Ambrosus

White Paper

Executive Summary

Origins of Ambrosus

I know that I am mortal and the creature of a day: but when I search out the massed wheeling circles of the stars, my feet no longer touch the earth, but, side by side with Zeus himself, I take my fill of ambrosia, the food of the gods...
– Ptolemy

The Ambrosus network is a blockchain-based ecosystem for supply chains, ensuring the origin, quality, compliance and proper handling of items tracked by the network. Ambrosus' primary focus is on improving supply chains for life-essential products, specifically food and medicine, although the protocol can be applied to almost any complex supply chain.

By using distributed ledgers, data processing and sensor systems, the Ambrosus platform can integrate across supply chain flows and enable transparency at every point within them. These new capabilities allow buyers and other participants in the supply chain to ensure that the standards of their Quality Assurance programs are being met. Ambrosus also enables the transmission of additional information between supply chain counterparties, as well as the creation of new applications and markets that utilize the platform's real-time data.

Ambrosus uses a novel incentive mechanism called the Amber token to provide these functions in a decentralized manner. The Amber token is used to keep information on the Ambrosus network up to date as products move across the supply chain without requiring a centralized actor to maintain resources. This token enables a transparent ecosystem with trustworthy data that can be freely accessed by interested parties.

This White Paper provides an overview of the Ambrosus platform, its architecture, and case studies. We have also created other guides that may be of interest to those learning about the Ambrosus network. These guides are available in English, Chinese (Mandarin), Russian, Arabic, Korean and Japanese and are available online at: https://ambrosus.com/#tech-docs.

Our open-source code is available on GitHub at https://github.com/ambrosus.

Table of Contents

1. Introduction

Since the world began to globalize after the initial industrial revolution, we have seen the rise of ever more complex supply chains to manage the subsequent flow of raw materials and goods around the planet[1].

These supply chains have been extremely successful, enabling the explosion of manufacturing, trade and innovation around the world that has been at the heart of globalization in the past few decades. The technologies and methods used to run these supply chains have not however kept pace with the growing interconnectedness and complexity of our world. Supply chains in many industries and sectors are creaking under the strain.

There are a host of challenges[1-2].

According to McKinsey, it has become a struggle for supply chain stakeholders to maintain an adequate overview of their networks[1]. That has made it increasingly difficult to ensure the quality and integrity of raw materials and finished products along the chain, fight contamination and counterfeiting, handle distribution, and maintain functioning and efficient logistics operations[3].

Highly complex chains with higher numbers of actors also create increasing opportunities for fraud, negligence, or other threats. Complexity also reduces transparency, making it more difficult to locate problems in a timely manner[1].

On the commercial side, today's global supply chains are riddled with archaic, slow and expensive processes that create significant friction along the chain and often make life difficult for participants, especially smaller producers or distributors. Even in the best of cases highly complex supply chains with multiple stakeholders imply intricate commercial relationships requiring complex governance structures that are increasingly difficult to manage using current practices[1].

At the same time, end consumers are demanding ever-higher levels of transparency about the origins of their products, as well as more personalization. This puts increased pressure on supply chains to innovate just when they are struggling to keep up with the status quo[1-3].

Many have – rightly – sounded the alarm, and are searching for new solutions.

1.1. A Data-Centric Solution

At its core, the solution to improving global supply chains revolves around handling data. Until now, it has been difficult to gather accurate data about the state and integrity of materials and products along the whole supply chain. Even where data is available, it is challenging to collect it, aggregate it, disseminate it and, above all, ensure its accuracy and integrity.

New technological developments are poised to change this.

These developments, which in particular include advances in sensor technology and the Internet of Things coupled with the capabilities of blockchain technology, smart contracts and decentralized applications (dApps), allow us to boldly rethink how global supply chains and markets might operate.

We envision a system of interconnected quality assurance sensors that can reliably record the entire history of a product[4]. A blockchain can then protect the integrity and verifiability of this sensor data. Finally, smart contracts can provide automated governance of supply chains and manage commercial relationships between actors along them[5-6].

1.2. The Ambrosus Project

Ambrosus is an ambitious project dedicated to making the vision we have described a reality. The project is made up of some of the world's leading experts and pioneers in the areas of sensor technology, data encryption, supply chains, blockchain, smart contracts and dApps, among others (see Team below).

Our team's mission is to create useful solutions for supply chains that enhance their quality, integrity and transparency, thus improving the quality and integrity of the products we all consume.

We believe this vision can be best achieved through self-governed, quality-focused networks to track products across relevant supply chains. These would be true ecosystems based on an open platform enabled by blockchain technology, with no centralized owner. The Ambrosus protocol is being developed to expressly allow the creation of such ecosystems.

1.3. Ambrosus Technology

Ambrosus is an end-to-end integrated solution that includes hardware, software, a protocol layer and developer tools.

The Ambrosus protocol and the software layer on top of it are built on the Ethereum blockchain as well as other distributed technologies that allow information from IoT devices to be recorded onto a decentralized network. We are also building a developer toolkit to facilitate the creation of apps on top of the network. This includes an open API tailored to the needs of food and pharmaceutical supply chain participants, one that is flexible enough to use with any type of commodity or consumer good. A JavaScript interface to Ambrosus sits on top of the blockchain layer, permitting users to develop to our platform without any blockchain programming knowledge.

To demonstrate how this can work, we have built a functioning prototype of an ecosystem that showcases the protocol's ability to collect information from IoT devices and record it on immutable decentralized databases. At the time of writing, we have released demo applications built on top of the current implementation of the protocol. These are publicly available online.

At the same time, the Ambrosus team is developing hardware sensors that feature plug-and-play compatibility with our blockchain network. The hardware products we have built to date include a range of non-invasive and rapid analytical devices for on-site measurement of biological samples. We are in the process of assembling IoT sensors around containers and printers to transform passive supply chain components into smart and intelligent systems.

Our development pipeline includes personalized tag methods as well as food grade tracers and biosensors to transform passive packaging solutions into smart conveying systems. These products connect to our blockchain through different gateways customized for different use cases.

Future iterations of our system will include ready-made and reusable connectors to rapidly share supply chain information with existing information services such as SAP or Oracle and which leverage GS1 standards such as EPCIS (Electronic Product Code Information Services)[7].

1.4. The Amber Token

The heart of the Ambrosus network is the Amber token, an ERC-20 compliant token that underpins all transactions on the Ambrosus network.

Amber is the world's first data-bonded token. It is used to bind continuously updated and verified logistical, environmental and biological data from the supply chain to its corresponding product as it travels between counterparties. It is also used to carry out transfers of value within the ecosystem. As such, the token performs both the utility and transfer of value functions within the ecosystem of applications built on top of Ambrosus protocol.

1.5. White Paper

In our view, Ambrosus is the most advanced project to date to tackle the complex and often life-essential challenges posed by today's global supply chains.

In the following chapters, we examine the Ambrosus protocol and the technologies being developed around the project. It is our hope that, with Ambrosus, we are creating tools that will enable all those involved in supply chains to meet industry challenges and create a new generation of trusted supply chains to meet the world's life-essential needs.

2. Ambrosus Protocol

2.1. Overview

In the following chapter, we describe key components of the Ambrosus protocol as well as important details relating to its structure and implementation.

2.1.1. Protocol Components

The Ambrosus protocol is constructed from three main components:

- **Measurements Repository:** Built around the Measurements Smart Contract, this component manages a distributed dataset for product-specific measurements that is built on top of a programmable blockchain (Ethereum) and distributed file system (IPFS). This smart contract is used to store readings of specified attributes collected for a given batch at specified points along a supply chain. Some of the properties of this smart contract include:
  - Authentication: The data source is authenticated and can be cryptographically verified.
  - Transparency: The collected data is publicly available to any interested party.
  - Immutability: The collected data is secured against changes or deletion.
  - Capacity: The system is capable of storing large quantities of small data packages.
  - Requirements Smart Contract: This enshrines the quality requirements to be compared with the content of Measurements Smart Contract. Some of the ways well-defined requirements can be used and reused include:
  - Monitoring: Users can verify that the quality of a particular batch of products fulfills pre-defined requirements.
  - Agreements: Multiple parties can automatically execute terms of agreements by comparing the content of the Measurements Smart Contract against the definition in the Requirements Smart Contract. This includes automatic payments settlement on the blockchain.

- **Amber token:** The data-bonded token architecture intrinsically ties data to AMB transactions on the blockchain, connecting chains together as products move through the supply chain.

Together, these components form the foundation of the Ambrosus protocol.

2.1.2. System Architecture

The Ambrosus protocol is built to support high data loads from hardware devices and network participants with substantially higher capacity than standard Ethereum software implementations. The platform's architecture is designed to be reusable in different industries, even those outside of the Ambrosus core team's focus. We discuss our system architecture in detail at the end of this chapter.

2.2. Measurements Repository

The Measurements Repository component of the Ambrosus protocol manages a distributed database for product-specific measurements. It is used to store readings of specified attributes collected for a given item at specified points along a supply chain. Key properties of the Measurement Repository include authentication, capacity, transparency and immutability. We will discuss first two in the following sections. The latter two properties will be a natural consequence of overall design.

2.2.1. Authentication

The Ambrosus network authenticates devices using public-private key cryptography. Each device on the network signs data transmissions with its unique private key in order to prove its identity as an authorised device. Signatures from devices can be verified against a list of authorised devices, which is a mapping of public keys to devices that is publicly available in a smart contract.

The Measurements Smart Contract includes a defined list of authorized measurement devices. Ambrosus-certified devices

can be added to the list through the Ambrosus platform. In future implementations of the Ambrosus network, we plan to introduce an open market for device manufacturers with associated reputation systems.

When an authorised device sends a message to the Ambrosus network, its public key is compared to the Authentication list for verification. Once verified, the message is accepted and recorded onto the blockchain.

If a non-authorised device sends a measurement, the signature verification fails and the measurement is simply ignored.

The diagram below demonstrates a data transmission from a measurement device to a customer device that is authorised on the Ambrosus network.

Illustration of a data reading on the Ambrosus network

2.2.2. Capacity

Although a single measurement is typically less than 100 bytes, the system is designed to collect potentially thousands of measurements per batch, and a batch may include data from multiple devices. Thus, in the long term, the Ambrosus network will need to handle terabytes of data daily.

To achieve this network capacity, Ambrosus has created a custom blockchain that integrates with the Ethereum blockchain and a distributed storage system.

In our early design of Ambrosus, we found that relying exclusively on the Ethereum blockchain for data storage was prohibitively limited in its capacity to handle Ambrosus' full data needs. The dual architecture that Ambrosus has created provides a scalable solution to the network's data capacity while maintaining decentralization, immutability and transparency.

New measurement data is stored as leaves in a Merkle tree. The Measurements tree nodes are then mapped to IPFS nodes. A Merkle tree is a structure that allows any party to quickly verify the validity of data in a branch or leaf using the root hash of the tree. In the Ambrosus network, this allows any network participant to quickly verify that a particular measurement is part of the given Measurements Repository. The root of the Merkle Tree is permanently stored in the Ambrosus network's Measurements Smart Contract. Every new measurement added to the Measurements Smart Contract creates a new version of the Merkle Tree with a new root, which can then be stored in the Measurements Smart Contract.

To retain a scalable system structure, Ambrosus chooses not to save a new root of the tree every time the tree changes (i.e., when a new measurement comes in). This would mean writing to the blockchain whenever new data arrives. Instead, the root of the tree is updated in the smart contract periodically (e.g., once every 100 readings).

Storing the Merkle tree root on the blockchain ensures the data cannot be modified once it is written into a contract. Ambrosus also maintains the entire history of all Merkle roots to ensure that no data has vanished or been altered between Merkle tree updates.

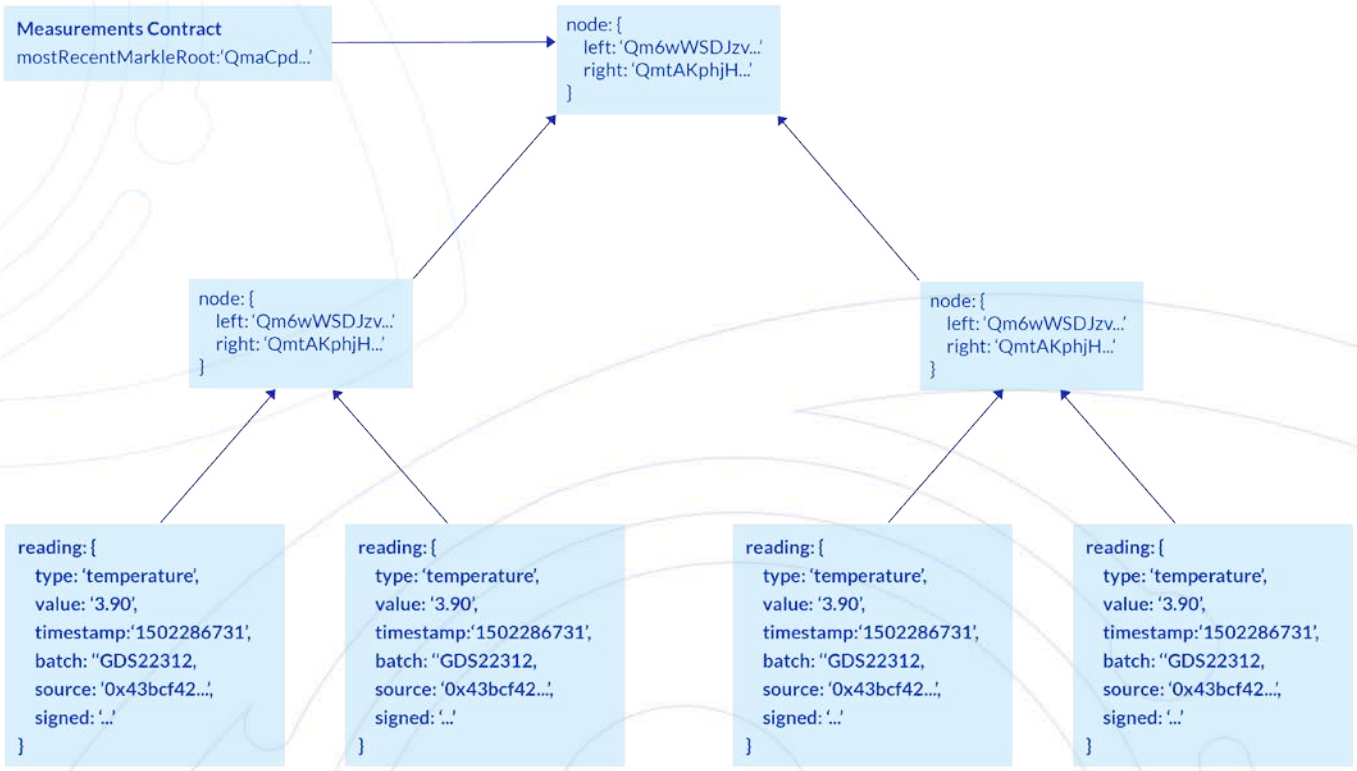


Illustration of Merkle Tree with readings and root stored in Ethereum contract

2.3 Requirements Smart Contract

The second component of the Ambrosus protocol is the Requirements Smart Contract. This portion of the protocol is used to define quality standards that can be directly compared to items in the Measurements Smart Contract. It is important that users create a set of well-defined, designed and tested Requirements contracts which are publically available on the blockchain. The requirements defined by users will be critical to applications monitoring items in the ecosystem.

In its simplest expression, the Requirements Smart Contract determines whether a product continuously meets standards defined by an interested participant in the Ambrosus network. For instance, a party may define distribution requirements to ensure food or pharmaceutical products remain safe for consumption. However, the concept of consumption is relative and depends on the product's purpose. For instance, a product might need to meet different requirements for:

- Consumption by humans
- Consumption by babies
- Consumption by animals
- Consumption by people with allergies
- Consumption by patients with certain conditions
- Instant consumption or future consumption
- Further processing (of different types).

For food products, Ambrosus can go further and define the various levels of quality for a particular product (e.g., low/mid/high/premium quality).

From a technical perspective, Requirements are lists of statements based on the readings from sensing devices. We can define a list of measurement ranges that are acceptable to an example

company in the food industry. The following is an illustrative list of Requirements for a batch of milk, defining a set of the following ranges:

- Temperature [4°C to 7°C],
- Fat [3.18% to 3.22%],
- Lactose [2% to 4%].

Similarly, monitoring systems in the pharmaceutical industry may define the following Requirements for frozen vaccine storage:

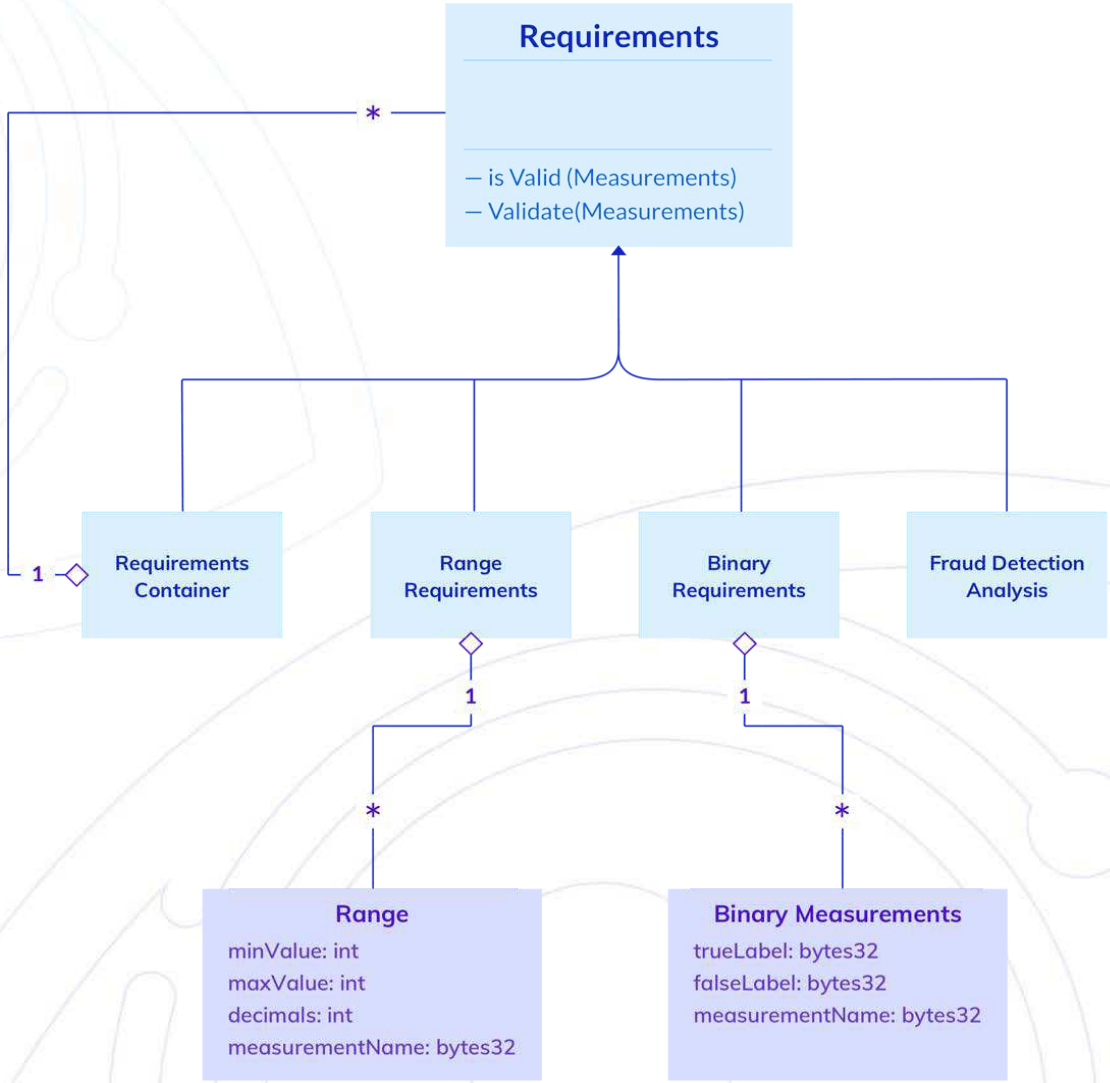
- Temperature [-25°C to -10°C],
- Humidity [2 to 3%],
- No direct sunlight or fluorescent light.

Requirements may be described using different quantifiable variables: range, binary (true/false) statements with information supplied by specific devices, or input from a human inspector (with the appropriate device and his own private key and reputation). Complex statements are also permitted (e.g., the temperature must be in the range [0°C to 10°C] for no longer than 10 minutes and [4°C to 7°C] thereafter). An alternative complex statement may define measurement timing (e.g., at least one temperature measurement must be taken every 10 minutes). These complex statements may also be coupled with instant financial rewards or penalties for assuring or failing to assure high quality, respectively.

We expect more advanced Requirements to use statistical analysis and machine learning to detect irregularities and support automated decision-making and real-time auditing. Those algorithms can be coded as Ethereum contracts or performed off-chain and verified on Ethereum.

As Requirements are sets of smart contracts working together and delivering from each other, in terms of object-oriented programming, Requirements can be viewed as a composite design pattern.

The diagram below provides a detailed overview of how Requirements are structured.



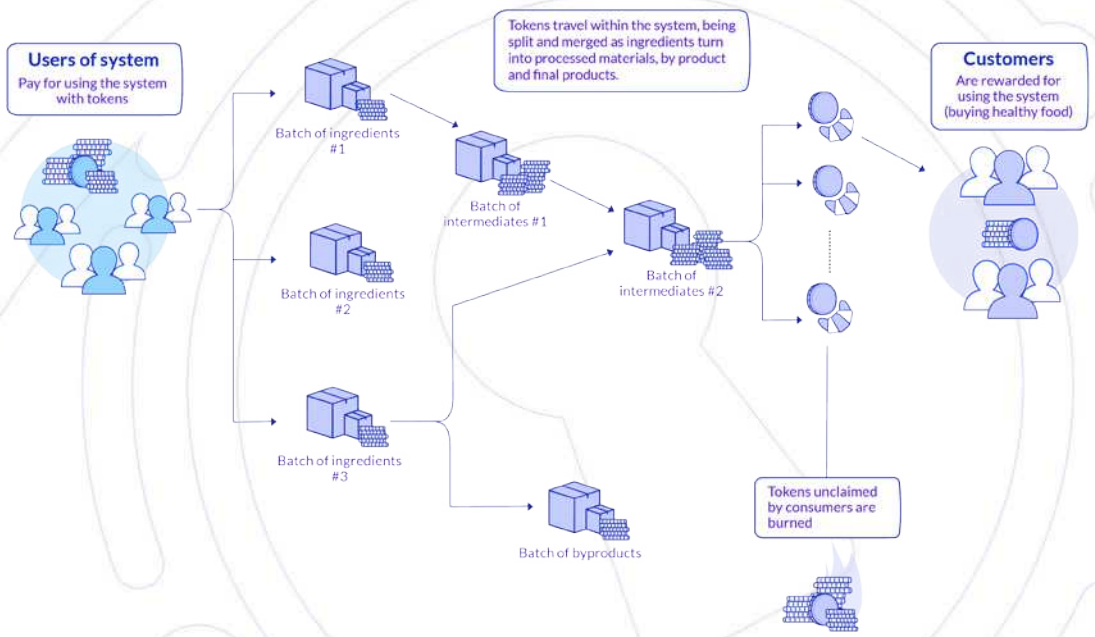
A simplified UML class diagram for a Requirements contract

2.4. Amber Token

Supporting the Ambrosus network is an ERC-20 compliant token called Amber. Amber is the first data-bonded token. As items move through the supply chain and are transformed in the manufacturing process, the Amber balance assigned to a particular batch can be split and merged into multiple other Measurements Smart Contracts, which together create a graph representing the history of a given item. Amber tokens are sent to the network alongside readings and remain locked in the Measurements Smart Contract until a batch has completed its movement through the supply chain.

Amber tokens remain bonded to a product until a defined expiration date or until the "termination event", which can be defined by a purchase, delivery or any other event on the supply chain.

End consumers can claim tokens at the end of the cycle. In this way, tokens can be recycled and return to the ecosystem. The value gained by recycling tokens incentivizes consumers to purchase Ambrosus-tracked products. This cycle also benefits producers, who receive free promotion.



Illustrative diagram of token travelling through the system

2.5. Optimizing Network Costs

To bolster adoption of Ambrosus, it is important to optimize the costs of using the network. Each individual supply chain uses unique transactions and contract deployments on the Ethereum network to handle data as items move through the chain. Running transactions on the Ethereum blockchain has become fairly expensive, and our custom blockchain implementation solves this issue.

Instead of the main Ethereum network, the main transactional network used by Ambrosus is the Ambrosus blockchain, a private version of the Ethereum blockchain. Note that the term "private" is potentially misleading here, as the network is public and can be accessed by anyone. The term is only used in this context to distinguish the Ambrosus blockchain from the Ethereum main network. All smart contracts related to the Ambrosus protocol will run on the Ambrosus blockchain, which will be periodically copied to the Ethereum main network for further validation.

While the Amber token crowdsale will initially take place on the Ethereum blockchain, Amber tokens will be transferred to the Ambrosus network once the construction of the Ambrosus blockchain is complete.

2.6. Architecture

2.6.1. Layered architecture

At the lowest level, Ambrosus is a set of core Ethereum smart contracts (including but not limited to the Measurements and Requirements Smart Contracts introduced in the previous sections). These serve as core business logic of Ambrosus and support data storage.

A JavaScript library sits above our contract layer. The JavaScript layer exposes the Ambrosus protocol interface to application developers. It abstracts the details related to particular implementation choices (e.g., we currently use Ethereum as a blockchain and IPFS as a distributed storage). This layer is also used to run software that does not need to be distributed and/or is expensive to implement as a smart contract, such as offline measurement verification. On-chain and off-chain operations are combined here into a single consistent interface.

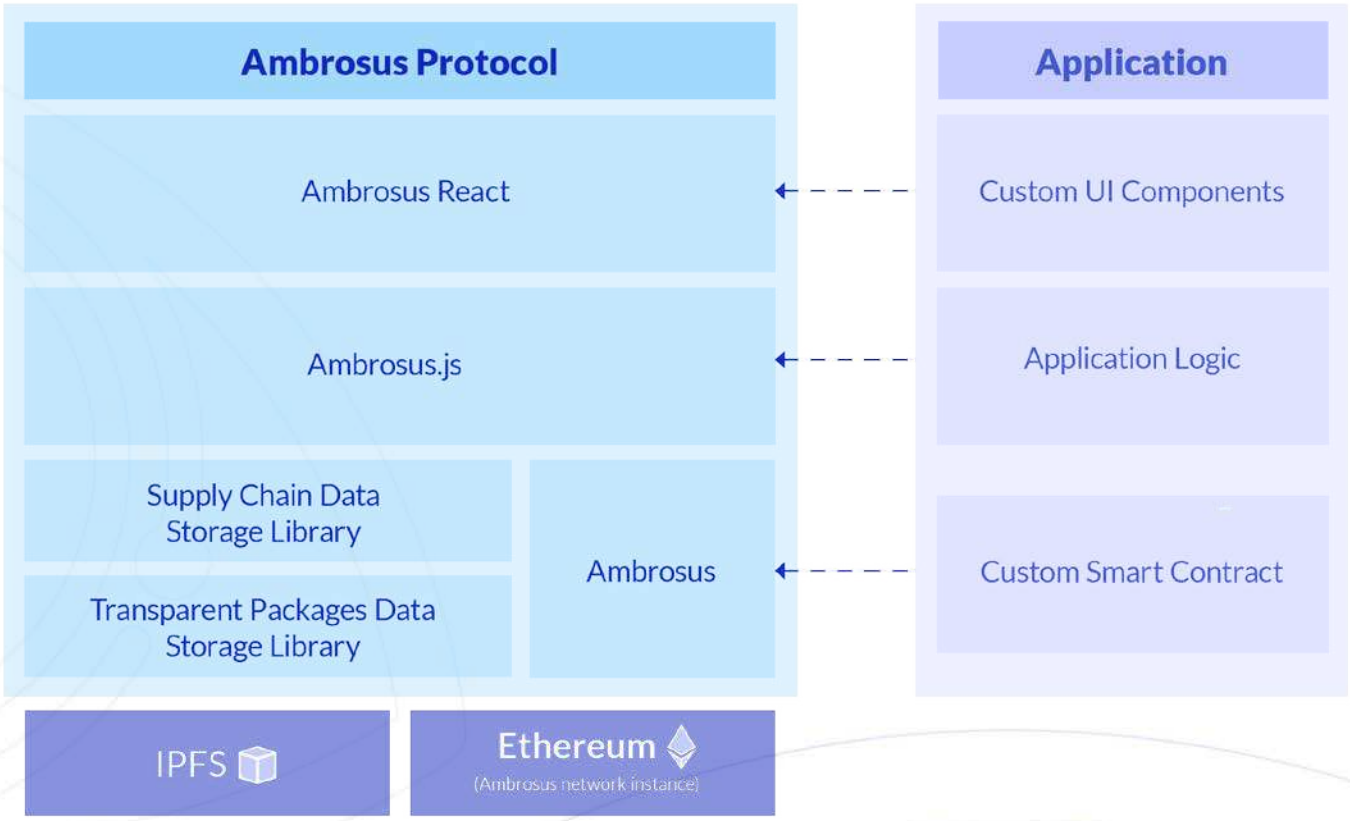
The top layer of Ambrosus consists of a React Component library. It provides UI components for building applications on top of Ambrosus network. This layer can be accessed by any web browser and connects to the JavaScript layer.

2.6.2. Data Architecture

Ambrosus uses an additional three-layer architecture for storing data:

1. The first layer is a library used to store large quantities of small data with blockchain and distributed file systems. This layer can store collections of individual data in a transparent, persistent and immutable manner. Core concepts here are signed data and Merkle trees.
2. The second layer is dedicated to supply chains. It employs concepts such as Measurements and Requirements Smart Contracts.
3. The top layer is Ambrosus.js, a protocol dedicated to food and pharmaceutical supply chains, with specific types of measurements and requirements related to those industries.

An overall technical overview of Ambrosus' architecture protocol along with the key dependencies is given below. We also provide a sample application to demonstrate how it interacts with Ambrosus.



Dependency diagram for an application using Ambrosus

Depending on the needs of a particular project, developers can use some or all of the features of our JavaScript and React libraries and/or the Measurements and Requirements Smart Contracts.

3. Supply Chain Data

The previous section focused on the software components of Ambrosus. This section describes how data originates on devices and its journey to Ambrosus' software.

3.1. Tag, Tracer and Sensor Systems

A key attribute of the Ambrosus network is its comprehensive support for IoT hardware and sensors, which provides the ability to tag and monitor physical objects and transmit data associated with them. This compatibility allows goods to be tracked throughout the supply chain and assures full integrity of readings. The Ambrosus network primarily collects data from tags, tracers and sensors.

A tag is an element set on the product itself, generally on top of the packaging, that provides information about the product and its identity. 1D/2D barcodes and passive electronic RFID stickers are examples of common tagging systems. A tracer is a natural compositional feature of a product or an added component inserted into a product, while a sensor is a device that detects and responds to some type of input from the physical environment. Sensors characterize the product and/or its environmental physico-chemical properties. A tracer will remain stable throughout its entire supply chain journey, whereas the correct sensor solution would need to be designed for each counterparty on the supply chain and will likely require more upfront investment and knowledge of product properties. Tracers are the ideal solution to track and trace products. When implemented in a supply chain, sensor solutions assess quality, safety and logistical conditions.

3.2. Detection Systems

Specific detection systems are selected and deployed by Ambrosus at various stages in the supply chain to offer the most effective and cost-efficient assessment of each product at each stage. A product's physio-chemical structure, composition and quality attributes may vary throughout the supply chain and must be continuously assessed to verify conformity with standards set by participants in the network.

There are several types of sensor systems that can be used to detect a product's physical state. Analytical systems are based on physical methods of analysis, including optical, electrical, acoustical and nuclear techniques. Biosensors and chemical sensors are further types of analytical systems which may be used to detect pH levels, allergens and other types of physical properties. Where appropriate, further methods such as immunological and enzymatic techniques or DNA and protein assays are also used to assess food. Environmental attributes such as temperature, light exposure, humidity, movement and oxygen are also recorded.

Hardware devices provide a platform to automate the input of data into a system and create a trusted basis of data input.

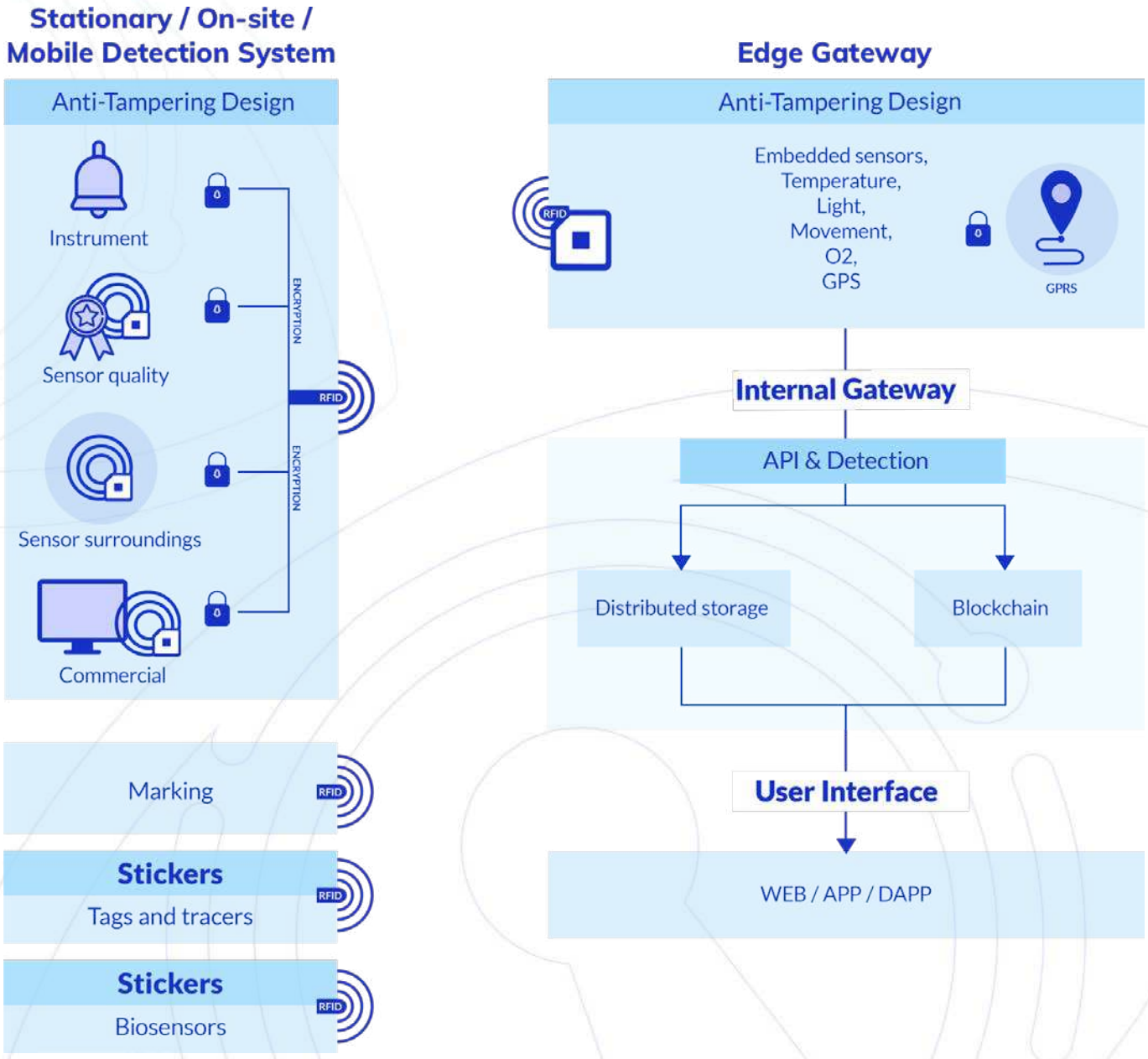
3.3. Data Transmission

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

1. Tag IDs, location and time, tracer, sensors and gateway IDs;
2. Digitized certificates and transaction IDs;
3. Product quality and safety attributes;
4. Transportation, handling and storage conditions as measured by sensors;
5. Producer operability, capability and workability;
6. Integrity of detection systems;

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 prior information can be retrieved at any supply chain stage.

The diagram below shows how data is transmitted across the Ambrosus network.



Ambrosus technology architecture

The data from the detection system is encoded and encrypted at the sensor level using hardware cryptography technology. The encrypted content is then sent to the edge gateway over various local communication interfaces such as BLE, NFC or RFID technologies, depending on the specific limitations of a particular implementation (e.g., bandwidth, cost or distance).

The bundle is then decrypted by the edge gateway, which has low power processing capabilities to analyse basic rules and will only forward product information required by the network. The edge gateway is a device composed of a microcontroller with the ability to collect, aggregate and select data from various devices, before performing basic analysis to transmit only the necessary data downstream to another edge gateway or the internal gateway. In many cases, the edge gateway will need to be powered by batteries or energy harvesting and be able to operate continuously for several weeks or months to enable mobile solutions.

Thus, some logic can be embedded and distributed through the edge gateways and even through sensors that have this feature. The overall architecture can be adapted by developers according to the specifications of each product, supply chain and application.

4. Team & Partners

Core: Angel Versetti (CEO), Dr Stefan Meyer (CTO), Marek Kirejczyk (Lead Blockchain Developer), Matthew Roberts (Lead Blockchain Developer); Prof Jean-Paul Sandoz (Lead Engineer); Prof. Esther Amstad (Lead Scientist); Katerina Ianishevska (Communication manager); Konrad Szalwinski (Lead Front-End Developer).

Advisors: Dr. Gavin Wood (Technical Advisor, Core Architecture); Dr. Jutta Steiner (Technical Advisor, Supply Chain); Dr. Vlad Trifa (Technical Advisor, Hardware); Prof. Malcolm Povey (Scientific Advisor, Food Reassurance); Dr. Fabiola Dionisi (Scientific Advisor, Quality Control); Prof. Sandro Carrara (Scientific Advisor, Biosensors); Jehan Chu (Strategic Advisor), David Drake (Strategic Advisor), Jaron Lukasiewicz (Strategic Advisor); Dhanesh Kothari (Mentor), Tom Lyons (Communications Advisor); David Wachsman (Public Relations Advisor).

Partners/Supporters: EPFL Innovation Park, Swiss Federal Institute of Technology; Department of Economic Promotion, Government of Canton of Vaud, Switzerland; United Nations 10-Year Framework of Programmes, Sustainable Food Systems Programme; EIT Food, European Institute of Technology; LDJ Capital; Kenetic Capital; Parity Technologies; Bitcoin Suisse; Crypto Valley Association; MassChallenge; Microsoft BizSpark; MME; WachsmanPR; Trek Therapeutics; Monaco Growth Forums; Lyons Communications.

APPENDIX

I. Case Studies

1. Initial Market Tests

Ambrosus is already actively working with industry partners to study various potential uses of the protocol. The list below contains market-fit studies we are currently running. Detailed documentation on our studies and the output of the pilot projects are regularly published in separate documents, which can be accessed at https://ambrosus.com/#tech-docs.

We are actively testing different solutions with industry partners. These solutions include:

- Traceability of various raw materials
- Brand protection for premium products
- Deploying a real-time compliance auditing system
- Monitoring correct delivery conditions for frozen goods
- Recording factory manufacturing procedures for audit traceability
- Secured data transmission and management for clinical trials
- Quality checker app for premium products originating from China

2. Food Industry: Compliance and Auditing

The food industry is dogged by regular scandals, the latest being the egg scandal in Europe, where consumers suffered from fraudulent practices involving fresh eggs contaminated by pesticides[8]. Mishandling and fraudulent processes are almost always eventually discovered, but by the time they are brought to public attention, the damage is done. Consumers have already bought, and likely consumed, the product, leading to potential health issues, loss of confidence, recalls, and other penalties. These problems stem from a lack of auditing. Companies are audited far too rarely, and the auditing process itself is time consuming and inefficient.

Blockchain has the potential to transform many business processes, making the data used in those processes more available, transparent, immediate and secure. The immutability, immediacy and transparency of information captured within the Ambrosus blockchain means that all necessary data can be recorded on the Ambrosus network and made available in near real time. In such a world, stakeholders are no longer simple recipients of post-hoc reports; they instead become part of a real-time process.

By applying blockchain technology to the food supply chain, Ambrosus is disrupting the whole food auditing process. One of the most exciting features of blockchain from a compliance perspective its practical immutability: as soon as data is saved onto the blockchain, it cannot be changed or deleted. This feature makes blockchain technology ideal for automated and transparent operations, allowing companies to meet their regulatory and compliance requirements in a cost-effective way.

In practice, digital smart tracers on a product will be connected to the Ambrosus network. As the product moves along the supply chain and passes different stages and sensors, Amber tokens will be sent and follow it, recording actions and their outputs immutably onto the blockchain. This creates an audit trail for regulatory bodies or government agencies to verify compliance, with all the information they require readily available in near real time.

This information is clearly valuable to businesses too. With its near real-time data, Ambrosus can support the greater automation of supply chain processes. This has an impact on the ongoing management of a supply chain, which can use on these automated process to make the work of businesses and government agencies easier at a fraction of the current cost.

The Ambrosus solution offers regulators direct access to the supply chain, allowing them to continuously monitor products and assure compliance with the most stringent laws and regulations. By relying on trustworthy, up-to-date data recorded on a blockchain, both businesses and governments can restore consumers' trust in the system.

3. Healthcare Industry: Data Information Management

The healthcare industry has been trying for a while now to encourage patients to take a more active role in managing their own care by self-administering medicines[9] which are usually taken at hospitals or bought in a pharmacy. Delivering personalized prescriptions to patients' homes would free up much-needed capacity elsewhere in the system and is thus an important challenge for the pharmaceutical industry.

But migrating from a system in which care is provided in a relatively small number of hospitals, clinics and surgeries to one in which care is provided through a widespread network of nurses and community carers has enormous ramifications. Pharma companies will need to distribute products to many more locations, including patients' homes. It will have to be able to deliver new therapies requiring rapid and constraining shipping solutions, especially to emerging markets, with better risk management and in compliance with more stringent quality requirements. The pharmaceutical industry will therefore have to harness the most efficient 'final mile' distribution networks in order to deliver medicines as economically as possible.

The immediate challenge is for healthcare to change its business model to a consumer-centric one, with a demand-driven supply chain. The key to preventing such a supply chain from becoming too fragmented and complex is seamless bidirectional management of information between patients and pharmaceutical companies. Information about patients and the medicines they need will thus be as important as the products themselves.

Ambrosus is designed for long and complex supply chains. For the healthcare industry, the Ambrosus protocol can connect digital smart tracers to medical products, with Amber tokens serving to connect the medical product and the sensor-generated data about it. As a product moves through the supply chain and passes along different stages and sensors, Amber tokens follow it persistently. This creates the highest assurance of traceability and compliance for all ingredients and components of drugs, while at the same time monitoring proper handling conditions for them. If necessary, the solution can even be tailored to the personal needs of individual patients. Any parameters can be encoded through the smart contracts which power the Ambrosus protocol.

The Ambrosus protocol acts as the backbone for the information platforms needed by logistics systems to record and exchange data securely and economically with suppliers around the world, to recall and analyse data very rapidly and to respond to sudden changes in supply and demand. The protocol is complemented by Ambrosus tracers and sensor systems that assure advanced tracking capabilities, which enable logistics systems to monitor products from the factory gate to the patient's door efficiently and securely, eliminating any scope for human error.

Amber tokens are tied to data for a specific product, from components of a medicine to logistics, and to the patients themselves. This information is directly bound to the physical product. The patient can thus use the Amber attached to their drug to extract all the information they need before taking the medicine. Ambrosus provides this functionality via a simple and intuitive user interface. Amber can thus act as a digital certificate attesting to product compliance, guaranteeing that the entire process and shipment procedures were carried out properly and following high standards. This will avoid manipulation and process failure and protect patients' health.

In short, Ambrosus offers an integrated supply chain solution dedicated to solving the challenges faced by the pharmaceutical industry of today and tomorrow.

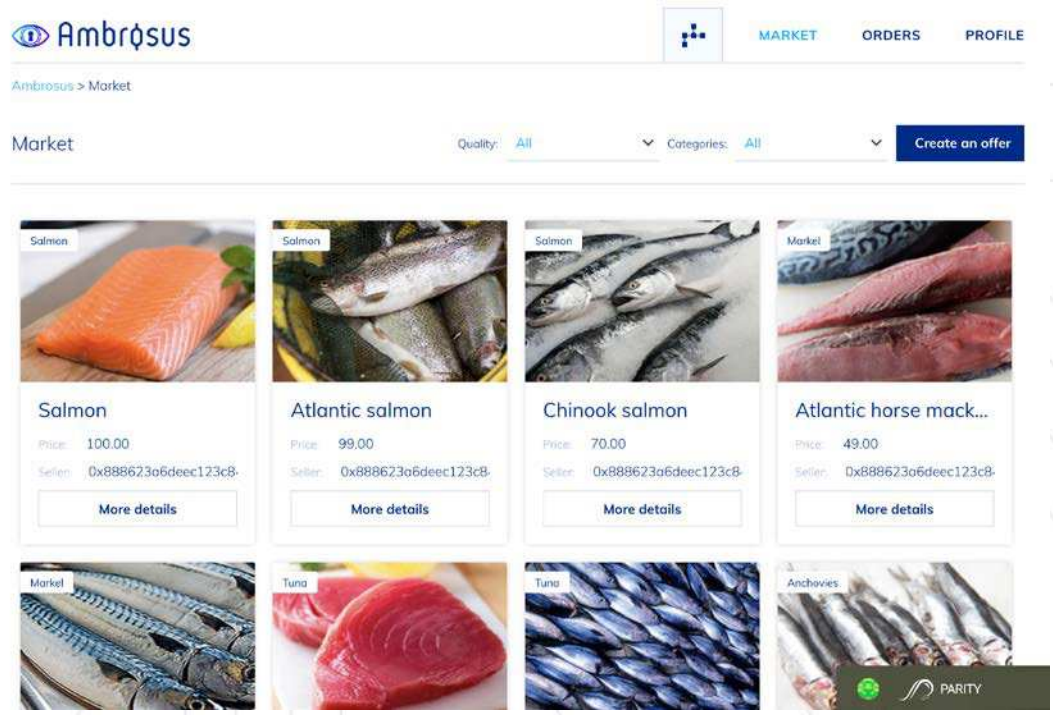
II. Current State and Future Work

At the time of writing, we have implemented a prototype of a protocol along with example apps which use the protocol.

1. Prototype

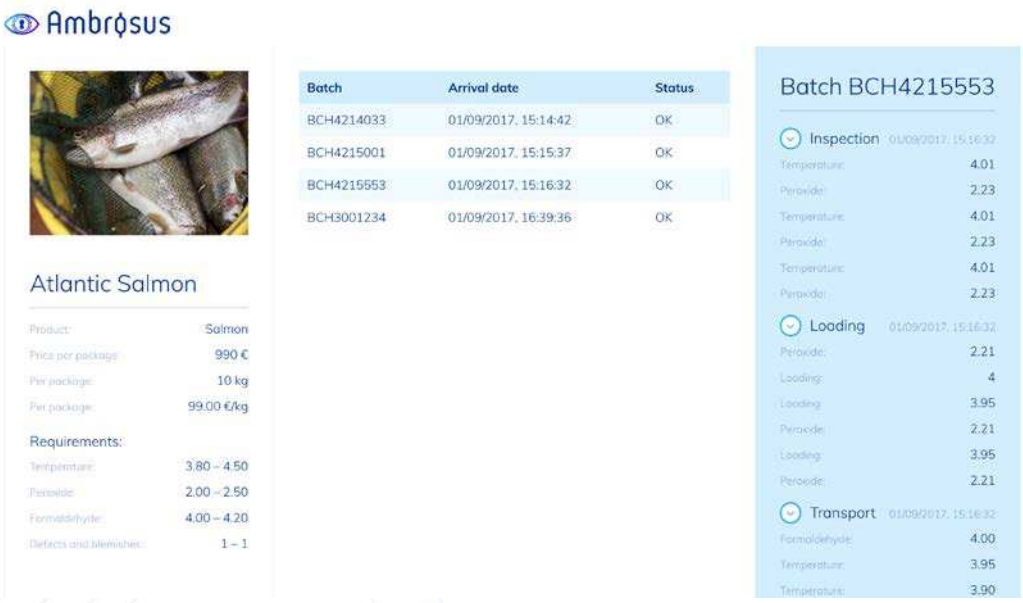
The screenshot below is from an application using the protocol. The app provides a distributed marketplace for food, where parties can agree on the quality of food delivered. Quality is measured and stored on distributed storage. An escrow allows agreement to be automatically settled based on sensor readings, allowing the creation of quality-conditional contracts.

A demo is available at: ambrosus-demo.com.



2. Protocol

The current state of the Ambrosus protocol is available on our Github page (https://github.com/ambrosus).



III References

[1] http://www.mckinsey.com/business-functions/operations/our-insights/the-challenges-Ahead-for-supply-chains-mckinsey-global-survey-results

[2] The top ten global health supply chain issues: Perspectives from the field, N. Privett, D. Gonsalvez, Operations Research for Health Care 3 (2014) 226–230

[3] Traceability in agriculture and food supply chain: A review of basic concepts, technological implications, and future prospects Article in European Journal of Operational Research January 2003

[4] Non-invasive sensing for food reassurance, Analyst,141,1587-1610, 2016; Xiaobo, Xiawei , Povey

[5] http://firstmonday.org/ojs/index.php/fm/article/view/548/469-publisher=First

[6] https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/

[7] https://en.wikipedia.org/wiki/EPCIS

[8] bfr.bund.de, health-assessment-individual-measurements-of-fipronil-levels-detected-eggs.pdf

[9] PwC, Pharma-2020-supplying-the-future.pdf

Many thanks for your attention.
Ambrosus Team

ambrosus.com
info@ambrosus.com

Ambrosus Technologies GmbH
EPFL Innovation Park, Station 13, 1015,
Lausanne, Switzerland
Gotthardstrasse 26, 6300, Zug, Switzerland
Tel. + 41 795 96 5876

Ambrosus