SENSING SYSTEM AND INTEGRITY OF SUPPLY CHAIN DATA

Data

When information is being transmitted from a device to the Ambrosus network, the data is bonded to an Amber token sent to the network. Common information that may be sent in a data transmission includes:

1. Tag ID, location and time;
2. Tracer, sensors and gateway IDs;
3. Quality and safety attributes of the products;
4. Transportation, handling and storage conditions as measured by various sensors;
5. Producer operability, capability and practicability (such as size of land, amount of workers, producing practices,..);
6. Integrity of the detection systems;
7. Digitized certificates;
8. Transaction ID;

An Amber token follows a product or batch along the supply chain, acting as a digital certificate that ensures the transparent transfer of information. All information can be retrieved at any supply chain stages. Selected information useful for the continuous supply process are made available to the stakeholders. The information necessary to fulfil consumer requests are also made available at the end of the chain flow.

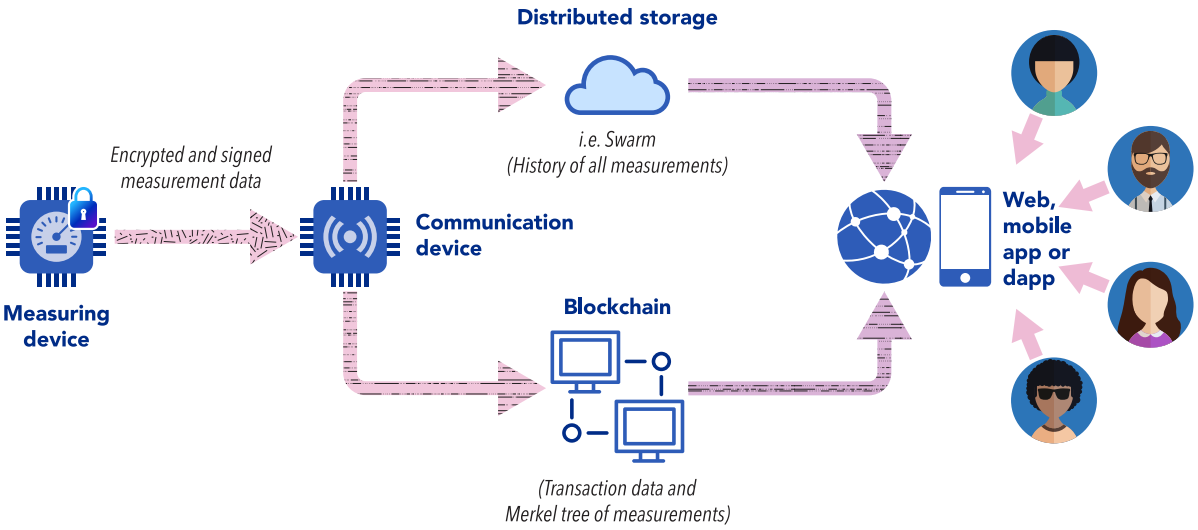

Figure 1: Path of the data throughout the Ambrosus solution

Tagging physical objects

Today, the initial raw materials, packaging or goods leaving the factories are generally tagged using a variety of 1D/2D barcodes, and in some cases passive tags such as RFID. . These systems are useful, but are not sufficient to assure that a given product is genuine or counterfeit. In order to assure the system is assessing the correct product, improvement in the tagging system is necessary and new, more product-oriented digital codes have to be considered.

The Ambrosus platform is considering the following product-oriented systems:

1. DNA labelling that provides a way to fingerprint proteins in medical products so that it is possible to determine where they have been manufactured.
2. Smart gels – also called unique tags – composed of an electronic emitter that can be applied at the surface of a biological product. These tags can be transparent and when applied on packaging they can assure integrity of the sealing and/or of the packaging by acting as an intelligent glue that reacts to fraudulent manipulation. For instance, when applied to corks (such as for the wine and alcoholic beverage industries), the gel changes colour if the cork is removed or a needle inserted to adulterate or extract the liquid.
3. Digital tracers comprised of capsules composed of an electronic embedded chip capable of communicating with the code in order to assure the presence of the product. These smart capsules can have a surface active bio-component combining the product with its packaging, thereby transforming passive elements into a smart and intelligent packaging system.

These different ways to tag a product are electronically active and connect to an electronic module (a chip inserted in a sticker at the packaging surface) in order to transmit the data in a similar way as the other sensors considered by Ambrosus. The tag or the tracer are connected with the sticker. If the connection is broken (product removed from the packaging, sticker counterfeited, product is adulterated), then the gateway is informed and can trigger an investigation.

Integrity of the data

Data generated by tags, tracers, on-site stationary and mobile systems is vulnerable to tampering if no proper anti-manipulation systems are deployed. The hardware we have developed helps mitigate this risk. The first architectural principle we have implemented prevents tampering through adapted sensor design. This consists of installing sensors that assess the product or the environment which are checked by dedicated sensors installed solely to ensure no fraudulent manipulation occurs. For example, by combining the system with anti-tampering mechanisms such as CCD cameras (Imperx solutions), embedded sensors (Kizzy tracking) or fully sealed containers (closure verified by miniature ultrasonic sensors), and sending it all through proper data encryption methodologies. The second architectural principle we have implemented sets a framework for sending information through encrypted channels. Our platform requires all data to be sent over secure and encrypted messaging, generally using HTTP and/or MQTT over TLS, and in some cases additional layer of end-to-end data encryption that is defined by the specific application or deployment of a system.

When sensors and instruments are designed as a fully interconnected system, devices can cross-check each other's integrity and subsequently reduce the threat of tampering. This design also validates the data integrity generated at the batch level without having to transit through the internal gateway.

At this stage, the sensors don't communicate with each other. They simply forward sensed data to one or several of the edge gateways, who will then pre-process the data, validate potential checks (has this object been opened during transportation, was this threshold exceeded for more than 10 seconds, etc.)

In future, in order to increase the security level, we will use sensor embedded cryptography. Hardware cryptographic blocks will be added to the sensor and entirely managed by the interface module between the sensors and the blockchain. Modern security solution are now provided for the IoT domain. In fact, we solution as provided by Riddle&Code to create a tamper-proof digital identity for all connected objects can be used. As a result, the sensors can be 'held accountable' for their actions. We assign a hardware-based digital identity to all devices by equipping them with a highly secure cryptochip that stores all information about the devices digital identity "off-the-bus". With every legitimate node then being registered on the blockchain, devices can easily identify and authenticate each other for various activities (sending of data, reception of data, and transfer of digital goods).

Gateways

The data from the detection system is encoded as a CSV string and then encrypted at the sensor level using hardware cryptography technology. The encrypted content is then sent to the edge gateway over several local communication interfaces such as BLE, NFC or RFID technologies depending on the specifics of each situation (bandwidth, cost or distance). The bundle is then decrypted by the edge gateway, which has low power processing capabilities to analyse basic rules and the ability to forward only important information about the product to the. The edge gateway is a device composed of a microcontroller having capabilities to collect, aggregate and select data from the different devices, performing basic analysis in order to check as much information as possible before transmitting only the necessary data downstream to another edge gateway or to the internal gateway. In many situation, it will need to be powered by batteries or energy harvesting and be able to operate continuously for several weeks or months to allow for mobile solutions.

Thus, part of the logic can be embedded and distributed through the edge gateways and even some sensors who have this feature. The overall architecture can be adapted and developed by the Ambrosus team according to the particular specifics of each product, supply chain and application.

Central gateways are much more powerful entities of the network that are able to receive large quantities of data from thousands of edge gateways and also transfer data to the blockchain and/or distributed storage. "central gateways" are more generally scalable and robust applications running on one or several physical machines in a private data center, or simply within the cloud. Those applications would be developed using a non-blocking IO model (written in scala, node.js or in other modern languages) and may have their own data base and outbound connections. Obviously, we see an ecosystem of various "central gateways" evolving (some built and managed by large industry consortia, while other by the open source community), where each company could chose the one most suited to their needs and expertise.

API version 1.0

The Ethereum Blockchain that we're using can only handle a limited number of transactions per second. When putting our sensor data on-chain, it degrades performance for our customers. That would imply a significant increase of the transaction fees and the system would become untenable. Therefore, we have come up with a way to keep the sensor data off the blockchain for our initial scaling up strategy by storing them on IPFS.

The data are put onto the blockchain if any side in the transaction disagrees with an outcome, to resolve disputes. If a party falsely alleges a dispute has occurred, then it can be proven and they can be penalized. This allows disputes to be settled on-chain only if needed and sensor data is kept off-chain in most cases. Merkalized abstract syntax trees keep validation rules minimal so that they only have to be revealed during a dispute. The idea of this dispute resolution is the same as the off-chain computing model for Ethereum contracts. State channels don't seem to factor into this as delivery contracts only have two states – success or failure. The details of the decentralized software and the core protocol can be found in the white paper.

Stationary and Mobile solutions

Fully integrated sensing systems with adapted in-house electronic configuration are developed accordingly and implemented for each application. The sensing system is wirelessly connected to the Blockchain platform. Transmissions of measurements are encrypted and all data are signed with device individual private key. In summary, a specifically designed sensing system is provided at each stage of the supply chain. It takes into account the attributes of the food commodities and products to be assessed while at the same time assuring no manipulation occurs during the detection phase until the data are safely stored onto the Blockchain.

Stationary systems

Monitoring devices installed along manufacturing lines or static instruments continuously generating data amongst production will generate most of the stationary systems. Today's quality assessment machines are too large to be mobile. Because they are thus static, the food is either plug into the machine during measurement time, or is mobile, i.e. moving on a conveyor belt, and travels through the instrument. To improve this situation, we are transforming printing systems (i.e. bar codes) into smart printer with scanners, able to scan compliance or production certificates in case they are not automatic. We are developing a solution to print QR codes using edible ink, or shelf-life pastilles reacting to spoilage. These machines will be our connection to the food by attaching a digital asset or a sticker to it. In fact, in applications where we provide an encapsulated digital asset we aim to control the development and the manufacturing of these devices that will be customized according to the customer's facilities.

Mobile systems

There is a lack of information about the quality of food commodities during transport and handling. Very basic information is missing such as temperature and light exposure. Depending on the implementation budget, there are mainly 3 solutions. The first one is data transfer using satellites, which allows connection to data in real-time for worldwide logistics. The second one uses GSM or GPRS (mobile phone antennas) to transfer data. This solution is actually under our radar to propose continuous monitoring of small sets of data transferred at 433MHz in csv format. The data is recorded during transport into the API and the whole recorded content can be downloaded all at once when connected to the receptor. This last solution is the cheapest but its main drawback is that it does not allow continuous data reception and therefore cannot foresee the quality of the batch being transported. The critical point with mobile sensors is assuring a correct standardization. Calibrated and certified sensors for continuous monitoring are expensive but accurate, whereas cheap sensors are not designed (yet) for certified measurement. Ambrosus hardware solution integrates cheap sensors into API through I/O connection and allows remote calibration to ensure day-to-day correct output reading. These techniques are now under investigation in the fish industry for tracing fish filet transportation: see document on operations.

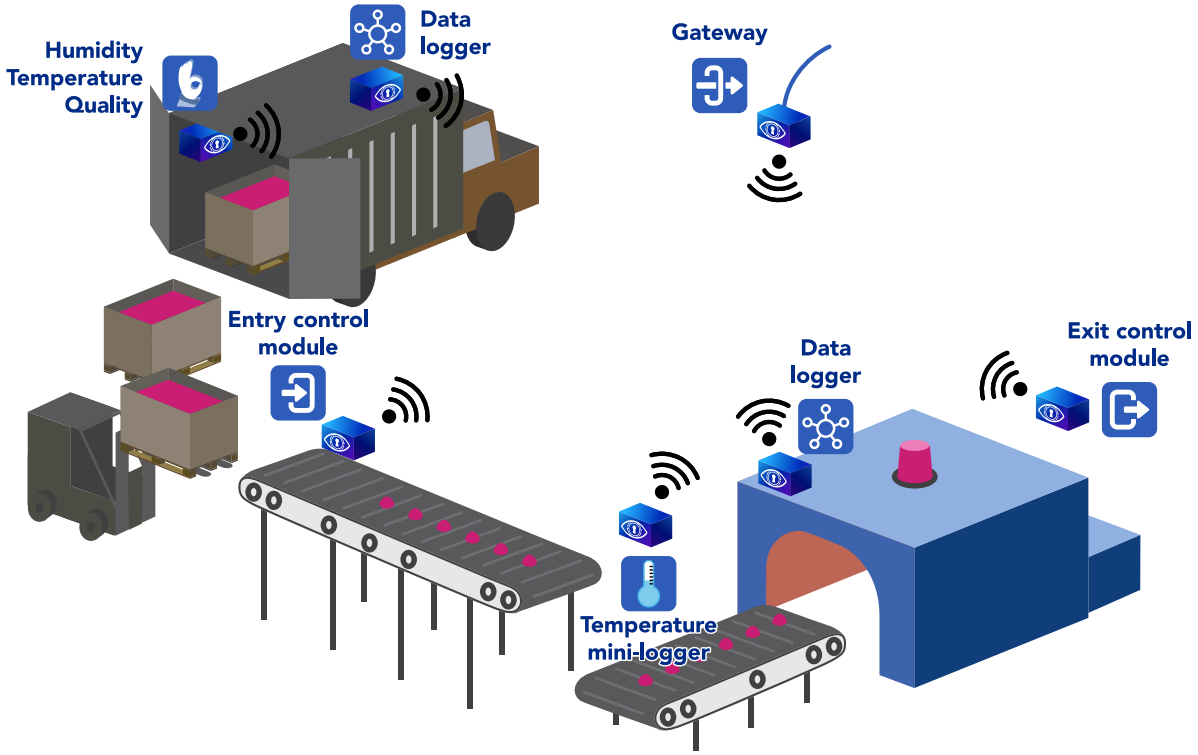

Figure 2: Mobile monitoring for certified temperature sensors, humidity and light interconnected through gateways. Any in-place system can be connected and direct visual information can be collected at transmission download in order to have rapid access to out of range data for the man handling the goods.

Security and integrity of sensors

We will create a registry of sensors that will allow us to take stock of most of connected IoT devices and to disconnect individual sensors if they become compromised or faulty. Every sensor will have a unique identification number and a private key that will allow Ambrosus to trace the exact origin of individual readings. The registry will include the following:

- Version number for sensors
- Type of sensor / unique ID
- Creation date
- GPS coordinates of individual sensors that is encrypted and viewable to some kind of owner contract
- Public key

The sensors connected to the edge gateway API are not necessarily miniaturized and integrated into that gateway. Sensors are actually placed according to their relevance to the measurement point. Sensors measuring the surroundings such as light, temperature, movement, and shock are integrated, whereas food quality assessment sensors are installed at a certain distance. Some have a wired connection, others are wireless, interconnected through encrypted NFC.

In order to assure low EM perturbations and simplification of encryption keys, we have developed a new system to exchange data through ultrasonic waves. With a reduced bandwidth, the system is limited for large amount of data transmitted and long distance transmission. However, it is well designed for proximity sensing systems such as mesh, and is particularly well adapted for transmission of encrypted data because it generates random encryption keys, which are provided from the emitter system and transmitted to the receiving part.

In addition, the ultrasound beam is directional which makes interception of the signal malevolent systems difficult. Furthermore, the transmission is interrupted in case of interception. This technology allows a fully independent system without any third party for authentication; in other words the sensors are talking to each other autonomously, exchanging encryption keys without external protocols.

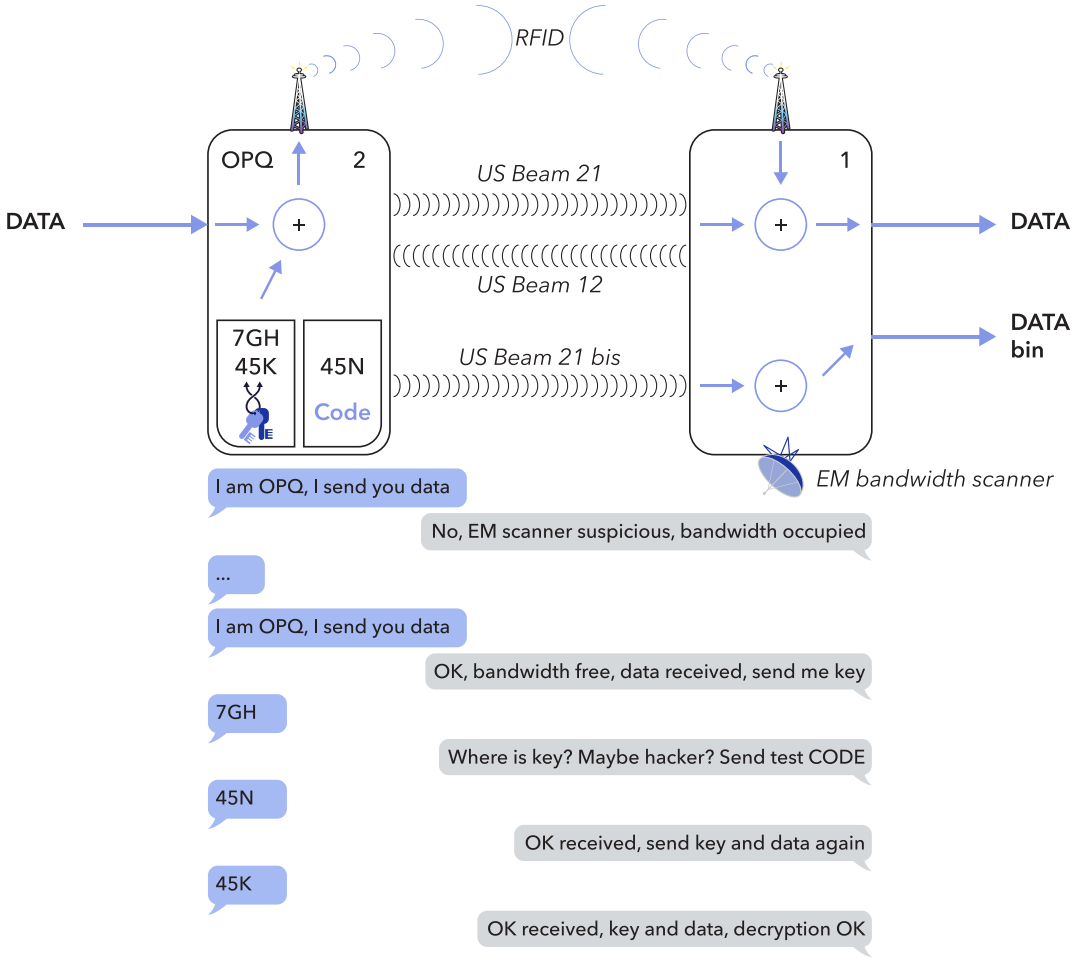

Figure 3: Ultrasound data transmission for encryption key transmissions between sensors

Future development of sensing systems and data format

The shift happening from analytical devices and image recognitions system to IoT sensors makes the data to handle smaller in size, down to a few bits. However, for sensors to perform the same assessment as analytical devices, multiple sensors have to be deployed. Single unit measurement devices have to be transformed into a complete system having multiple entries and its own embedded logic. That's the tendency of the future, to embed the logic at the sensor level. In fact, future developments in the electronic show a move from 2D IC to 3D, where transistors integrate a 3rd dimension to save space and multiply storage capacity. And we're not even talking about what quantum CPUs will bring to the field, changing drastically the capacities of the logic. This 3D approach allows having sensors with a first layer comprising the transducer, a second one for signal processing and the remaining layer for the capacity, down to a few nanometres.

Thus, cutting-edge sensors will perform the full assessment, transmitting only pertinent information to the edge gateway, where it will be analysed and sent over to IPFS. The overall architecture will reduce the size of the data down to the strict minimum before sending it to the Blockchain platform. The limitation to this principle is the energy these intelligent sensors require. However, thanks to the history of the watchmaking industry, the EPFL runs now research programs aiming lowering the energy consumption of embedded logic. These projects mainly try to reduce functioning voltage and develop the ability to extract energy from the surroundings.

Therefore, at this early stage, data will be handled and pre-analyzed in the Gateway (central command) through a dedicated software which will select the data to be transferred according to the operational purposes. When fully intelligent embedded sensors will appear on the market, transforming the way the logic is split throughout our architecture, they will be new requirement for the blockchain protocol which we will adapt. In any case, they will be a massive amount of small data generated which will have to be handled at the entry point of the blockchain platform and the interface architecture will be adapted. Therefore, embedding logic closer to the edge will increase upscaling speed of this technology, but will require a flexible architecture.

Business architecture

Outcomes of the quality sensors, digitalization outcomes of the sensing system and the certificates of compliance data transit through our different gateways. The Ambrosus API connect the data to the Amber and handle and store them in the Ambrosus software or core protocol. Either directly downloaded from the API or as a hash or a matrix from intermediate storage. The data are protected from hacking, data manipulation and fraud. Anyone can audit the entries, which include the unique ID of stakeholders as well as smart tags linking physical products to digital entries on the blockchain ledger. We are building our product system on top of the platform infrastructure set-up of the Ethereum blockchain protocol. Technical description can be found in the white paper.

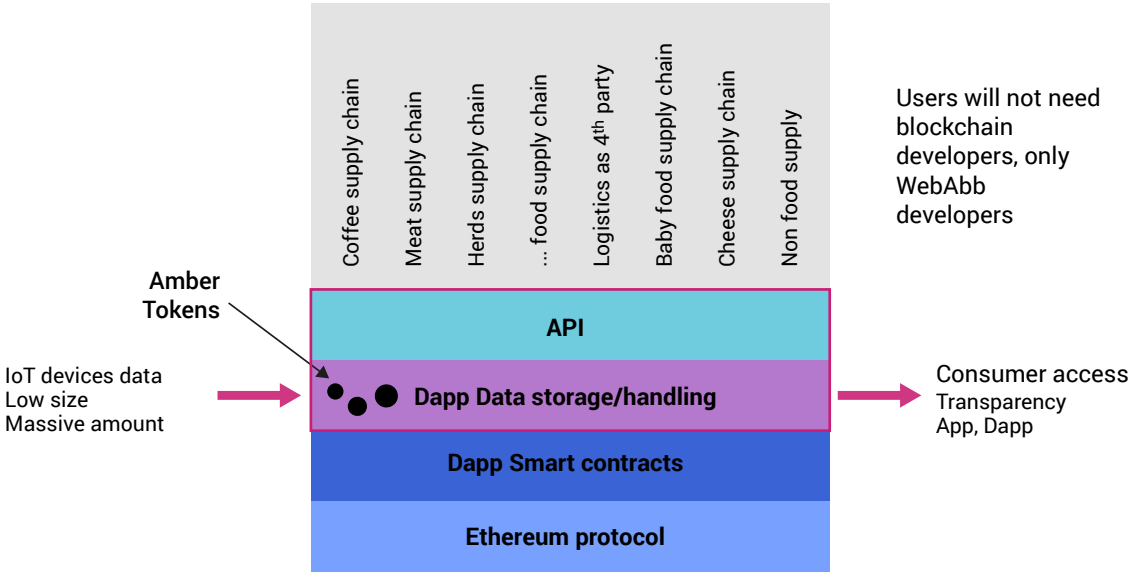

Figure 4: Business Architecture of the Ambrosus Technology API