentials) to demonstrate their ability to repay their loans.

   Insurance companies are also unwilling to insure fish farmers because evaluating and ascertaining the value of the potential future loss is difficult, and the reasons for the loss can be unclear, if and when the fish die unexpectedly.

   Thus, fish farmers bear all the risks and losses caused by natural disasters, water-borne diseases, and market price fluctuations.

2) With collaboration between the financial institutions and IoT service companies for fish farming, the high-tech and services allow the fish farmers to obtain the loans and insurance for their fish farms.

   The IoT service company for fish farming collects the aquatic data of the fish farm, data on fish farmer's production and operations upon the approval by the fish farmers. The acquired data are stored in blockchain to be tamper-proof. If these tamper-proof data are requested by the financial service, the data can be sent to the financial institutions, e.g. banks and insurance companies. The financial institutions use the aquaculture data to generate the credit data for fish farmers, which contributes to farming operational transparency and trust in business. When the farmer applies for a loan from a bank, the fish farmer will submit a business contract signed with the IoT service company for fish farming aquaculture monitoring service, purchase information, and other entrusted payment agreement to the bank. The data offered by the IoT service company for fish farming sufficiently alleviate the asymmetry that causes the risks between the bank and fish farmers. The banks and insurance companies are provided with the authorized and tamper-proof aquaculture data of the fish farm and farming, evaluate the data, and determine whether they will provide a loan or insurance service to the fish farmers.

### 6.2.3 Actors: people, components, systems, integrated systems, applications and organizations

Table 5 shows various actors involved in the system. It also provides the description of each actor and its interactions with physical/virtual entities or other actors.

**Table 5 – Actors for financial services for fish farmers**

| Actor name | Actor role | Actor description | Actor interactions (transactions between actors) |
|---|---|---|---|
| Sensor nodes for fish farming | IoT devices | Various devices which acquire the data/information relevant to the fish aquaculture, such as oxygen level, PH value, temperature of the pond. | IoT gateway |
| Oxygen controllers | IoT devices | Devices to start the aerator if the oxygen level is below the pre-set value. | IoT gateway |
| IoT gateway | IoT gateway | A device which communicates with the sensor nodes in the proximity network and aggregates the data/information from the sensor nodes, and transmits the aggregated data/information to the aquaculture monitoring platform. | Sensor nodes, oxygen controllers, and aquaculture monitoring platform |
| Aquaculture monitoring platform with blockchain | Application and service sub-system | A platform to provide the monitoring service of the fish aquaculture, supported by blockchain where the fish aquaculture data are stored. | IoT gateways, APP, and financial service portal |
| APP | Application and service sub-system | An application software for the fish farmers to access the service of the aquaculture monitoring platform. | Aquaculture monitoring platform |
| Financial service portal | IoT user / digital user | A web-based financial application for the fish farmers to apply for financial services. | Aquaculture monitoring platform |
| Bank | IoT user / human user | Participants who provide loans to the fish farmers according to the aquaculture data and credit data of the fish farmers. | Financial service portal |
| Insurance companies | IoT user / human user | Participants who provide insurance services to the fish farmers according to the aquaculture data and credit data of the fish farmers. | Financial service portal |
| Fish farmers | IoT user / human user | Individuals who apply for and attain the aquaculture service and financial services. | Financial service portal |



### 6.2.4 Issues: legal contracts, legal regulations, and constraints

Fish farmers sign contracts including the legal privacy data protection with aquaculture service providers and financial service providers.

### 6.2.5 Reference standards and/or standardization committees

None.

### 6.2.6 Relation with other known use cases

The use case of financial service for fish farming refers to reference by Xiaoping Yang, et al. (see Bibliography).

### 6.2.7 General remarks

None.

### 6.2.8 Data security, privacy and trustworthiness

Table 6 describes the security, privacy and trustworthiness associated with the data and information collected and stored in the system.

**Table 6 – Data security, privacy and trustworthiness for financial services for fish farmers**

| **Data security requirements and implications for applications, systems, etc.** |
|---|
| The aquaculture data are the key reference for the financial institutions to determine whether or not to provide the financial services to fish farmers; thus, the security of aquaculture data is maintained and the data are not tampered with. |
| **Privacy requirements and implications for applications, systems, etc.** |
| The aquaculture data from fish farmers are only accessible by the fish farmers, aquaculture service providers and authorized financial institutions. |
| **Trustworthiness requirements and implications for applications, systems, etc.** |
| The identities of the participants for the financial services are validated, authenticated, and trustworthy. The aquaculture data which generate the fish farmer's credit data are trustworthy. The aquaculture data are collected by sensor nodes and recorded in the platform supported by blockchain. |

### 6.2.9 Conformity aspects

None.

### 6.2.10 User requirements and interactions with other actors

The fish farmer's requirement is to obtain the loan in time when needed, while the bank's and insurance company's requirement is to provide the loan and insurance services with manageable risk.

The IoT service company for fish farming as an aquaculture service company operates the platform integrated with IoT system and blockchain which collects the fish pond data, identifies and eliminates risk factors for fish farmers, banks and insurance companies. It establishes the new business domain and market for fish farmers and financial institutions. The farmers report their fish farming data, which are validated with the platform, and the banks and insurance companies offer relevant financial services to the fish farmers because of the secured and trustworthy data from the platform.

### 6.2.11 Drawing of use case

This use case describes the IoT/blockchain-based business model of how to offer financial services to fish farmers and also how to minimize the aquaculture risks through the collaboration of the IoT service company for fish farming, fish farmers, bank, and insurance companies.

As shown in Figure 4, in the traditional way as described in 6.2.2.2 1), the fish farmers bear all the risks from weather, water-borne diseases, and price fluctuation; therefore, the success in fish harvesting is not guaranteed or known because of these unforeseeable factors, i.e. risks.

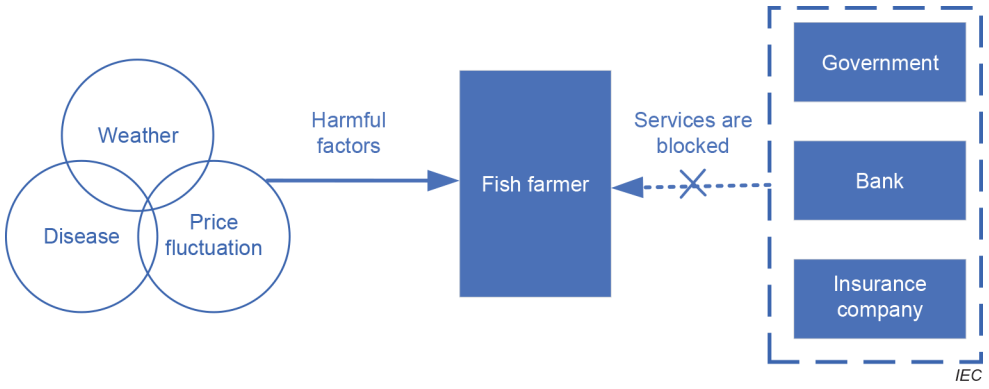



**Figure 4 – The financial risks without collaboration**

Through the collaboration of the IoT service company for fish farming, bank, and insurance companies, as shown in Figure 5 and described in 6.2.2.2 2), the IoT service company for fish farming uses the IoT sensing system to collect the real-time fish farming data from the pond. The system automatically monitors the various parameters of the water condition, and forecasts the potential danger to the fish in the pond and triggers remedial operations if the predicted emergency situation occurs. Therefore, the unforeseen risk is minimized by the high-tech aquaculture services supported by the IoT and blockchain technologies. The entrusted data are shared with banks and insurance companies that provide the financial service to the fish farmers. Even if loss events caused by risks occasionally take place, fish farmers will be compensated for their loss by the insurance companies.

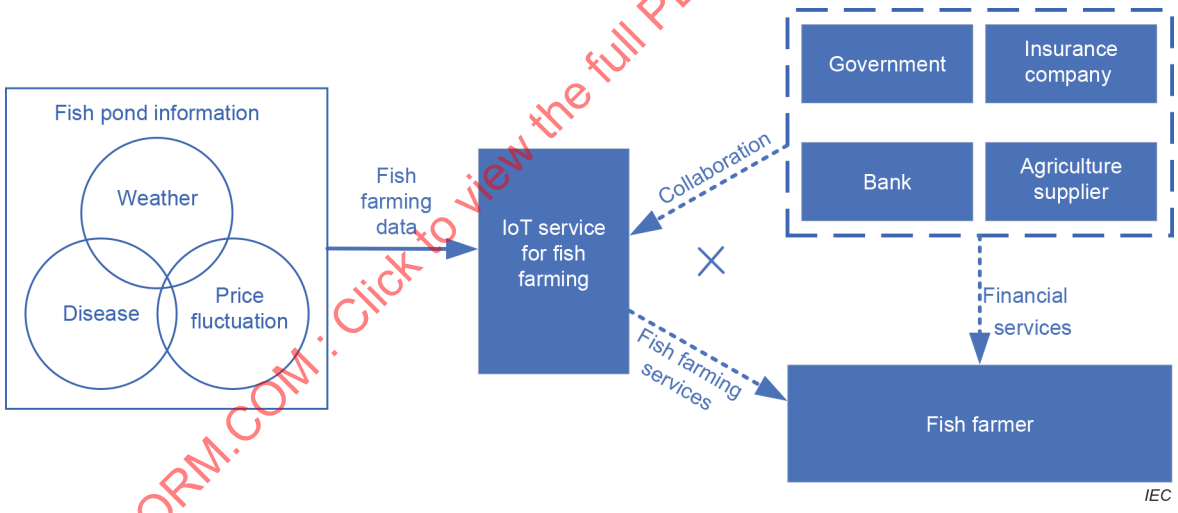



**Figure 5 – Financial risks minimized through the collaboration of multiple participants**



### 6.2.12 Data flow diagram of use case

With different stakeholders in the fish farming business, as shown in Figure 6, the following two types of data flow are necessary for the business model.

1) Fish farming data to the fish farmers

   The fish farming data are collected by sensor nodes, and the data are processed, analysed and recorded in the platform supported by blockchain technology. Some of the key data, including the oxygen level and PH of the pond, are sent to the fish farming APP on the fish farmer's smart phone. Therefore, the fish farmers can monitor the fish and pond water quality data in real time, on demand. And through the APP, the fish farmers can control the feeds and aerator based on the data and information presented through the APP.

2) Credit data of fish farmers to the financial institutions

The fish farmer's credit data are the most important information for the financial institutions to assess the credit of the fish farmers and their business. The credit data are generated from aquaculture data, e.g. the fish farming data, fish fry, automatic feed data, fish medicine data, etc.

When a fish farmer submits a loan application to a bank, the bank gets the applicant's aquaculture data via the interface with the aquaculture monitoring platform and generates the credit data by its financial service portal, enabling the bank to evaluate the loan application and to determine the loan amount that can be offered to the farmer.

When a fish farmer applies for an insurance coverage to an insurance company, the insurance company gets the applicant's aquaculture data via the interface with the aquaculture monitoring platform and generates the credit data by its financial service portal, enabling the insurance company to evaluate the insurance application and to determine the amount of insurance coverage that can be offered to the farmer.

The data flow may not be exclusively exhibited, data flow for other stakeholders may exist.

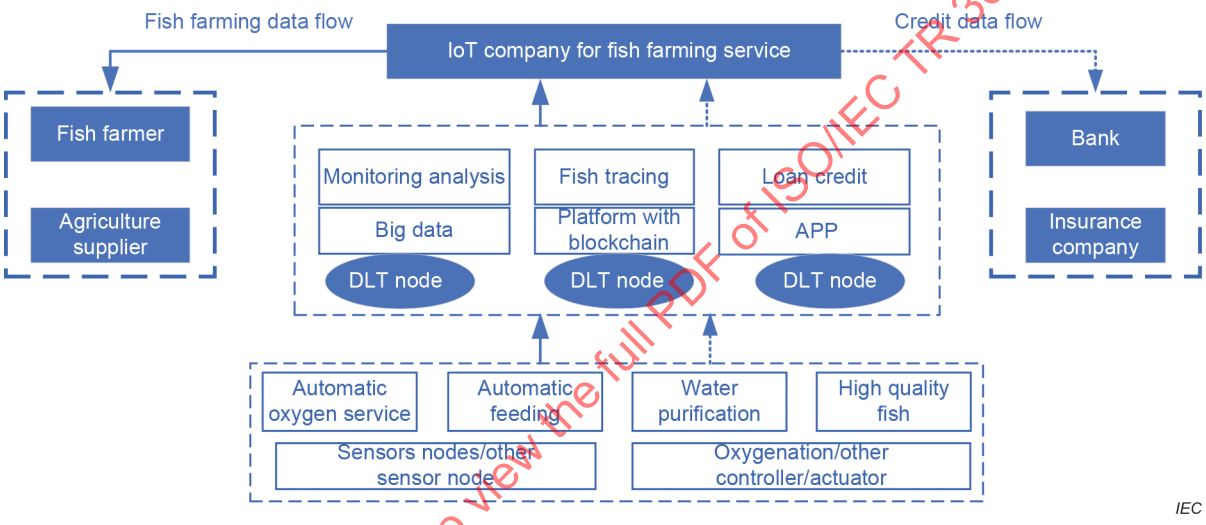



**Figure 6 – Data flow diagram of financial service for fish farming**

### 6.2.13 Sequence diagram of use case

Figure 7 shows the sequence diagram that describes the steps to set up the interactions among all the actors in the fish farming business model presented in this use case. Table 7 provides additional details of the steps shown in Figure 7.

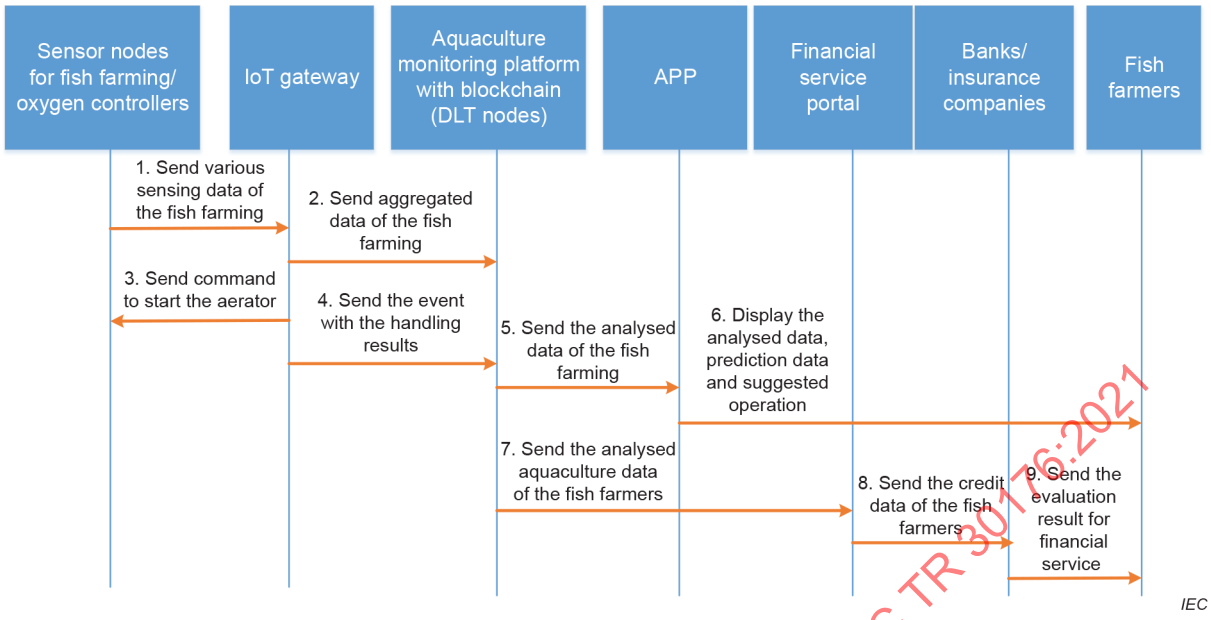



**Figure 7 – Sequence diagram of the financial service for fish farming**

**Table 7 – Steps of the financial service for fish farming**

| Scenario | | | | |
|---|---|---|---|---|
| **Scenario name:** | Realizing the financial service for fish farming | | | |
| **Step No.** | **Event** | **Information producer (actor)** | **Information receiver (actor)** | **Information exchanged (IDs)** |
| 1 | Send various sensing data of the fish farming | Sensor nodes | IoT gateway | Sensing data of the fish farming |
| 2 | Send the aggregated data of fish farming | IoT gateway | Aquaculture monitoring platform with blockchain | Aggregated data of the fish farming |
| 3 | Send the command to start the aerator | IoT gateway | Oxygen controllers | The controlling command if the oxygen level is low |
| 4 | Send the event with the handling results | IoT gateway | Aquaculture monitoring platform with blockchain | Event procedure and handling results |
| 5 | Send the analysed data of the fish farming | Aquaculture monitoring platform with blockchain | APP | Analysed data of the fish farming |
| 6 | Display the analysed data, prediction data and suggested operation | APP | Fish farmers | Analysed data, and prediction data, and suggested operation |
| 7 | Send the analysed aquaculture data of the fish farmers | Aquaculture monitoring platform with blockchain | Financial service portal | The analysed aquaculture data of the fish farmer who applies for financial services |
| 8 | Send the credit data of the fish farmers | Financial service portal | Banks/insurance companies | The credit data of the fish farmers with their credit evaluation models |
| 9 | Send the evaluation result for financial service | Banks/insurance companies | Fish farmers | Evaluation result of the financial services for the fish farmers |

## 6.3 Chattel mortgage services

### 6.3.1 Scope and objectives of use case

The scope of this use case is to describe how to realize chattel mortgage services by using IoT system and blockchain.

The objective of this use case is to help enterprises apply for loan services provided by banks efficiently and with a lower cost, and to help the banks to minimize the financial risks.

### 6.3.2 Narrative of use case

#### 6.3.2.1 Short description

This use case describes how to integrate IoT system with authorized device and platform integrated with blockchain to monitor the real-time status of chattel asset in the warehouse and during transportation, and provide the authorized data to the relevant stakeholders such as banks, chattel asset owners, chattel asset monitoring organizations, etc.; so as to prevent fraudulent activities and reduce unnecessary high risks in providing chattel mortgage services.

#### 6.3.2.2 Complete description

In traditional chattel mortgage processes, financial industry lacks efficient management for accessing, assessing and sharing the information of chattel assets and mortgage among stakeholders such as financial institutions. Further, there is no chattel asset monitoring and tracking which can quantify and validate chattel assets used as mortgage for loan applications. Even worse, some bad actors commit fraudulent activities by taking advantage of loopholes (i.e. no monitoring and lack of shared information between financial institutions), which damages both the financial and the chattel asset industries.

With the development of IoT and blockchain technologies, IoT systems with blockchain are highly applicable to the real-time monitoring and tracking of the mobile chattel assets in warehouse or in transit, which resolves and avoids the unnecessary high risks borne by both the financial institutions and the chattel asset industries.

### 6.3.3 Actors: people, components, systems, integrated systems, applications and organizations

Table 8 shows diverse actors involved in the system. It also provides the description of each actor and its interactions with physical/virtual entities or other actors.

**Table 8 – Actors for chattel mortgage services**

| Actor name | Actor role | Actor description | Actor interactions (transactions between actors) |
|---|---|---|---|
| Sensor nodes for the chattel asset | IoT devices | Various devices which acquire the data/information relevant to the goods in warehouse or in transit, such as number, weight, size, temperature, humidity, etc. | IoT gateway |
| IoT gateway | IoT gateway | A device which communicates with the sensor nodes in the proximity network and aggregates the data/information from the sensor nodes, and transmits the aggregated data/information to the chattel asset monitoring platform by which it is authenticated first | Sensor nodes, and goods monitoring platform |
| Chattel asset monitoring platform with blockchain | Application and service sub-system | A platform that provides the monitoring services of the chattel asset, supported by blockchain where the data of the chattel asset are stored. The chattel asset monitoring platform with blockchain is owned and operated by chattel asset monitoring service organizations | IoT gateways, APP, financial service portal |
| APP | IoT user / digital user | An application software for the users to access the service of chattel asset monitoring platform | Chattel asset monitoring platform |
| Financial service portal | IoT user / digital user | A web-based financial application for the enterprises to apply for financial service. | Chattel asset monitoring platform |
| Bank | IoT user / human user | Participants who provide loans to enterprises according to the monitoring data and other supply chain data of the enterprises. | Financial service portal |
| Enterprise | IoT user / human user | Organizations who apply for and obtain the loan from the bank with chattel mortgage service. | Financial service portal |



#### 6.3.4 Issues: legal contracts, legal regulations, and constraints

All the sharing or using of the data relevant to the enterprises to apply for the financial service must observe the laws and regulations of data security and privacy protection in the international and regional area.

#### 6.3.5 Reference standards and/or standardization committees

None.

#### 6.3.6 Relation with other known use cases

None.

#### 6.3.7 General remarks

None.

#### 6.3.8 Data security, privacy and trustworthiness

Table 9 describes the security, privacy and trustworthiness associated with the data and information collected and stored in system.

**Table 9 – Data security, privacy and trustworthiness for chattel mortgage services**

| **Data security requirements and implications for applications, systems, etc.** |
|---|
| The data security requirements are essential for the enterprises. For example, the data of the chattel asset monitoring platform are not tampered with, and the data are encrypted and stored in a distributed manner. |
| **Privacy requirements and implications for applications, systems, etc.** |
| The privacy requirements are important for enterprises and chattel asset monitoring service organizations offering data service. Enterprises and the chattel asset monitoring service organizations who offer their data/information to the chattel asset monitoring platform are authenticated. The data/information of enterprises and stakeholders is not obtained by unauthenticated users. |
| **Trustworthiness requirements and implications for applications, systems, etc.** |
| The trustworthiness requirements are fundamental and essential for the banks. The chattel asset monitoring platform provides banks with reliable and tamper-proof data/information. |

### 6.3.9 Conformity aspects

None.

### 6.3.10 User requirements and interactions with other actors

The user requirements for enterprises are to get loans and obtain other financial services by banks.

The user requirements for banks are to prevent and reduce the financial risks while providing financial services to the enterprises with chattel assets, such as the duplicate chattel mortgage with the same assets or chattel mortgage without real assets.

With the help of the chattel asset monitoring service organization who provides the chattel asset monitoring platform in warehouse and in transit, the banks interact with the enterprises easily through the financial service portal based on the trusted data of the chattel assets.

### 6.3.11 Drawing of use case

Figure 8 describes the relationships between the enterprises that own chattel assets and request a loan, the bank, and the organization that provides the chattel asset monitoring services with IoT and blockchain technologies.

The interaction procedures for the three stakeholders include the following.

1) Enterprises submit loan applications to the bank.
2) The bank authorizes the organization to deliver the chattel asset status data.
3) The organization obtains the chattel asset monitoring data generated from enterprises.
4) The organization sends the chattel asset status data to the bank for chattel asset evaluation, which acts as an important evidence in judging the loan repayment capacity of enterprises.
5) After reviewing the loan application from enterprises and evaluating the asset status data, The bank makes its final decision whether or not to approve the loan application, and sends the loan result to enterprises.

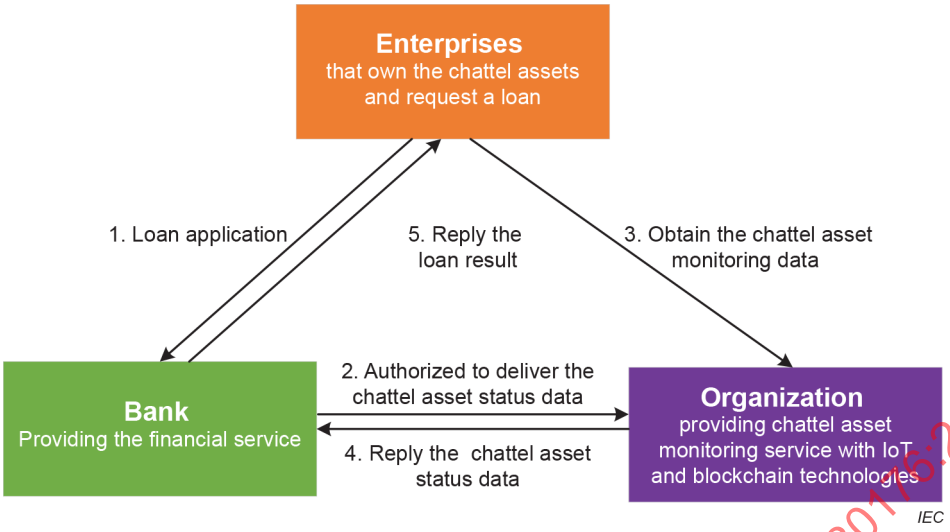



**Figure 8 – Stakeholders and their relationships in chattel mortgage monitoring financial services**

### 6.3.12 Data flow diagram of use case

There are three types of data flows in this chattel asset monitoring, as shown in Figure 9.

1) The monitoring data flow for chattel assets in warehouse

   The monitoring data for chattel assets in warehouse are collected by different types of sensor nodes recording the weight, contour, movement, position and other information about the assets, analysed by the IoT gateway in warehouse, and recorded in the chattel asset monitoring platform integrated with blockchain, displayed for the IoT users, such as financial institution, chattel asset owner, and chattel asset monitoring organization.

2) The monitoring data flow for chattel assets in transit

   The monitoring data for chattel assets in transit are collected by different types of sensor nodes recording the movement, vibration, tilting and other information, analysed by the IoT gateway in transit, and recorded in the chattel asset monitoring platform integrated with blockchain, displayed for the IoT users, such as financial institution, chattel asset owner, and chattel asset monitoring organization.

3) The order receipt management data flow for the IoT users

   The order receipt management data – including chattel asset status data (e.g. chattel asset type, specification, quantity, asset position in the warehouse, etc.) and chattel asset transaction data (e.g. pledgee, pledger, order number, order amount, etc.) – are generated, updated, managed by a chattel asset monitoring organization, according to the order of the chattel asset mortgage business.

   The order receipt management data are shared with the authorized IoT users, such as the financial institution and the chattel asset owner.

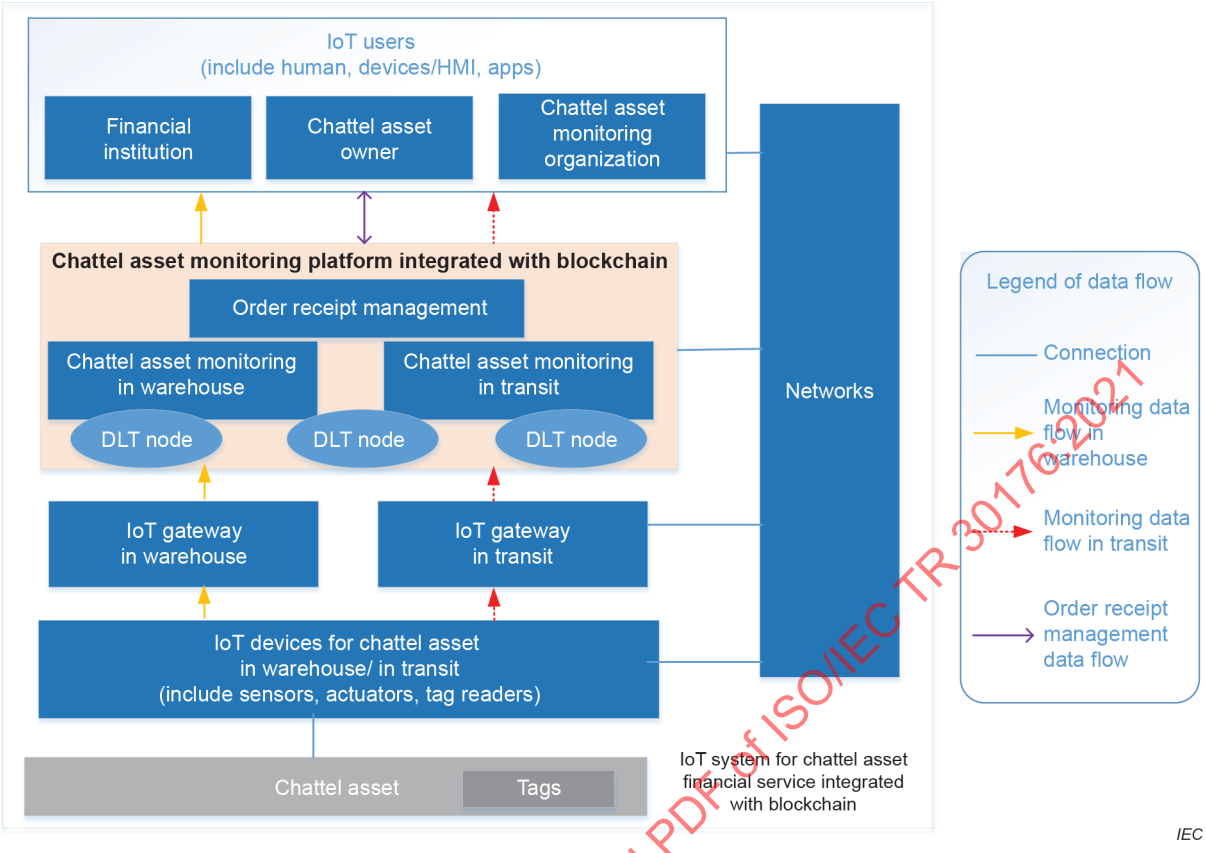



**Figure 9 – Data flow diagram of chattel mortgage service**

### 6.3.13 Sequence diagram(s) of use case

The sequence diagram shown in Figure 10 describes the steps to set up the interactions for all the actors in the system. Table 10 provides additional details of the steps shown in Figure 10.

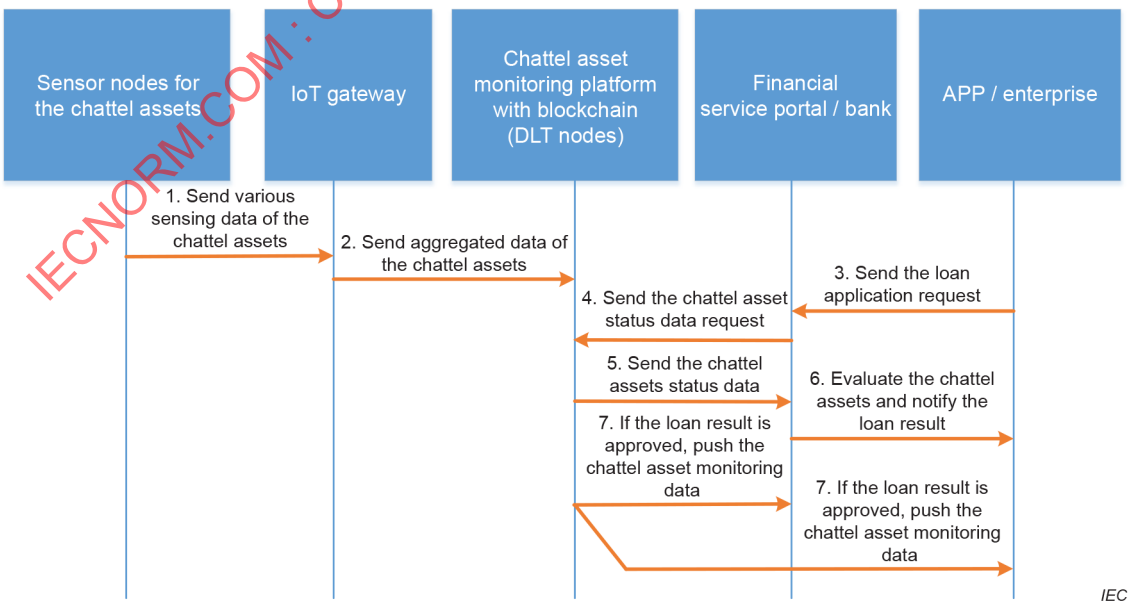



**Figure 10 – Sequence diagram of the chattel asset financial service**

**Table 10 – Steps of the financial service for chattel mortgage service**

| Scenario | | | | |
|---|---|---|---|---|
| **Scenario name:** | Realizing the chattel asset financial service | | | |
| **Step No.** | **Event** | **Information producer (actor)** | **Information receiver (actor)** | **Information exchanged (IDs)** |
| 1 | Send various sensing data of the chattel asset | Sensor nodes | IoT gateway | Sensing data of the chattel asset in warehouse and in transit |
| 2 | Send the aggregated data of chattel asset | IoT gateway | Chattel mortgage monitoring platform with blockchain | Aggregated data of chattel asset in warehouse and in transit |
| 3 | Send the loan application request | APP/Enterprise | Financial service portal/Bank | Loan request data including basic information of enterprise and the relevant orders of the chattel asset. |
| 4 | Send chattel asset status data request | Financial service portal/Bank | Chattel mortgage monitoring platform with blockchain | Request data including the basic information and orders of chattel asset for the relevant enterprise. |
| 5 | Send the chattel asset status data | Chattel mortgage monitoring platform with blockchain | Financial service portal/Bank | Chattel asset status data including the proof of the order for the chattel asset |
| 6 | Notify the loan result after the financial service portal evaluates the chattel assets | Financial service portal/Bank | APP/Enterprise | Loan result (i.e. whether it is approved) and loan limit |
| 7 | If the loan request is approved, push the chattel asset monitoring data | Chattel asset monitoring platform with blockchain | Financial service portal/Bank and APP/Enterprise | Monitoring data including the status, move-in, move-out and in-transit data, the ownership of the chattel asset |



## 6.4 Distributed energy trading

### 6.4.1 Scope and objectives of use case

This use case describes a peer-to-peer (P2P) distributed energy trading of an IoT-enabled and blockchain-based infrastructure.

The objectives of this use case are to provide a new way for the energy trading to improve the cost, security and flexibility of the energy trading in the microgrid.

### 6.4.2 Narrative of use case

#### 6.4.2.1 Short description

A blockchain-based trading infrastructure offers a distributed platform that enables peer-to-peer trading of energy between consumers and prosumers in a secure manner. The identity privacy and security of transaction is higher in the distributed platform compared to the traditional system, in which the energy transaction is usually performed through the central platform which is vulnerable to security threats.

#### 6.4.2.2 Complete description

In the traditional energy trading, the demand and supply of the energy are not transparent, so the cost of energy consumption has been higher and frequently the demand could not be satisfactorily met in an effective way. Additionally, some of the existing grid networks lack the necessary security with the transactions involved between mediators and other third parties.

The proliferation of distributed energy resources (DERs) along with widespread IoT technologies allows customers to become prosumers who can switch smoothly between power production and consumption. Prosumers take on a market role which contributes in implementing the fully distributed energy trading system.

The real-time operation information of microgrids is collected periodically by smart meters and phasor measurement units. The consortium blockchain platform is proposed to facilitate a secure P2P system for energy trading in Industrial Internet of Things (IIoT). The platform is highly useful in situations where renewable energy is generated at the prosumer's end. Surplus energy available from the prosumer can be sold in transactions with other peers in the blockchain network and the purchased energy is transferred to the grid. Each prosumer makes intelligent decisions on when and how much energy to purchase, consume, store, or sell. The prosumers involved in the transactions can use a smart contract, which is a legally binding agreement in blockchain computer codes. The smart contract includes the specific terms and conditions of the transactions which can be used for the involved prosumers to directly interact with each other.

When the microgrids are regarded as one of the fundamental market entities that can participate actively in energy trading, each microgrid needs to register in order to be authorized to participate in the energy trading system. Each microgrid interacts for energy transactions or settling existing energy transactions, which allows the peer-to-peer energy trading among the network of microgrids to be realized automatically.

In some occasions, both private blockchain and consortium blockchain can be used based on how the IIoT is structured. Private blockchain consists of smart meters and aggregators which store the metering information of the amount of energy owned by each user in a microgrid. The surplus energy owned by users can be traded in a microgrid or cross-regional microgrids. Consortium blockchain consists of aggregators which are also the representatives of nodes in private blockchain, and the cross-regional information sharing as well as energy trading can be realized by consortium blockchain.

### 6.4.3 Actors: people, components, systems, integrated systems, applications and organizations

Table 11 shows various actors involved in the system. It also provides the description of each actor and its interactions with physical/virtual entities and/or other actors.

**Table 11 – Actors for distributed energy trading**

| Actor name | Actor role | Actor description | Actor interactions (transactions between actors) |
|---|---|---|---|
| Smart meters | IoT devices | Various devices which acquire and report the data/information relevant to monitoring energy allocated for trading. | Aggregator |
| Aggregator (EAG) with blockchain | IoT gateway | A blockchain-based device or platform in the microgrid which communicates with the smart meters or other measurement units and aggregates the data/information, and exchanges information among other aggregators. | Smart meter or other phasor measurement unit, and wallet |
| Wallet | IoT user / digital user | An application software for human users to store, record and transfer the digital currency, token or points which is used for circulation in certain scenarios. | Aggregator, energy seller, energy buyer |
| Energy seller | IoT user / human user | Participant who provides the energy for sale. | Wallet |
| Energy buyer | IoT user / human user | Participant who demands, purchases and consumes the energy. | Wallet |

### 6.4.4 Issues: legal contracts, legal regulations, and constraints

The registering and using of the wallet must obey the relevant legal contract and regulations in local area.

### 6.4.5 Reference standards and/or standardization committees

None.

### 6.4.6 Relation with other known use cases

The use case of distributed energy trading refers to references Tejasvi Alladi, et al., Zhiyi Li, et al. and Zhitao Guan, et al. (see Bibliography).

### 6.4.7 General remarks

None.

### 6.4.8 Data security, privacy and trustworthiness

Table 12 describes the security, privacy and trustworthiness associated with the data and information collected and stored in the system.

**Table 12 – Data security, privacy and trustworthiness for distributed energy trading**

| **Data security requirements and implications for applications, systems, etc.** |
|---|
| The detailed energy production by each seller in the microgrid is encrypted, secured, tamper-proof, and is accessible only by the authorized buyers. |
| **Privacy requirements and implications for applications, systems, etc.** |
| The privacy information of trading behaviour is not exposed to their peers, such as amounts and patterns of energy generation and consumption. The completed energy transactions contain rich information sources for inferring potential trading behaviour of the microgrids' network. More importantly, sensitive commercial data (e.g. production cost coefficients of local generation) and critical operation information (e.g. operating states and security margin of local generation) of individual microgrids must not be revealed to their peers in order to preserve their privacy to the greatest extent. |
| **Trustworthiness requirements and implications for applications, systems, etc.** |
| Market operations for energy trading are trustworthy and treated transparently without distinction or prejudice to any microgrids. Careless or malicious participants are penalized or mitigated in order to minimize their adverse effects on market operations. |

### 6.4.9 Conformity aspects

None.

### 6.4.10 User requirements and interactions with other actors

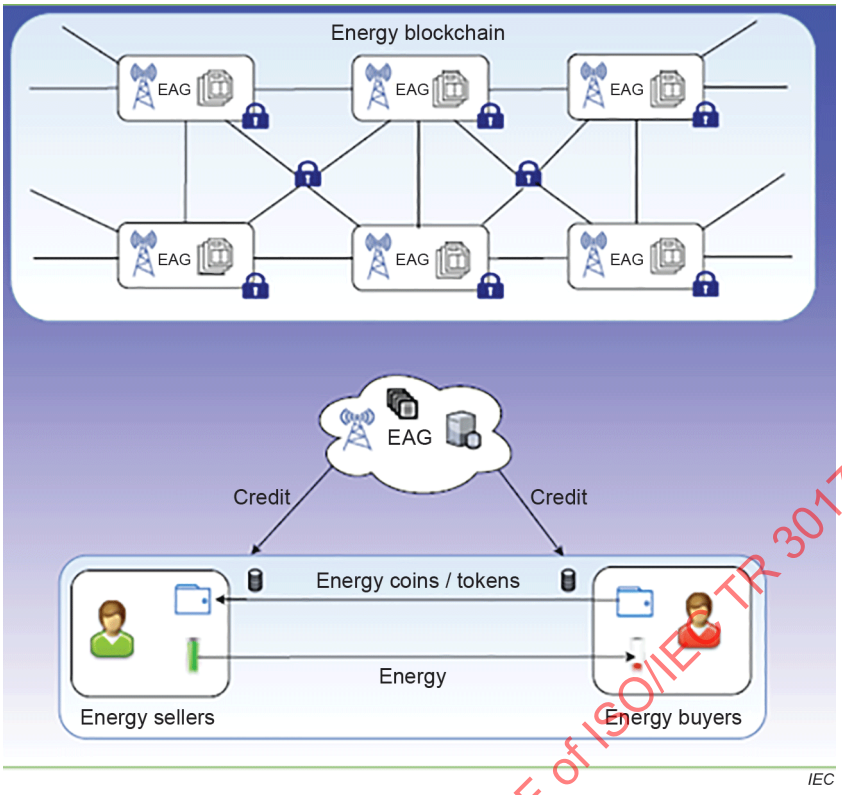
The requirements of the prosumers in the energy trading include smooth and easy decision making on when and how much energy to purchase, consume, store, or sell, and realizing the energy trading in a secure and efficient way.

The energy sellers and energy buyers interact directly in a distributed manner by smart contracts embedded in the energy trading blockchain.

### 6.4.11 Drawing of use case

This architecture uses a consortium blockchain-based energy trading system, which includes a blockchain platform and IIoT nodes for facilitating a secure P2P energy trade. The DLT nodes in the blockchain comprise energy aggregators (EAG), built-in smart meters in the IIoT nodes, and prosumers (e.g. solar panels or electric vehicles) providing the flexibility to choose their roles as buyers or sellers or idle nodes according to their requirements. The architecture for P2P energy trading is illustrated in Figure 11.

EAG can store and manage the energy transaction records. The energy sellers and buyers who register and get credit values from the EAG can trade energy directly. The energy is transmitted from the sellers to corresponding buyers by power lines or wireless power transfer, and the smart meters record the amount of the trade energy in real time. All the energy trades are recorded in the blocks of the blockchain.




SOURCE: Figure 3 of Tejasvi Alladi, et al.

**Figure 11 – Architecture for P2P energy trading**

### 6.4.12 Data flow diagram of use case

There are two types of data flows in distributed energy trading. Figure 12 shows the data flow in a microgrid and between microgrids. The upper part of Figure 12 describes the data flow between microgrids, and the lower part of Figure 12 describes the data flow in a microgrid. The EAG in a micriogrid stores the metering information of the amount of energy owned by each user, and the records of the energy transaction in a microgrid or cross-regional microgrids.

1) The energy trading data flow

The prosumers choose their roles as sellers or buyers based on the amount of the generated energy, the demanded energy, and surplus energy if it exists. The energy sellers and buyers can send their surplus energy data and demand energy data to the EAGs to initiate the trade. The energy trading data includes the energy demands or tradable energy. The request can be matched and negotiated by the DLT nodes. For example, DLT nodes are comprised of the EAGs and smart meters which load with consensus algorithms of the blockchain. If the sellers accept the negotiation with DLT nodes, the energy trading transaction will be generated and initiated in the blockchain including the price and the amount of the energy.

The real-time amount of energy transmission is collected by the smart meters of the energy sellers and energy buyers in a microgrid or between microgrids for each transmission. If all the energy transmission is performed, the buyers will pay for the energy trading at the negotiated price.

2) The transfer transaction data flow

If the energy trading payment is initiated by the smart contract in EAG, transfer transaction between the energy sellers and energy buyers with respective wallet addresses is verified by the DLT nodes through the consensus algorithms in blockchain. If it is verified successfully, the transfer transaction will be recorded in the blockchain, and the payment will be transferred from the wallet address of energy buyer to the wallet address of energy seller.

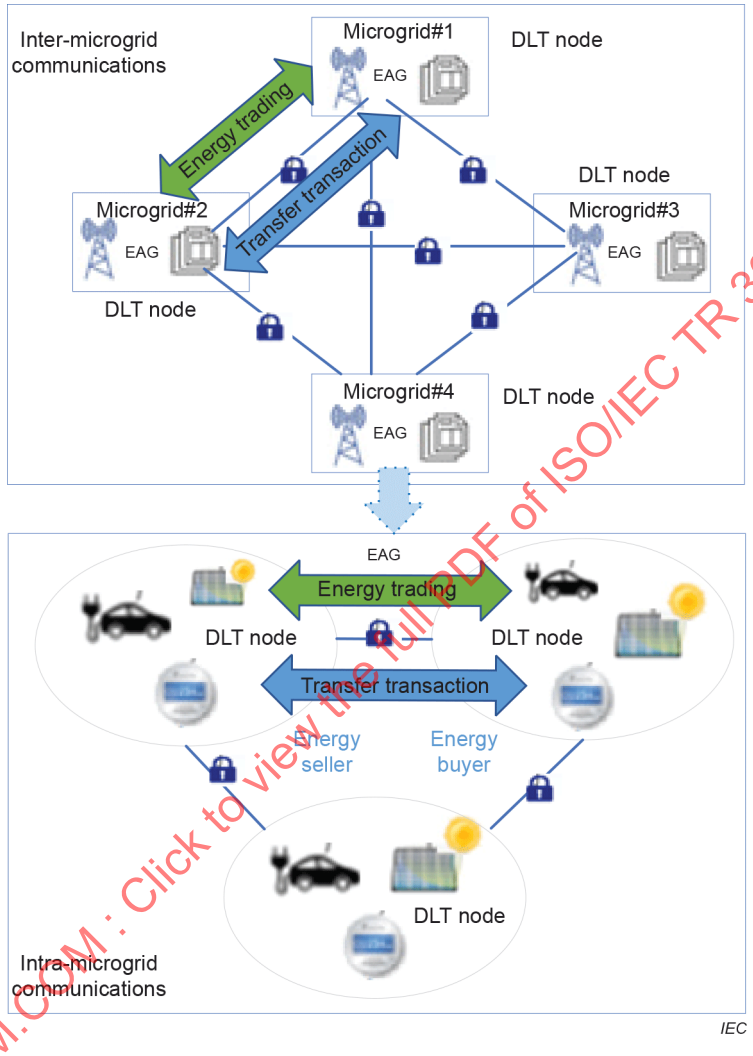



**Figure 12 – Data flow diagram based on hierarchical cyber enhancement framework for energy trading**



### 6.4.13 Sequence diagram(s) of use case

This sequence diagram shown in Figure 13 describes the steps to set up the interactions for all the actors in the microgrids. Table 13 provides additional details of the steps shown in Figure 13.

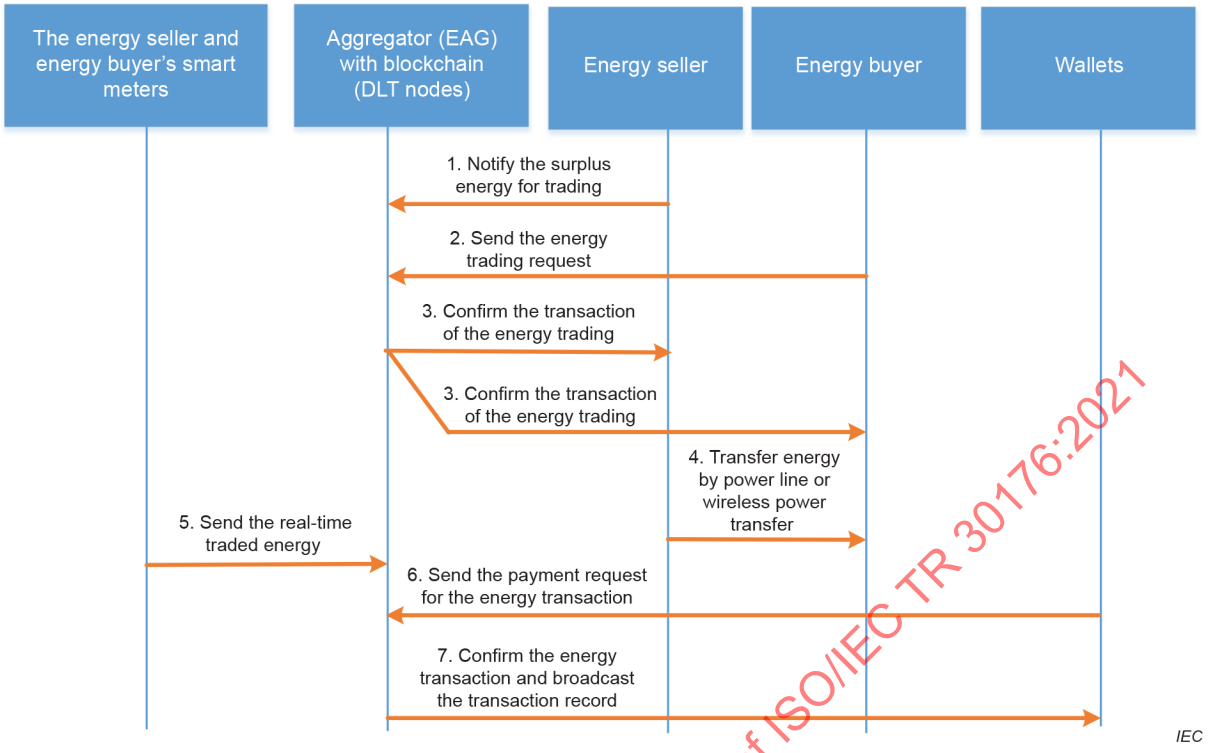



**Figure 13 – Sequence diagram for the energy trading process**

**Table 13 – Steps of the distributed energy trading**

| Scenario | | | | |
|---|---|---|---|---|
| **Scenario name:** | Realizing the distributed energy trading | | | |
| **Step No.** | **Event** | **Information producer (actor)** | **Information receiver (actor)** | **Information exchanged (IDs)** |
| 1 | Notify the surplus energy for trading | Energy seller | Aggregator (EAG) with blockchain | The amount of energy for trading |
| 2 | Send the energy trading request | Energy buyer | Aggregator (EAG) with blockchain | The amount of demanded energy |
| 3 | Confirm the transaction of energy trading | Aggregator (EAG) with blockchain | Energy seller/Energy buyer | The negotiated transaction data for each energy trading including the price, the amount of traded energy. |
| 4 | Transfer energy by power lines or wireless power transfer | Energy seller | Energy buyer | The electric power is transferred. The information of transferred energy is recorded in the smart meter. |
| 5 | Send the real-time traded energy | The energy seller and energy buyer's smart meters | Aggregator (EAG) with blockchain | The real-time amount of energy transmission. |
| 6 | Send the payment request for the energy transaction | Wallet | Aggregator (EAG) with blockchain | The payment information including the payment, the amount of traded energy, and the buyer and seller for the energy trading. |

| Scenario | | | | |
|---|---|---|---|---|
| **Scenario name:** | Realizing the distributed energy trading | | | |
| **Step No.** | **Event** | **Information producer (actor)** | **Information receiver (actor)** | **Information exchanged (IDs)** |
| 7 | Confirm the energy transaction and broadcast the transaction record to each wallet | Aggregator (EAG) with blockchain | Wallet | The transaction including the payment, the amount of traded energy, the buyer and the seller for the energy trading. |

## 6.5 Automated parking payment service

### 6.5.1 Scope and objectives of use case

The scope of this use case is to describe the automated parking payment service with IoT system and blockchain.

The objective of this use case is to realize seamless payment service for users, in order to pay the parking fee without delay and to enhance customer experience.

### 6.5.2 Narrative of use case

#### 6.5.2.1 Short description

Automated parking payment is a new way for users to pay a parking toll without manual payment and without use of a smart phone. This use case will give the main idea of what the seamless payment is and how to realize the seamless parking payment by automatically calculating and paying parking fees. The entire process is automatically realized by authorized devices, platform integrated with blockchain, wallet, and smart contracts.

#### 6.5.2.2 Complete description

In most the parking toll systems, the users usually need to queue to pay for parking fees when they leave a parking lot. It takes time to calculate and pay the fees both for the parking fee collectors and for the parking users.

In some pilot projects, IoT system and blockchain technology is used in the parking toll system, enabling users to pay the parking fee from their electronic wallet automatically even without stopping their vehicle. The authorized device, such as camera, detects and records the arrival time and the departure time for vehicles entering and leaving the parking lot, respectively. This information triggers the bills for the user in the smart contract. The payment transaction is recorded in the parking management platform with blockchain, which has the vehicle plate number and the wallet information of the user. This information is pre-registered and associated with the user's account, and the bill will be paid via the user's wallet automatically.

### 6.5.3 Actors: people, components, systems, integrated systems, applications and organizations

Table 14 shows various actors involved in the system. It also provides the description of each actor and its interactions with physical/virtual entities or other actors.