Honey authenticity: Introduction exploring the authenticity challenge

The challenge

Honey is a complex, naturally occurring product that has become a target for adulteration, like other high-value food products such as olive oil, whisky and wine.

Technology is increasingly playing a role in tackling many of the pressures facing food production and the supply chain, such as availability, quality, safety, nutrition and authenticity.

However, unlike other food products at risk of adulteration, which are made from harvested produce such as olives or grapes, honey is sourced from free roaming bees and their hives, which are not always pinned to a fixed location. As such, the tech-enabled provenance trails that have been suggested for other high-value food products are not as straightforward for honey.

Contested tests

In addition, testing protocols are contested due to the very nature of honey. There is a range of technical tests that can be applied to test the various components of the official honey definition (see p7). However, across the community of stakeholders in the honey sector, there is no consensus on exactly how these technical tests should be applied.

While the various tests that are used by labs to produce Certificates of Analysis (CoA) are inherently sound, there is a human element involved in understanding the nature of the variability of honey samples and how that is interpreted in results when it comes to application and interpretation. This is reflected in the language used in the analysis.

Consensus and compliance challenges

All of this matters as there are significant areas of disagreement and ambiguity. These include over the application of the test processes, the representativeness of the databases, the interpretation of the test results (with regard to the official definitions of honey), and the sharing of the data that underpins some of the tests. The legal ramifications are also complex. While technologies such as blockchain exist for food chain security, these do not address the challenges faced by regulators and food business operators when it comes to sharing data from certain testing methods such as nuclear magnetic resonance (NMR) technology and stable isotopic analysis. In particular, information is required on the collection of reference samples, curation of databases, interpretation and reporting of data.

In recent years there has been discussion and investigation into how tests can be combined and interpretations aligned, but there remain challenges in obtaining consensus for regulatory compliance. The recent reports2 from the Government Chemist set out these challenges clearly.

Data trust frameworks: a way forward

A potential route forward could be a new mechanism to achieve trusted and trustworthy data sharing between key stakeholders along the honey analysis and supply chain. Previous work on how a data trust framework might enable the permissioned sharing of data among collaborating stakeholders offers one such approach to the challenge of regulatory compliant testing for honey authenticity.

This report has been produced to present the findings and recommendations of a short investigation carried out on behalf of the FSA. The work offers a way forward to this challenge and builds on the recommendations from a previously funded FSA project on data trusts, which included a honey case study.

Approach

We see honey authenticity as a socio-technical challenge, recognising the interaction between people and technical systems.

The Data Trust Framework as described in the previous FSA reports and a paper in the journal Nature6 offers a solution that adopts these principles and builds on similar approaches implemented elsewhere, for example iSHARE in the Netherlands.

iSHARE: a successful and evolving example of a data trust framework

iSHARE is a Dutch initiative comprising a set of identification, authentication and authorisation agreements that enable organisations in the transport and logistics sector that participate in the iSHARE scheme to share data effortlessly. iSHARE enables them to:

- avoid costly and time-consuming integrations in order to share data
- share data with new and previously unknown partners
- maintain full control over their own data at all times. They have the final say about the terms under which their data will be shared, why, with whom and for how long.

The iSHARE Foundation, as the governing data institute, plays a crucial role. By signing up with the Foundation, logistics enterprises can join the network of organisations that all operate in line with the iSHARE Agreements.

The iSHARE Foundation works independently, transparently and not for profit. Among other things, the Foundation ensures that the agreements are upheld, manages the accession-related processes and facilitates further improvements to the scheme.

What is a data trust framework?

A trust framework can be defined as a legally enforceable set of specifications, rules and agreements that govern a multi-party system established for a common purpose, designed for conducting specific types of transactions among a community of participants, and bound by a common set of requirements.

Who does a trust framework serve?

A trust framework can therefore be implemented as a club established to meet the needs of members who have similar needs that they cannot easily satisfy on their own and are not met elsewhere. A key component of the implementation is the identity framework that ensures that not only trust is maintained, but that the underlying legal guarantees can be appropriately

implemented. Multilateral agreements can then be used among participants to enable secure collaboration and thus provide business models that extend the value that can be created from existing resources and processes.

An outcome driven collaborative approach

The secure sharing of data offers new business models. Peer-to-peer intermediation is enabled by an initiative that captures the needs of the community through collaboration of participants. This is supported by a collection of agreements necessary to sustain the ecosystem.