

Applications, limitations, costs, and benefits related to the use of blockchain technology in the seafood industry



Illustration: Nofima

Nofima is a leading institute for applied research within the fields of fisheries, aquaculture, and food research. We supply internationally renowned research solutions that provide competitive advantages along the complete chain of value.

«Sustainable food for all» is our vision.

Contact information

Telephone: +47 77 62 90 00

post@nofima.no

www.nofima.no

NO 989 278 835 VAT



Main office in Tromsø

Muninbakken 9–13

Box 6122

NO-9291 Tromsø



Stavanger

Måltidets hus

Richard Johnsenngate 4

Box 8034

NO-4068 Stavanger



Sunndalsøra

Sjølsengvegen 22

NO-6600 Sunndalsøra



Ås

Osloveien 1

Box 210

NO-1433 ÅS



Bergen

Kjerreidviken 16

Box 1425 Oasen

NO-5844 Bergen

Report

<i>Report number:</i> 5/2022	<i>ISBN:</i> 978-82-8296-707-5	<i>ISSN:</i> 1890-579X
<i>Date:</i> 08 March 2022	<i>Number of pages + Appendixes:</i> 35	<i>Project number:</i> 12929
<i>Title:</i> Application, limitations, costs and benefits related to the use of blockchain technology in the seafood industry		
<i>Tittel:</i> Anvendelse, begrensninger, kostnader, og nytteverdi relatert til bruk av blockchainteknologi i sjømatindustrien		
<i>Author(s)/project manager:</i> Petter Olsen ¹ , Shaheen Syed ¹ , Melania Borit ² and Celine Boechat ¹ ¹ Nofima, ² UiT the Arctic University of Norway		
<i>Department:</i> Industrial economics, Seafood industry		
<i>Client/Customer:</i> Highlands and Islands Enterprise through the Northern Periphery and Arctic (NPA) programme 2014-2020		
<i>Client's/Customer's reference:</i> Click to enter		
<i>Keywords:</i> Blockchain technology, food traceability, information logistics		
<i>Summary/Recommendation:</i> This report was commissioned to outline applications, limitations, costs, and benefits related to the use of blockchain technology in the seafood industry, and in particular to evaluate the pros and cons of having a blockchain-based food traceability system compared to a traditional electronic traceability system. This is an update of the previous Nofima report on a similar topic from 2019. The key concepts relating to traceability, and the components of a food traceability system are outlined in this report, as well as an indication of how traceability relates to other methodologies and approaches for ensuring food product authenticity. The core principles of blockchain technology are outlined, including different types of blockchain implementations, their characteristics, and some examples of solution providers and existing applications in the seafood industry. The last part of the report compares the functionality of traditional vs. blockchain-based food traceability systems, evaluates costs and benefits, and provides some practical advice on implementation issues, exemplified in the seafood supply chain. The overall conclusion is that unless speed of operation or confidentiality are considered to be the most important characteristics of the traceability system, a blockchain-based implementation may be very suitable. The main benefit related to a blockchain-based food traceability system is that, at least for now, the blockchain-based systems are more homogenous than traditional electronic traceability systems, so interoperability between different blockchain-based systems is likely to be easier to implement than interoperability between different traditional electronic traceability systems. Lack of interoperability is one of —, or probably the biggest current obstacle preventing system-wide, farm-to-fork food product traceability, so this advantage associated with blockchain-based implementations is significant.		
<i>Sammendrag på norsk:</i> Rapporten gir en oversikt over konsepter og systemer relatert til sporbarhet i sjømatindustrien, og gir også en grunnleggende innføring i blockchainteknologi. Tradisjonelle elektroniske sporbarhetssystemer basert på relasjonsdatabaser sammenlignes med blockchainbaserte sporbarhetssystemer, og fordeler og ulemper med de respektive løsningene evalueres. Hovedkonklusjonen er at dersom hurtighet eller konfidensialitet er de viktigste systemegenskapene så er tradisjonelle sporbarhetssystemer sannsynligvis bedre. Hovednyten av blockchainsystemer er at de er likere i oppbygging og struktur, og at det derfor er lettere å dele og integrere data mellom bedrifter og mellom verdikjeder. Dette er en veldig viktig utfordring i næringsmiddelindustrien, da manglende integrasjon er en av de viktigste utfordringene som hindrer tilgang til data som registreres på ulike steder i kjeden, og nytteverdien av blockchainbaserte sporbarhetssystemer er signifikant dersom de kan bidra til å løse dette problemet.		

Preface

This report is an update of the Nofima report on blockchain (Olsen, P. Borit, M. Syed, S, 2019) downloaded by more than 2000 people. The original report was focused on the use of blockchain in the food industry taking red meat and herbs and spices as supply chain example. This time we are focusing on the seafood supply chain.

Abbreviations and acronyms used in this report

API	Application Programming Interface
BaaS	Blockchain as a Service
CoC	Chain of Custody
EAN.UCC	European Article Numbering — Uniform Code Council
EC	European Commission
EDI	Electronic Data Interchange
EIT	European Institute of Innovation and Technology
EU	European Union
FAO	Food and Agriculture Organisation of the United Nations
FBO	Food Business Operator
GC-MS	Gas Chromatography–Mass Spectrometry
HPLC	High-Performance Liquid Chromatography
IoT	Internet of Things
IPOA-IUU	International Plan Of Action to Prevent, Deter, and Eliminate Illegal, Unreported, and Unregulated fishing
IUU	Illegal, Unreported and Unregulated Fishing
NIR	Near-InfraRed (spectroscopy)
NMR	Nuclear Magnetic Resonance
SSCC	Serial Shipping Container Code
TRU	Traceable Resource Unit

Table of contents

1	Background	1
2	Methodology	2
3	Conceptual framework	3
3.1	Traceability and traceability systems	3
3.1.1	Traceability concept, terms, and definitions	3
3.1.2	Traceability systems and their components	4
3.1.3	Drivers of traceability systems	5
3.1.4	Traceability and analytical methods	6
3.1.5	Traceability and chain of custody	6
3.1.6	Traceability and transparency	7
3.2	Blockchain and blockchain technology	7
3.2.1	Blockchain definition	7
3.2.2	Blockchain characteristics	9
3.2.3	Blockchain types	10
3.2.4	Permissioned vs. permissionless	12
3.2.5	Blockchain infrastructure	13
3.2.6	Blockchain and transparency	13
4	Application of blockchain technology in the food sector	16
4.1	Overview of providers of blockchain technology	16
4.2	Overview of existing applications of blockchain technology in the food sector	17
5	Comparison of functionality of traditional vs. blockchain-based traceability systems	19
6	Cost, benefits, and practical considerations relating to blockchain-based systems	23
6.1	Food product supply chains in general	23
6.2	Seafood supply chain example	24
6.3	Norwegian seafood trust example	28
6.3.1	Kvarøy Arctic experience of IBM food trust	30
6.4	How authorities may use data recorded in a blockchain-enabled system	31
7	Conclusions and recommendations	33
8	References	34

1 Background

Blockchain technology has existed since 2008 and it is expected that this technology will disrupt many traditional business sectors and models, in particular those that are virtual in nature; online banking is one such example. Blockchain technology will definitely have relevant applications also in the food industry, but there is no doubt that blockchain suppliers are currently overselling their products and promising more than they can deliver. This report aims to disentangle hype from truth when it comes to the capability of blockchain technology to achieve traceability in food supply chains and analyses two broad themes:

- 1) How does blockchain compare and contrast with alternative technologies and methodologies to achieve a similar outcome and what are the key selection criteria for deciding which technology to adopt?
- 2) What are the cost benefits and practical considerations of blockchain as applied to the food industry?

Section 2 explains the methodology followed by this study and Section 3 defines the core concepts used here. Section 4 gives an overview of providers of blockchain technology and briefly describes various applications of the blockchain technology in the food sector. Section 5 compares the functionality of traditional vs. blockchain-based traceability systems and examples of costs, benefits, and practical considerations in seafood supply chains and for authorities are presented in Section 6. Conclusions and recommendations are made in Section 7.

2 Methodology

This study employed a methodology that involved the conceptualization of key terms (Section 3) and a literature review of the application of blockchain technology in the food sector (Section 4). The conceptualisation of terms related to food traceability and electronic traceability systems was based on relevant scientific publications and reports in this area, in particular general publications that focused on defining terms and concepts. The conceptualisation of terms related to blockchain and blockchain technology was partly based on relevant scientific publications and reports in this area, and partly on online articles, white papers, and expert user opinions. This study is limited to application of blockchain technology in the (food) production industry and, as such, it does not analyse other possible applications of blockchain technology, of which there are many. The conceptualisation, and the subsequent literature review, forms the basis for the comparison of the functionality of traditional vs. blockchain-based traceability systems (Section 5) and the analysis of costs, benefits, and practical considerations relating to the use of blockchain technology in seafood sectors and for authorities (Section 6).

3 Conceptual framework

3.1 Traceability and traceability systems

The following constitutes a short, and by no means exhaustive, primer on traceability terms and concepts. The terms and concepts outlined are the ones needed for comparing a traceability system based on blockchain technology with a traditional electronic traceability system.

3.1.1 Traceability concept, terms, and definitions

There are numerous definitions of traceability, most of them recursive in that they define traceability as “the ability to trace” without defining exactly what “trace” means in this context. An attempt to merge the best parts of various existing definitions while avoiding recursion and ambiguity was made by two of the authors of this report (Olsen & Borit, 2013):

Traceability

- The ability to access any or all information relating to that which is under consideration, throughout its entire life cycle, by means of recorded identifications

This emphasises that any information can be traced, that traceability applies to any sort of object or item in any part of the life cycle, and that recorded identifications need to be involved. “That which is under consideration” is normally a batch (i.e. a unit of food or material used or produced by a food business operator (FBO)) or a trade unit (i.e. a unit of food or material sold by one partner, transported to, and received by another FBO). In scientific literature, the common term for “that which is under consideration” is a Traceable Resource Unit (TRU) (Kim *et al.*, 1999). The TRU is then “the unit that we want to trace” or “the unit that we record information on in our traceability system”.

Internal traceability is the traceability within a link or a company. Internal traceability is the backbone of traceability in general; everything else depends on each company in the chain having good systems and good practices when it comes to recording all the relevant internal information. Chain traceability is the traceability between links and companies, and it depends on the data recorded in the internal traceability system being transmitted, and then read and understood in the next link in the chain. For an illustration of the relationship between internal traceability and chain traceability, see Figure 1.

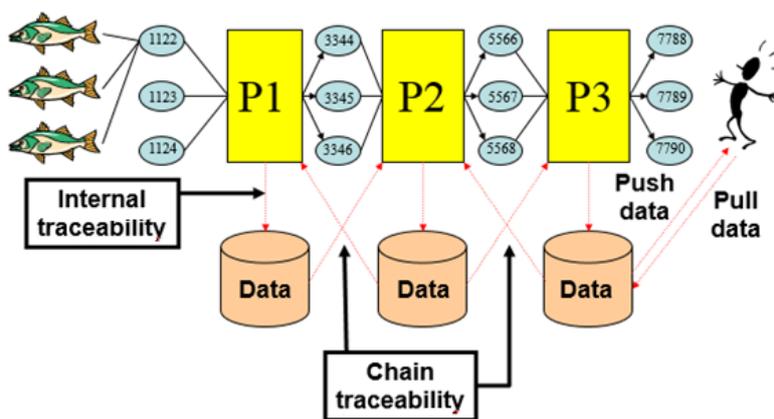


Figure 1 Internal versus chain traceability (TraceFood 2008)

3.1.2 Traceability systems and their components

For traceability, we want to “access any or all information relating to that which is under consideration”, so this means that the information recorded in the first link of the chain must somehow be made available in (or transported to) the next link of the chain. This is what the traceability system does; it makes sure that the recorded information is made available elsewhere and it is not lost. This means that if we want to describe or analyse the properties of a traceability system, we need to distinguish clearly between the following component types:

- The systems and processes that relate to the identification of the TRUs, which includes choosing a code, deciding on uniqueness and granularity of the code, and selecting how to associate the identifier with the TRU.
- The systems and processes that relate to the documentation of the transformations in the chain, which includes recording of the TRU transformations¹, the weights or percentages, and the related metadata.
- The recording of the attributes of the TRU, which can basically be anything that describes the TRU (e.g. attributes of the producing FBO, origin of the TRU, description of the TRU, measurements taken on the TRU, process parameters recorded when the TRU was produced etc).

The components of a traceability system are illustrated in Figure 2.

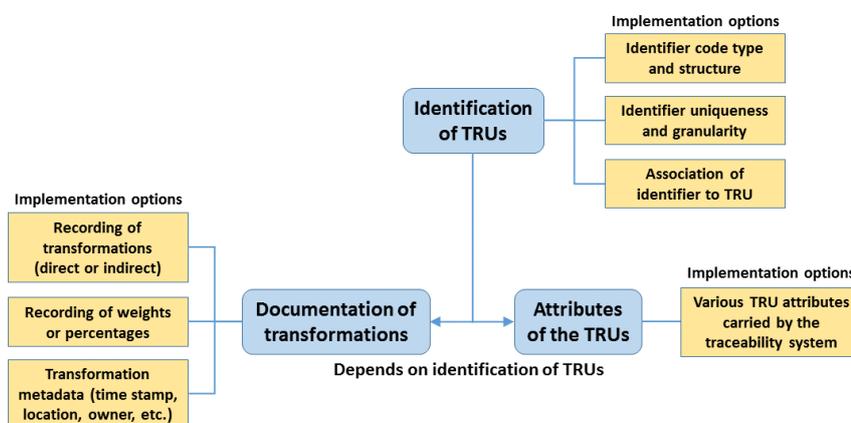


Figure 2 The components of a traceability system (Olsen & Borit, 2018)

¹ A transformation is an instant or a duration of time where, at a given location, a process uses a set of inputs (TRUs) to generate outputs (new TRUs).

3.1.3 Drivers of traceability systems

Different purposes/drivers for implementing a traceability system trigger different expectations in producers and consumers that do not always correspond to the traceability system in use. Table 1 summarises different characteristics of traceability systems, including drivers for implementing these.

Table 1 Traceability systems: purpose/driver, objective, attributes, standard and example (Borit & Olsen, 2016).

Purpose/Driver	Objective	Attributes	Standard	Example
Safety	Consumer protection (through recall and withdrawal)	Specified in food & fish safety regulations	Mandatory	EU regulation
			Voluntary (1)	US regulation
Security	Prevention of criminal actions (through verifiable identification and deterrence)	Specified in security regulations Verification of selected attributes on package and/or food	Regulatory (2)	US Prevention of Bio-terrorism, regulation
			Voluntary (no common standard)	Brand & product protection
Regulatory quality	Consumer assurance (through recall and withdrawal)	Specific attributes included in regulations	Regulatory (3)	EC labelling, mandatory consumer information.
Non-regulatory quality & marketing	Creation and maintenance of credence attributes	Specific attributes included in public standards	Voluntary (common standard) (4)	Public Quality seals (e.g. Label Rouge, France) Organic fish, Eco-labelling
Food chain trade & logistics management	Food chain uniformity & improved logistics	Specific attributes required to food and services suppliers by contract	Private standards (4)	Own traceability systems (e.g. Wal- Mart)
			Public standards for encoding information	EAN.UCC 128 (5), (e.g. with TRACEFISH (6) standard) SSCC (7)
Plant Management	Productivity improvement and costs reduction	Internal logistics and link to specific attributes	Voluntary (internal traceability; own or public standards)	From simple to complex IT systems.
Documentation of sustainability	Natural resource sustainability	Specified in environmental protection regulations	Mandatory	EU IUU Regulation
			Voluntary	FAO IPOA-IUU (8)

- 1) Recall and withdrawal can become compulsory if a responsible company does not take action.
- 2) Includes the possibility of mandatory disposal, recall and withdrawal, legal and police actions but primary purpose is prevention.
- 3) Includes the possibility of mandatory disposal, recall and withdrawal and administrative actions, but primary purpose is consumer assurance.
- 4) Could include voluntary (contractual) recall and withdrawal and agreed (contractual) sanctions.
- 5) GS1 System standardizes bar codes (www.GS1.com)
- 6) TRACEFISH, "Traceability of Fish Products" (EC funded project) <http://www.tracefish.org/>
- 7) SSCC: Serial Shipping Container Code (UCC)
- 8) IPOA-IUU: I International Plan of Action to Prevent, Deter and Eliminate Illegal, Unreported, and Unregulated fishing

3.1.4 Traceability and analytical methods

An important realisation is that what is recorded in a traceability system are (largely unsubstantiated) claims about the food product in question, and that these claims might not be true, either because of errors or because of deliberate fraud. There are methods and instruments for testing the veracity of claims related to biochemical food properties and these claims are particularly relevant because of the potential food safety implications if an erroneous claim is made. These methods include DNA-based analyses, stable isotope and trace element analyses, analysis of lipid profiles, high-performance liquid chromatography (HPLC), gas chromatography-mass spectrometry (GC-MS), nuclear magnetic resonance (NMR) spectroscopy, near-infrared (NIR) spectroscopy, metabolite profiling, chemical profiling, proteomics, and many more. Collectively these methods are referred to as “analytical methods”. What they have in common is that they analyse a food item sample and conclude with respect to the value of one, or a set of biochemical food item properties. Properties that to some degree can be verified by analytical methods include species, geographical origin (broadly), process status (e.g. fresh or frozen), presence of additives, some aspects of organic production, remaining shelf life, and some others, depending on the type of food item. While the list of food item properties that can be verified analytically is extensive and growing as the methods and technologies improve, it is worth noting that this is only a small subset of the properties recorded in a traceability system. Analytical methods cannot tell you who the owner of the TRU is, or the name of the farm or farmer, or the route the TRU took in the supply chain, or whether the production was ethical or fair trade, or similar. While practitioners and publications sometimes refer to these types of methods as “methods for traceability”, that is inaccurate, at least in relation to most definitions of traceability (including the one chosen here), because they do not deal with “recorded identifications”. What these methods can be used for is to verify some of the claims in the traceability system. It is important to keep in mind that a traceability system is made up of statements that are claimed to be true, but we do not know for sure that they actually are true, so that is something we need to check.

This means that analytical methods are very important when we are dealing with traceability, but these methods do not in themselves provide traceability. What they do provide is a way of verifying most of the claims relating to biochemical attributes of the food item in question. While these claims are only a subset of the total number of claims in a traceability system, they are among the most important ones, because if there is a food safety problem related to a food item, it will be detectable through application of analytical methods, and food safety, as we have seen, is a strong driver for implementing a traceability system.

3.1.5 Traceability and chain of custody

“Chain of custody” (CoC) is a term related to — , and sometimes confused with traceability, and in this report it is useful to clarify the distinction between the terms. CoC encompasses the responsibility for, and control of inputs and outputs as they move through each step in the relevant supply chain, and a chain of custody system is the set of measures designed to implement a CoC, including documentation of the measures taken. There are several different models for implementing CoC systems, including identity preserved, segregation, and mass balance, but to describe each of these is beyond the scope of this study. The main differences between traceability and CoC are summarised in Table 2.

Table 2 Main differences between traceability and chain of custody (CoC) (after (Borit & Olsen, 2016))

	Traceability	Chain of custody (CoC)
Objective	To associate recorded data with TRUs; to document what happens	To prevent mixing that violates the CoC requirements; to document that no such mixing has occurred
Of what?	Anything	With respect to some particular property which the CoC is in relation to, often origin or ecolabel status
The traced unit	A batch or a trade unit (the TRU)	The units with the same CoC identifier
Mix/join units	Yes, but must be documented	Only the units with the same CoC identifier
After mix/join	New unit and new identifier created	Considered same unit and receiving the same CoC identifier

3.1.6 Traceability and transparency

Being directly linked to trust building among stakeholders, transparency is a critical element in risk communication (Hofstede, 2004; Renn, 2008). Transparency of a supply chain is the degree of shared understanding of —, and access to product-related information as requested by a supply chain's stakeholders without loss, noise, delay, or distortion (Hofstede, 2004). Nevertheless, transparency and traceability are not the same thing, because the latter only sets the framework for the former (Egels-Zandén *et al.*, 2014). A good traceability system can provide product-related information to stakeholders with little loss, noise or delay, but when it comes to distortion one has to remember that a traceability system basically contains mostly unverified claims, and if we want transparency, we also need some mechanisms for verifying the data (see Section 3.1.4). A traceability system can provide a coherent overview of all the raw materials, ingredients, transformations, processes, and products in the supply chain and one cannot really have transparency without traceability, but for transparency some other components are needed as well. While the concept of traceability is quite generic and could be summarised as “keep a record of what you are doing in the chain”, transparency has a specific application and target audience in mind (e.g. general public vs. decision-makers).

3.2 Blockchain and blockchain technology

3.2.1 Blockchain definition

A blockchain is type of database that contains a digital recording of the history of some transactions. While databases and database systems come in a wide variety of structures and architectures, the blockchain data structure is more narrowly defined and blockchain systems have several features that set them apart from traditional digital ledgers or relational databases. Blockchain systems are normally distributed across a network of computers, thus not centrally managed, and the transactions within a blockchain are shared among all the participants of the blockchain network. The transactions are checked and validated through a consensus mechanism before they become part of the blockchain, and consensus is required so all the blockchain participants agree on the ‘truth’ of the blockchain, that is, the blockchain that contains all the valid and executed transactions. By linking transactions cryptographically to previous transactions, data immutability is secured; meaning that changing or tampering with the data becomes (practically) impossible. One of the main advantages of a blockchain is that transactions can be traced back all the way to the start of the blockchain, so that it can provide info of an asset on the blockchain and inform how this asset has originated and changed over time. Figure 3 shows a graphical representation of how a blockchain system can work; from creating a transaction, to validating that transaction, to finally appending the transaction to the blockchain.

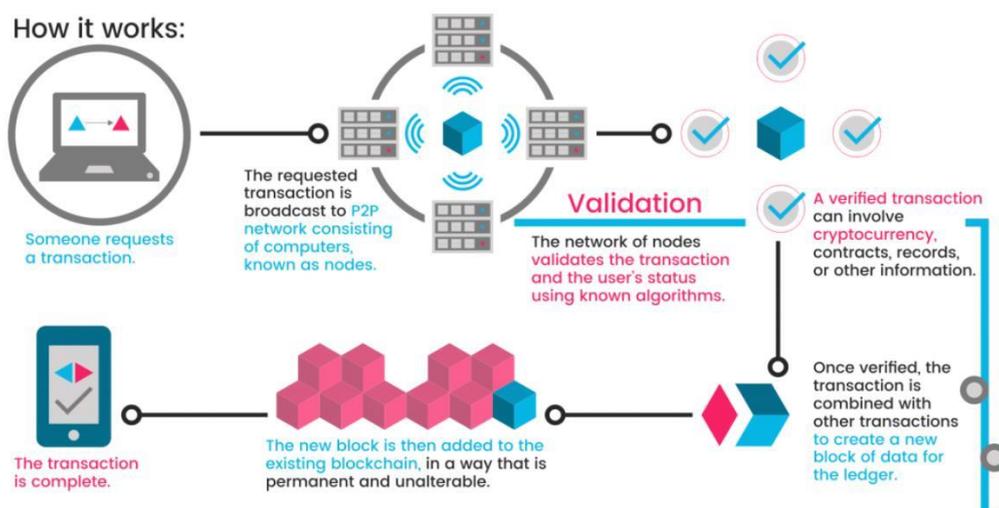


Figure 3 Graphical representation of a blockchain system (Blasetti, 2017).

Normally, blockchain implementations are based on five basic principles that underly its technology (Lansiti & Lakhani, 2017), see list below. However, while the blockchain technology is typically viewed from the perspective of a public blockchain — and commonly tied to its use in cryptocurrencies — it does not mean that the blockchain technology is exclusively tied to the characteristics found in such systems.

1) Distributed database

- a) Each user in the network has access to the full database and all its transactions.
- b) No single user controls the database.
- c) Every user can verify the transactions directly.

2) Peer-to-peer transmission

- a) Communications between users in the blockchain happens directly without the use of an intermediary.
- b) Each user stores and broadcasts information to the full network.

3) Transparency with pseudo-anonymity

- a) Every transaction on the blockchain is visible to anyone who has access to the blockchain.
- b) Each user has a unique address (typically a public-key) that identifies them.
- c) Users can be anonymous or can choose to reveal their identity.
- d) Transactions occur between user addresses.

4) Irreversibility of records

- a) Once a transaction is stored into the blockchain it cannot be altered.
- b) Transactions within blocks are linked to other blocks.
- c) Algorithms are used to make sure transactions are recorded permanently, are chronologically ordered, and are available to all users on the network.

5) Computational logic

- a) Blockchain transactions can be tied to computational logic and can thus programmed.
- b) Users can set up algorithms to trigger transactions between nodes.

Care should be taken when looking at the usability and applicability of the blockchain technology. In many cases, the advantages of the blockchain technology are almost always linked to public blockchains, such as found within the bitcoin cryptocurrency blockchain. The blockchain technology, as proposed by Satoshi Nakamoto (Nakamoto, 2008) (the inventor of the bitcoin cryptocurrency), is an open source technology. Anyone can fork the code and alter it according to his or her own use case. For instance, developing a blockchain technology for a restricted set of users would change the technology into a more centralised ledger system. Since the inception of blockchain, one of the core promises of blockchain technology has been decentralisation. However, as the technology matures many have come to acknowledge that there must be trade-offs in practice—even calling decentralisation a myth. No business can be fully centralised or decentralised without compromising in another area such as security, privacy, performance or scalability. This is an important consideration when determining the best blockchain approach for any use case. Understanding the differences between public and private blockchains is crucial to understanding the kind of trade-offs necessary to consider when developing a blockchain solution.

3.2.2 Blockchain characteristics

Blockchain implementations normally have the following four main characteristics: decentralisation, persistency, anonymity, and auditability (Zheng *et al.*, 2017; Wang *et al.*, 2018).

Decentralisation

In a traditional centralised transaction system, each transaction needs to be validated by a central trusted agency, such as a bank. Validation is required to make sure transactions are authenticated. This validation process can result in cost and performance bottlenecks at the central servers. With blockchain technology, transactions within the blockchain network can be performed between two users without the need for authentication by a single central authority or agent. In doing so, blockchain can reduce the server costs and mitigate the performance bottlenecks at the central server.

Persistency

Each transaction that is broadcasted throughout the blockchain network needs to be confirmed and recorded in blocks that will then be distributed to the whole network. As a result, any node in the blockchain network will have a copy of the blockchain. This also means that any node will validate the block and check the validity of the transactions it contains, making tampering of the data (nearly) impossible. Falsification of data, in terms of inconsistencies with existing blocks, can easily be detected.

Anonymity

Users interact with the blockchain network by using a generated address. This address is completely removed from a physical address, or an address tied to a specific user account. Blockchain users can, effortlessly, create a multitude of accounts, avoiding any form of identifying exposure. A high degree of privacy is achieved when creating blockchain transactions, although a perfect privacy preservation has been shown to not be possible. For instance, public keys, transactions, and therefore balances are visible to the whole network resulting in some form of identity detection (see (Meiklejohn *et al.*, 2013; Kosba *et al.*, 2016)).

Auditability

All transactions on the blockchain are validated and recorded with a timestamp. This makes it possible to check the veracity of previous records and verify existing ones as the history of transactions all the way up to the genesis block (first block of transactions) are maintained and accessible. This characteristic of the blockchain improves traceability and transparency of the data stored in the blockchain by ensuring that information once recorded is never overwritten or lost.

3.2.3 Blockchain types

Public vs. private vs. consortium/federated blockchain architecture

General considerations

Currently, the blockchain system can be categorised into three types: (1) public blockchain, (2) private blockchain, and (3) consortium or federated blockchain (sometimes also referred to as hybrid blockchains). This section describes some differences between the three types of blockchains from a more general perspective.

Public blockchains

Public blockchain are open source and not permissioned. This means that anyone can download the public blockchain technology and start running a public node on his or her local device, validate transactions within the network, and participate in the consensus process (the process of creating new blocks that are then added to the blockchain) without permission. Anyone can also send transactions to the blockchain network, and if valid, can see them stored permanently in the blockchain. In addition, anyone can read the transactions listed on the blockchain, for instance with a public block explorer. Typically, these transactions are anonymous or pseudo-anonymous.

Examples of public blockchains are Bitcoin (bitcoin.org), Ethereum (ethereum.org), Monero (monero.org), Dash (dash.org), Litecoin (litecoin.org), and Dogecoin (dogecoin.com). Public blockchain technology has the potential to disrupt current business models through disintermediation. In addition, there is no need to maintain servers or system admins, which radically reduces the costs of creating and running decentralised applications.

Consortium or federated blockchains

Consortium or federated blockchains are typically managed by a group of people, entities, or trusted authorities. In essence, joining the blockchain network is restricted and it is only granted to a selected set of nodes. This is one of the main differences when comparing it to a public blockchain, where any person with access to the Internet can participate in the process of verifying transactions and creating new blocks. Consortium blockchains are faster (higher scalability) and provide more transaction privacy. Such blockchain types are typically used in the banking sector. The consensus process is controlled by a pre-selected set of nodes; for example, one might imagine a consortium of 15 financial institutions, each of which operates a node and of which 10 must sign every block in order for the block to be valid. The right to read the blockchain may be public or restricted to the participants.

Examples of consortium blockchain are R3 (Banks), EWF (Energy), B3i (Insurance), and Corda. Successful implementations of consortium blockchains can reduce transaction costs, reduce data redundancies, replace legacy systems, simplify document handling, and create full compliance mechanisms. There is still debate whether consortium blockchains systems can actually be defined as a blockchain.

Private blockchains

A private blockchain is regarded as a centralised network since it is fully controlled by one organisation. With private blockchains, write permission to the blockchain is commonly kept centralised to one organisation. Reading the blockchain may be (partly) public or restricted to a selected few; for example, by being invited to join the network or having granted access. A private blockchain is almost always a permissioned blockchain. Private blockchains are thus highly restricted. The access control mechanism can vary, for instance, existing participants can invite new members, a regulatory authority can issue a license to participate, or a group of members can make such decisions. Private blockchains are a way of taking advantage of blockchain technology by setting up groups and participants who can verify

transactions internally. In contrast to public blockchains, members who control the blockchain are at risk for security breaches, similar to a centralised system. Private blockchains have their uses in scalability, state compliance of data privacy rules, and other regulatory issues. Examples of private blockchains are MONAX and Multichain. Private blockchains, similar to consortium blockchains, are argued not to be proper blockchains.

Comparison of the blockchain types

The three types of blockchains are compared here based on six criteria: consensus determination, read permission, immutability, efficiency, centralisation, and consensus process.

Consensus determination

Consensus determination relates to the validation of a new block—including all its transactions—and demonstrates to the blockchain network that some form of block validation has been established. A consensus is required to allow the full network to accept the new block and its transactions into the blockchain, and it creates a starting point from where subsequent new blocks can build upon. In a public blockchain, each node could take part in the consensus process, there is no entry requirement to mine blocks. Within a consortium blockchain, only a selected set of nodes are responsible for validating new blocks, typically nodes that have been granted some form of authority or trust. Within private blockchains, one organisation or trusted authority is fully responsible for validating the blocks and the underlying consensus mechanism.

Read permission

Read permission relates to the visibility of the transactions within the blockchain. Within a public blockchain, anyone can view the transactions; from the first all the way up to the latest. There is no restriction in terms of reading the transactions. However, with private or consortium blockchains, the read permission is regulated and can be constructed in a variety of ways. For instance, only some transactions are visible to everyone or some transactions are visible to some users. Read permissions are up to the trusted authorities who maintain the blockchain.

Immutability

Immutability relates to the ability of transactions or values within the blockchain being altered or tampered with. For example, a value x of transaction y in block z will be changed to a different value. The public blockchain technology is often characterised for its high degree of immutability since transactions are stored in different nodes in the distributed network, which makes it nearly impossible to tamper with a public blockchain. One of the current trends in mining blocks within a public blockchain, for example with the bitcoin cryptocurrency blockchain, is that miners join their computational power in mining pools, which, when they have more than 51% of the computational power of the network, could potentially endanger the immutability of the whole blockchain network. For private and consortium blockchains, immutability is low since the majority of block validators can easily reverse or tamper with the blockchain if they choose to do so.

Efficiency

Efficiency relates to the handling of transactions and blocks within the blockchain network, or simply put, how the flow of data propagates throughout the network. Within a public blockchain, the propagation or broadcasting of transactions and blocks takes more time, typically because there are more nodes in the network. When taking network safety into consideration, restrictions on public blockchain would be much more strict. As a result, transaction throughput is limited and the latency is high. Within consortium and private blockchains, the small number of validators could make data propagation more efficient.

Degree of centralisation

A centralised network relates to control that is carried out by a single entity, for instance, a trusted party. The main difference between the three types of blockchain types is that a public blockchain is fully decentralised; meaning that no single authority handles or controls the blockchain network. The consortium blockchain is partially centralised and private blockchain is fully centralised as it is controlled by a single group.

Consensus process

The consensus process relates to the process whereby new blocks and its transactions are validated and are appended to the existing blockchain. This 'new' validated block becomes the starting point from where subsequent new validated blocks will be linked to. The validation process is the consensus process, and the mechanisms behind the process itself can take on many variations, which will be described later on. Within a public blockchain, anyone can join the consensus process and start validating blocks. There is no entry requirement other than hardware to be able to execute the validation mechanism (such as solving computational puzzles). In contrast, with a consortium and private blockchain, participating in the consensus process is restricted; a permission is required to join the process. Since the consensus process determines what new transactions are being entered into the blockchain, within a private and consortium blockchain, typically a validation node needs to be certified to take part in this process.

A summary of the three blockchain types with their six characteristics is given Table 3.

Table 3 Overview of blockchain types

	Public	Consortium/Federated	Private
Consensus determination	everyone	selected (few)	single authority
Read permission	public	public, partly public, restricted	public, partly public, restricted
Immutability	nearly impossible	possible with majority of validators	possible
Efficiency	low	high	high
Centralised	no	partially	yes
Consensus process	permissionless	permissioned	permissioned

It is important to note that when choosing a specific type of blockchain it does not necessarily mean that one is better than the other. In other words, what might work for one might not necessarily work for another. The implementation of the blockchain type is highly case dependent. Presently, there are no real standards to measure the quality of the blockchain against, which would also mean that relying on the blockchain vendor's pros and cons might not necessarily paint the right picture. Other criteria not mentioned above might include governance, trust, and resources aspects of the blockchain. In essence, the choice for a type of blockchain would for a large part depend on (1) who is allowed to participate in the blockchain network and execute the consensus protocol, and (2) who is able to view of the content of the blockchain, such as the transactions.

3.2.4 Permissioned vs. permissionless

Permissionless

A permissionless blockchain is a blockchain where no permission is required to read the blockchain, to make transactions to the blockchain, and to validate or mine blocks. A permissionless blockchain can also be viewed as a public blockchain, with the Bitcoin blockchain network being the most popular example. A major advantage of a permissionless (or public/open) blockchain network is that guarding

against bad actors is not required and no access control is needed. This means that applications can be added to the network without the approval or trust of others, using the blockchain as a transport layer.

Permissioned

Permissioned blockchains are blockchains where a permission is required to join the blockchain, to have a copy of the blockchain, and in some cases, to be able to validate blocks. Examples of permissioned blockchains are for instance Hyperledger and R3 Corda. Permissioned blockchains use an access control layer to govern who has access to the network. In contrast to public blockchain networks, validators on private blockchain networks are trusted parties chosen by the network owner. There are no anonymous nodes that validate transactions nor nodes that receive mining rewards. Permissioned blockchains do rely on a consensus mechanism to make sure new blocks on the blockchain are validated and that there exists only one version of the truth. The consensus protocol comprises of three basic steps: (1) determine whether to accept or reject a transaction, (2) sort all transactions within a time period into a sequence, and (3) verify and save into the blockchain. Permissioned blockchains are also called consortium, federated or hybrid blockchains.

Comparison between permissioned and permissionless blockchain types

The comparison between permissioned and permissionless blockchain types in relation to public and private blockchain is depicted in Table 4.

Table 4 Overview of characteristics between permissionless/permissioned and public/private blockchains. Adapted from (Carson et al., 2018).

	Permissionless	Permissioned
Public	<ul style="list-style-type: none"> • Anyone can join, read, write and commit • Hosted on public servers • Anonymous, highly resilient • Low scalability 	<ul style="list-style-type: none"> • Anyone can join and read • Only authorised and known participants can write and commit • Medium scalability
Private	<ul style="list-style-type: none"> • Only authorised participants can join, read, and write • Hosted on private servers • High scalability 	<ul style="list-style-type: none"> • Only authorised participants can join and read • Only the network operator can write and commit • Very high scalability

3.2.5 Blockchain infrastructure

Besides the investments made into setting up or developing the blockchain system, there are very few additional hardware investments to make that would enable information to be stored onto the blockchain. Where one would store the information in a digital database, ledger, or supply chain system, one can now store their information directly (e.g. application programming interfaces) or indirectly (e.g. web interface) on the blockchain. Besides manual entering data into the system, scanners or other electronic reading devices can be used.

Data connector application programming interfaces (APIs) allow companies to efficiently upload supply chain data from existing data stores (such as SAP) to their blockchain system for seamless integration of data from enterprise systems to blockchain solutions. Organisations that do not work with enterprise software can enter data through web interfaces.

3.2.6 Blockchain and transparency

By using blockchain technology, the digital ledger can become more transparent (Nugent *et al.*, 2016; Abeyratne & Monfared, 2016; Underwood, 2016; Wust & Gervais, 2018). Since the blockchain, especially in public blockchain types, are distributed, all network participants have a copy of the same blockchain (i.e. digital ledger). Any new update to the blockchain is governed by a consensus

mechanism, which enables a high degree of immutability, and results in everyone having the same copy of the blockchain—resulting in a high degree of shared understanding. In other words, the participants within the blockchain network agree on a single truth of the blockchain and no single participant can make changes or tamper with transactions in the blockchain. This decentralised characteristic of the blockchain creates a high degree of transparency.

However, blockchain technology is not limited to being just decentralised as the centralised or private blockchains also have some advantages for corporations over the public ones. Private blockchains are useful for corporations who want to use the power of decentralised ledgers to improve the ongoing function. From a technical perspective, centralised and decentralised blockchain types are very similar. In both cases, the network consists of nodes responsible for storing and securing the digital ledger, and they require a consensus mechanism to establish a single ledger.

The biggest difference between centralised and decentralised, or public and private, is the number of nodes that participate in the network and make changes to the network (i.e. create new blocks). In the Bitcoin public blockchain case, there are no barriers to entry when it comes to accessing the ledger and taking part in the consensus mechanism to create new blocks. In contrast, in consortium or private blockchains (e.g. IBM's Hyperledger Fabric), typically the organisation deploying the blockchain controls many aspects of the blockchain, including participation and access. Thus, the advantage of centralised blockchains is that it offers more customisability and control over the network, resulting in less resources necessary to secure the network, making them essentially more environmentally friendly. At the same time, since the organisation deploying the blockchain can choose what hardware the network runs on, they can typically achieve higher overall throughput.

A disadvantage of centralised blockchain systems is that they are less secure, since there is not as much computing power securing the network as compared to (public) decentralised blockchains. It only requires a few of the nodes hosting the network to collude by amassing enough resources to hack the network. This can cause the blockchain to be less transparent, since the degree of shared understanding can more easily be tampered with. This is even worse when the blockchain network is fully centralised, thus managed by a single organisation or entity.

Within a public blockchain, all the information stored within blocks is publicly visible to anyone. This can be made clear by illustrating it with the Bitcoin public blockchain. Public blockchains typically have an explorer; an online chain browser that displays the content of individual blocks, accounts, balances of addressees, and transactions. Bitcoin has many explorers, for instance, BlockExplorer (blockexplorer.com) or Block Explorer (blockchain.com/explorer), which can be utilised to find information of particular blocks and its content. For example, each block contains a summary of when it was created, the reference (i.e. hash) to the previous block, the solution to the cryptographic puzzle, who mined the block and other information. In addition, the transactions are listed that show from which account to which other account Bitcoins were transferred and the amount. Every transaction and every created block since the first genesis block are publicly available and fully transparent. However, account holders are listed by their public key addresses (which is also utilised to digitally sign a transaction), which do not reveal the identity of the individual. This, in the case of Bitcoin, makes the blockchain have a high degree of traceability on the one hand side, but are still private on the other hand. In contrast, the transactions (or any other type of data) within consortium and private blockchains are commonly not completely visible to the public. Depending on the implementation, the information stored on the blockchain can be fully, partly, or not viewable by the public. Verifying the authenticity of the transaction for an outside party becomes harder. Also since private ledgers commonly are not available for public use, they are of little use to anyone besides the corporations that deploy them. Transparency of the transactions is thus lower in such types of blockchains compared to fully public blockchains.

An inherent trade-off exists between privacy and transparency within blockchain technology. When the blockchain is fully transparent—in terms of the transactions on the blockchain—anyone can view information stored on the blockchain and by whom that information was added; meaning that no privacy is provided. Likewise, a fully private system provides no transparency. However, a system can still provide significant privacy-guarantees while making the process of state transitions transparent, e.g. a distributed ledger can provide public verifiability of its overall state without leaking information about the state of each individual participant (Wust & Gervais, 2018). To achieve privacy in a public system, techniques of cryptography can be utilised. However, using cryptography comes at a cost of lower efficiency. The cryptocurrency Zerocash (zerocash-project.org) for example makes use of computationally expensive cryptography to provide full anonymity while still providing sufficient transparency to publicly verify the ledger state.

4 Application of blockchain technology in the food sector

4.1 Overview of providers of blockchain technology

The blockchain technology is open source and free to use, adjust, and extend in any way. The downside of adopting the original source code is that a successful implementation of the blockchain depends on a full understanding of the underlying code base. However, such implementations provide the most degrees of freedom, as every aspect of the blockchain can be tailored towards the specific use case. During recent years, there is a wide array of approaches to implementing a blockchain technology. Many players have emerged, each with their own merits, and a couple of implementation types are listed below.

Blockchain as a Service (BaaS)

The Blockchain as a Service (BaaS) concept can be mapped to the definition of 'Software as a Service' (SaaS), which is a software distribution model in which a third-party hosts an application and offers the application's functionality (i.e. service) through the Internet. Typical examples of SaaS solutions are Google Apps, Dropbox, Salesforce, and Cisco WebEx. This type of service is sometimes called 'on-demand software'. A subscription or registration is typically needed to make use of the functionality or service. Other variants are, for example, platform as a service (PaaS) and Infrastructure as a Service (IaaS). Blockchain as a service follows the same ideology, and it prevents users from developing blockchain systems from scratch.

Some of the big cloud providers such as Amazon (with AWS), Microsoft (with Azure), and IBM (with BlueMix) are starting to offer blockchain as a service on their cloud platforms. Users adopting BaaS solutions will benefit from not having to deal with the problems concerning configuration, setting up a working blockchain, and not needing hardware investments.

Amazon AWS blockchain solutions:

Amazon offers end-to-end BaaS solutions with a wide range of blockchain frameworks for developing blockchain applications. Examples of frameworks are Hyperledger Fabric, Hyperledger Sawtooth, Ethereum, and Corda. Amazon offers developers a one-click deploy of the underlying blockchain and connectivity to supplemental applications.

Microsoft Azure blockchain workbench:

Microsoft offers modular, pre-configured networks and infrastructure. Development of blockchains can be done by the blockchain workbench. The workbench is a collection of Azure services and capabilities designed to create and deploy blockchain applications to share business processes and data with other organisations. Microsoft provides the infrastructure scaffolding for building blockchain applications, allowing developers to focus on creating business logic and smart contracts. Other Azure services can easily be integrated. Examples of blockchain solutions offered are Corda, Ethereum, and Hyperledger Fabric. A solution architecture for supply chain track and trace is also offered.

IBM BlueMix Blockchain:

IBM offers BaaS on their BlueMix cloud platform. IBM blockchain solution and services are built on Hyperledger technologies which provide the framework and tool set. IBM claim to have successfully implemented over 400 blockchain solutions, and their best practices can be found in their enterprise ready blockchain services.

Blockchain first

A blockchain first implementation works directly with the blockchain tools and stack. A complete assembly is required, which makes this type of implementation difficult. The upside is that working

directly with the blockchain creates the most degrees of freedom, and allows for a high degree of innovation. Typically, new blockchain technology provider companies start building their solutions by working directly with the blockchain tools. Examples here include working with the original Bitcoin (github.com/bitcoin/bitcoin) and Ethereum (github.com/ethereum) source code available on Github.

Development platforms

Several development platforms exist that allow for fast development of a blockchain implementation. Such platforms focus not on a specific blockchain technology, but allow for rapid development with a strong focus on the blockchain programmability. Examples include, BlockApps (blockapps.net), Blockstream (blockstream.com), Monax (monax.io), Parity (parity.io), Hyperledger (hyperledger.org), and Tendermint (tendermint.com).

Vertical solutions

Vertical blockchain solutions are industry specific, and are based on private blockchain or ledger infrastructure. Some vertical blockchain solutions are arguably not a proper blockchain solution, but more a distributed ledger solution (which can be viewed as a subset of the blockchain technology). Examples include Axoni (axoni.com), Chain (chain.com), Clearmatics (clearmatics.com), Digital Asset Holdings (digitalasset.com), itBit (itbit.com), and R3 (r3.com).

APIs & Overlays

This approach uses the blockchain as an asset, ownership or identity-binding infrastructure, and it is typically used for a specific purpose, for example, ownership rights, title registries or other specific services with a built-in trust-based component. Examples include Blockstack (blockstack.org), Factom (factom.com), Open Assets (openassets.org), and Tierion (tierion.com).

4.2 Overview of existing applications of blockchain technology in the food sector

There are relatively many applications (test/trials) of blockchain in food chains, addressing specific issues (e.g. traceability) or sectors. However, there is a lack of common technology that can connect different blockchains (Ciaian, 2018). Most existing blockchain systems for traceability management have been developed since 2015 (Galvez *et al.*, 2018).

Table 5 Table 5 summarises some of the blockchain technology initiatives/projects in the agricultural and farming food-supply chain, together with the objective(s) of the implementation of this technology. For a summary of topics that have been addressed in current research on blockchain for agriculture, see (Bermeo-Almeida *et al.*, 2018).

Table 5 Selected applications of blockchain technology in the food-supply chain

Goods/Products	Initiative/Project/Company involved	Objectives
Agri-food	AgriOpenData (Galvez <i>et al.</i> 2018)	Allow quality and digital identity to be certified
Agri-food	Supply Chain Traceability System for China Based on RFID & Blockchain Technology (Galvez <i>et al.</i> 2018)	Trusted information throughout the agri-food supply chain
Beef	“Paddock to plate” project, BeefLedger; JD.com (Kamilaris <i>et al.</i> 2018)	Food traceability
Beer	Downstream (Kamilaris <i>et al.</i> 2018)	Food traceability
Chicken	Gogochicken; Grass Roots Farmers Cooperative; OriginTrail (Kamilaris <i>et al.</i> 2018); ZhongAn (Ciaian 2018)	Food traceability, food safety concerns of urban consumers
Coffee	FairChain coffee: Bext360 in partnership with Moyee Coffee (Ciaian 2018)	Traceability, transparency of the value added
Dairy	Blockchain-based food supply chain traceability: a case study in the dairy sector (Casino, Fran, <i>et al.</i> 2021)	Food traceability
Fish	Provenance (Galvez <i>et al.</i> 2018)	Auditable system
Fresh food	Ripe (Galvez <i>et al.</i> 2018)	Enabling data transparency and transfer from farm to fork
Fruits	FruitChains (Galvez <i>et al.</i> 2018)	Public, immutable, ordered ledger of records
Grains	AgriDigital (Kamilaris <i>et al.</i> 2018)	Financial
Large enterprises	IBM (Galvez <i>et al.</i> 2018)	Food tracking project
Mangoes	Walmart, Kroger, IBM (Kamilaris <i>et al.</i> 2018)	Food traceability
Olive oil	OlivaCoin (Ciaian 2018; Kamilaris <i>et al.</i> 2018)	Financial, Small farmers support
Orange juice	Alber Heijn & Refresco (International Supermarket News 2018)	Show customers how and by whom products are made
Pork	Walmart, Kroger, IBM (Kamilaris <i>et al.</i> 2018)	Food traceability
Pork	Arc-net (Galvez <i>et al.</i> 2018)	Brand protection and security through transparency
Scotch Whisky	CaskCoin (Ciaian 2018)	Investing in maturing Scotch Whisky
Seafood	The Blockchain Supply Chain Traceability Project (FAO 2019)	Tracking fish products from vessels to food shops
Seafood	Building trust and equity in marine conservation and fisheries supply chain management with blockchain. (Howson, P. 2020).	Trust and sustainability in the seafood supply chain
Soybean	HSBC & Cargill; ING & Louis Dreyfus Co. (Hochfelder 2018)	Help authenticate products as well as eliminate the "paper trail" of verification at every stage of the supply chain
Sugar cane	Coca-Cola (Kamilaris <i>et al.</i> 2018)	Humanistic
Turkeys	Cargill Inc., Hendrix Genetics (Ciaian 2018; Kamilaris <i>et al.</i> 2018)	Food traceability, animal welfare
Wine	Chainvine (Galvez <i>et al.</i> 2018), Winecoin (Ciaian 2018)	Increase performance, revenue, accountability, and security

5 Comparison of functionality of traditional vs. blockchain-based traceability systems

Consider the question “What is a steak dinner?”. Is it still a steak dinner if you serve fries instead of a baked potato? Is it still a steak dinner if you serve it with pepper sauce or bearnaise sauce? Is it still a steak dinner if you serve it on paper plates rather than on proper dinner plates? Most people would say yes to all these questions; it is still a steak dinner, even if you change the context and the serving options. You cannot, however, take away the steak; then you would no longer call it a steak dinner.

The challenge when analysing blockchain is that the term is traditionally associated with one, or a very limited set of “serving options”. A block is a just set of recorded transactions, and a blockchain is just a chain of such blocks, linked in way so that each block refers to the previous block in a way that makes it impossible to change any part of the previous block (or rather, it would be immediately discovered if you made a change). For a computer scientist, a blockchain is simply a data structure similar to a linked list, where hashes rather than pointers are used to refer to the previous link in the chain. This is the “steak” analogy; if you do not have this data structure, then what you have should not be called a blockchain.

What then are the “serving options”? Any article on this subject will tell you that blockchain implementations are online, distributed (multiple copies of the database / the blockchain exist), that there is a consensus mechanism to decide how to synchronise these multiple copies, and that there is a signing process which uses public and private keys to ensure identification and to enable encryption. This is all true for bitcoin, which, as previously indicated is a public blockchain, but is it necessarily true for all block chain implementations, including hybrid blockchains and private blockchains? The answer, at least in principle, is no; all these additional attributes traditionally assigned to blockchain implementations are just implementation choices. Other implementation choices could have been made, and the underlying data structure would still be a blockchain. A programmer on a standalone offline computer could write a blockchain implementation based on a single version of the blockchain, with no consensus mechanism needed, no signing process needed, and no encryption needed. In principle this should be called a blockchain, because the underlying data structure for the implementation as well as the data recorded would be identical to a (single copy of) an online public blockchain, implemented in the traditional way with a consensus mechanism, a signing mechanism, and encryption using public and private keys.

This is what makes it difficult to compare blockchain-based traceability system with a traditional electronic traceability system, which normally uses a relational database as the underlying data structure. Strictly speaking, the only difference between the two systems is the structure of the underlying database, and that means that while inherent differences between the implementations exist, these differences are fairly small and relate to the immutable, inherently consistent nature of the blockchain data structure. This is, however, not how blockchain implementations are usually described or analysed. Rather than comparing blockchain against non-blockchain implementations, most analyses compare online against offline implementations, or distributed against centralised, single copy implementations, or encrypted against non-encrypted signatures.

As an example, a statement that is repeated in many articles on applications of blockchain in the food industry is the following “*In a Walmart blockchain project, it took 2.2 seconds to trace mangoes to the farm. Without blockchain, this would take the retailer 6 days, 18 hours and 26 minutes to identify the original farm*” (Collak 2018). Let us accept the first statement, that using a traceability system based on blockchain technology it took 2.2 seconds to trace mangoes back to the farm. However, the second statement is clearly untrue, and cannot serve as a basis for evaluating the relevance of the blockchain solution. It might be true that in the (apparently very inefficient) previous traceability system it took more

than 6 days to trace the mangoes back to the farm, but that has nothing to do with the system being based on a relational database (or whatever kind of database) rather than blockchain; it is related to the change from fragmented, non-integrated, possibly partly manual data to online, distributed, harmonised, and connected data.

As part of the comparison of blockchain-based vs. traditional electronic food traceability systems, it is worth enumerating some of these “serving options” in Table 6.

Table 6 Attributes and implementation options for traditional vs. blockchain-based traceability systems

	Traditional electronic traceability system	Electronic traceability system based on blockchain technology
Underlying database	Relational database (usually)	Blockchain
Immutable database?	Possible by setting ‘append only’ flag on database, but very unusual	Yes
Single copy of database?	Normally, yes. Traditional databases often use client-server network architecture, where a single, master copy of the database is stored on a centralised server.	No, normally multiple copies (but strictly speaking this is an implementation option)
Consensus mechanism?	Needed if there are multiple copies of the database, unusual	Yes (but strictly speaking this is an implementation option)
Online? Cloud-based?	Not uncommon for large companies, and for modern chain traceability systems	Yes (but strictly speaking this is an implementation option)
User authentication	In a client-server implementation, the server authenticates a client’s credentials	Based on cryptography with private keys and public keys (but strictly speaking this is an implementation option)

So, what does this mean? Should we compare a blockchain implementation to a “bad” traditional traceability system, to an average one, or to one that is as similar to a blockchain implementation as possible, with all the same implementation options?

There is no clear answer to this question; it depends on what you want to measure, and it depends on what you want to achieve by making the comparison. If you want to argue for the desirability of blockchain solutions, you compare blockchain solutions to fairly bad traditional traceability systems, like in the Walmart example. A better approach is to analyse the attributes and implementation options separately and indicate pros and cons of each.

Suitability of database

A traditional database can store anything, and it is normally state-based, i.e. it stores the current state or value of the data. A blockchain stores transactions, and as transformations in a (food) supply chain are similar to transactions, the blockchain is well suited for storing data related to food (or product) traceability.

Data quality and veracity

Ensuring quality and veracity of recorded data is a significant challenge for both types of systems; there is a risk of ‘garbage in, garbage out’. Accidental errors in recorded data are likely to be equally frequent in the two types of systems. Deliberate fraud, however, is probably less likely (but certainly still possible) in a blockchain-based system, as the person committing the fraud will know that if fraud is discovered in a blockchain-based system, the provider of the fraudulent statement can be unambiguously and quickly identified, and this obviously increases the risk of being caught.

Immutability, integrity and transparency

In a traditional database, data elements can be overwritten, although it is not uncommon to keep a version log, indicating who did the overwriting, when, and where. The data recorded in a blockchain is immutable by design, which means that we know that recorded data has never been overwritten. Thus, a traditional database has no built-in integrity; it stores the latest recorded (or claimed) state of each data element independently. In a blockchain implementation, the state of each variable is not stored; instead all the transactions that led up to this state is stored. Using a feed silo as an example, in a traditional database the current amount and type of feed would be stored (probably also the previous feed transactions to and from the silo). In a blockchain implementation, the current amount of feed would not be stored; only the entire list of transactions to and from the silo. In a traditional database, the current feed level recorded in the database would be an unsubstantiated claim. In a blockchain implementation, the current feed level would be calculated by going through all the recorded transactions, thus providing more transparency and integrity to the stated feed level value.

Confidentiality

While a blockchain implementation, especially a private blockchain, can provide data confidentiality, that is not what it was designed for. In a blockchain implementation, confidentiality and tiered data access protocols are designed externally, and on an ad-hoc basis. Blockchain scores highly on transparency, and in this context transparency and confidentiality are to some degree mutually exclusive qualities; if you score well on one, you cannot really score well on the other.

Trust

Trust is not a trivial attribute to evaluate in this context, because the different implementations treat the concept of trust differently. In a traditional traceability system, you are asked to trust the owner of the system and the database, and if anything turns out to be wrong (false claims, food fraud etc.), the reputation of the owner of the database (and in practise, the brand) suffers. Blockchain was designed to work without trusting any particular organisation; the trust in the veracity of the data would be supplied by the design of the blockchain system. While this in itself is a useful attribute, it is not really how trust in the food sector works. To remove the need to trust any organisation and to democratise the responsibility for data veracity is relevant in a purely virtual system, but that is not what the food sector is. Brand owners will still need to be trusted, both to provide data, but most of all for producing safe, nutritious, and high-quality food. While using a blockchain-based system provides no disadvantage in relation to trust, the inherent blockchain quality of “not needing to trust any single organisation” is not really applicable in the food sector.

Speed and efficiency

Obviously, this integrity comes at a great cost. A blockchain implementation will always be slower than a traditional implementation, because in addition to supporting the functionality that a normal database supports (writing and reading data) it also needs to verify signatures/identities using cryptography, and it needs to execute a consensus algorithm to determine which blocks gets added to the blockchain during the next update. This is in addition to the inefficiency related to the built-in redundancy in the blockchain, where there are multiple copies of the database, and where all transactions since the creation of the blockchain is stored and accessed.

Robustness

The redundancy has an upside, which is robustness. Robustness is an indication of how sensitive the data and the database is to mistakes, errors, or incidents, including things like power-outs, hacking, server crashes and malfunctioning software or hardware. In a traditional system robustness is provided by external processes, and these may vary; significant amounts of data may be lost if something goes wrong and the protective measures are not in place. In a blockchain-based system, a degree of

robustness is inherent in the system, both for the state of the data, which can be recreated by traversing the recorded transactions, and for the database, which is normally online, and duplicated many times.

Interoperability

In principle, interoperability, i.e. how well different systems exchange information, could be seen as independent from the traditional/blockchain choice. In practice, however, this is not the case. As indicated above, a traditional electronic traceability system has a large number of implementation options, and the relational database can be structured in many different ways. At least for now, blockchain implementations are more homogenous, in that they all store transactions rather than data element values, they are all online, they are all immutable, they all employ cryptography for verifying identity etc. The fact that blockchain systems are more homogenous makes them more interoperable, and in fact many of the reported blockchain success stories are based on the improvement in operability and data sharing along the supply chain rather than on any of the blockchain attributes in itself. For traditional traceability systems to become (more) interoperable would depend on widespread adoption of standards both for Electronic Data Interchange (EDI) and for data content; unfortunately, there are too many competing standards in this area, so the current level of interoperability is fairly low. In this report, we highlight improved interoperability as the most important benefit of using a blockchain-based electronic traceability system in the food industry. This benefit is not, strictly speaking, based on any particular characteristic of the blockchain structure or database; it is based on the fact that interoperability between blockchain implementations are simpler, because blockchain implementations are more similar than traditional electronic traceability implementations which can be built on a wide range of operating principles, system architectures, and database types.

6 Cost, benefits, and practical considerations relating to blockchain-based systems

To evaluate costs, benefits, and to consider some practical considerations, we have evaluated how a blockchain-enabled food traceability system may be used in supply chains for food products in general, and in the supply chains for seafood. We have also indicated how authorities seeking to get access to food item properties and to verify the veracity of the associated claims may utilise a blockchain-based system.

6.1 Food product supply chains in general

Based on the evaluation criteria identified in the previous section, the overall comparison of a traditional traceability system with a blockchain-based system is indicated in Table 7. Grey colour indicates a disadvantage or an existing challenge, light blue colour indicates a small advantage for the system type in question, and deep blue colour indicates a significant advantage.

Table 7 Costs and benefits of blockchain-based systems in the food product supply chains in general

Comparison criteria	Traditional electronic traceability system	Electronic traceability system based on blockchain technology
Suitability of database	Records (claimed) variable states, versatile	Records transactions, well suited for recording transformations
Data quality and veracity	Data provider must check and vouch for data quality and veracity	Data provider must check and vouch for data quality and veracity, but fraud frequency may be lower, as risk of getting caught is higher
Immutability, integrity and transparency	Data elements can be overwritten; needs additional recording (transaction log or similar) to document this	Only the transactions are recorded, which means a higher level of integrity and transparency of the claimed values
Confidentiality	Easy to integrate tiered levels of access	Can be done, but to some degree it goes against the philosophy of what a blockchain implementation is meant to support
Trust	Based on trust in the food business and the brand	Still based on trust in the food business and the brand, but trust may be higher because of higher degree of data integrity and transparency
Robustness	Duplication, back-up, and other means of providing robustness must be provided by external processes	Robustness and duplication of data is built into the system
Speed and efficiency	As good as you can get	Significant overhead related to duplication, error checking, consensus mechanisms, and calculating the state of variables based on transactions
Interoperability	There is a plethora of systems, implementations, and database structures, there are a number of standards for TRU identification and Electronic Data Interchange, and there are very few standards defining how the recorded data elements should be named and measured. This means that system interoperability (exchange of data) is a big problem.	Blockchain-based systems are less diverse; they all record transactions (transformations) rather than state values, and they are all immutable. Interoperability and data interchange between blockchain-based food traceability systems is easier than between existing systems, any many of the success stories reported is because a higher degree of interoperability has been achieved.

There are minor costs and benefits related to the first five comparison criteria, as indicated by the light green shading (green indicates a potential benefit). As indicated above, the two criteria where the difference between the traceability system is biggest is “Speed and efficiency” which strongly favour a traditional system, and “Interoperability” which strongly favour a blockchain-based system.

When deciding between a traditional implementation of an electronic traceability system and a blockchain-based one, it is important to determine which system qualities are most important. If database transparency, integrity, and robustness is important, then a blockchain solution can be very relevant. On the other hand, if speed and data confidentiality are considered to be the most important system attributes, a traditional electronic traceability system is probably better.

The relevance and utility of improved interoperability should not be underestimated. While interoperability is technically possible for traditional traceability systems, it is difficult to get a large and diverse group of companies to agree on what standards and data formats to use. It is probably easier to get a large and diverse group of companies to agree to all use blockchain-based systems, and then significantly improved interoperability will be a much-desired side effect of that decision.

6.2 Seafood supply chain example

Even if in certain cases, the fisher can sell his/her products directly to the consumer, in the majority of cases, the supply chain consists of many steps and includes many actors (e.g., primary processors, secondary processors, distributors, transporters, middleman), especially when it comes to big fishing companies and aquaculture, as illustrated in Figure 4. The more mid-chain players there are, the higher the complexity of the supply chain and with it the higher chance of data-loss and fraud.

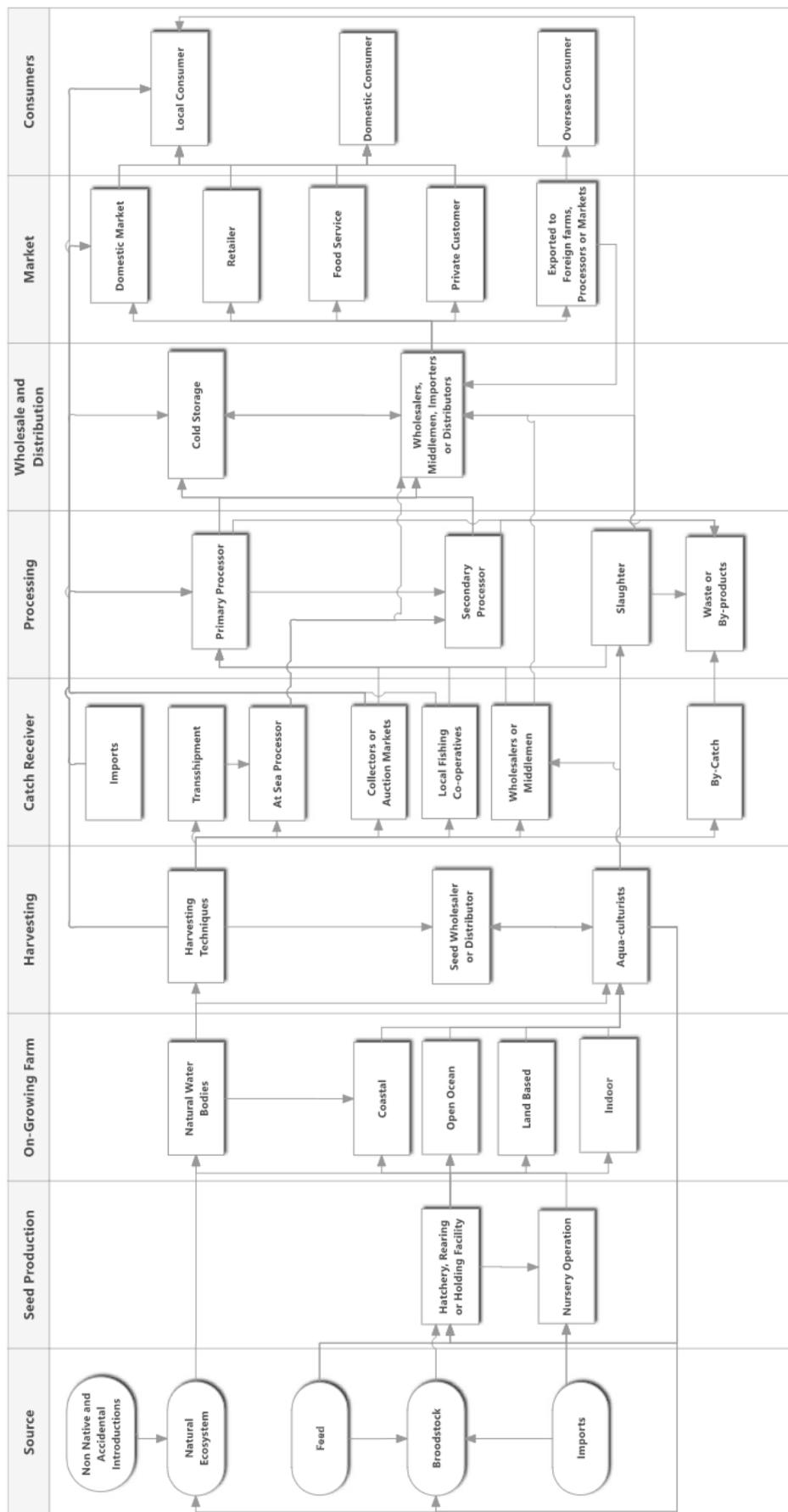


Figure 4 Seafood supply chain (M. Fox et al., 2018)

According to Future of Fish, a non-profit organisation/innovation hub for the seafood industry, the seafood supply chain has five attributes.

Product differentiation

There is a whole spectrum of degrees of differentiation: on one end are commodities characterised by a lack of differentiation. These refer to high-volume products aggregated from many sources and for which all individual units are considered identical regardless of how, where, when, and by whom they were produced or harvested. On the other end of the spectrum are differentiated products that can be distinguished from one another based on specific information such as harvest location, fishing method, certification status, etc. The degree of differentiation can be based on 1. Geography: aggregation of all products from multiple vessels in a single fishery; 2. Product qualities: specifically graded products (based on size, quality, sustainability) from vessels in a fishery with or without origin data; 3. Vessel: batches of product, such as from a single landing, net haul, or trap set; 4. Individual fish: typically high-value species that may be individually tagged with unique codes, and includes tuna, lobster, salmon, and snapper.

A supply chain that deals with differentiated products needs a more elaborate data management- and traceability system to track and verify the information associated with the unit of differentiation.

Brand presence

Some supply chains are driven by brands that dictate product specifications and other protocols that producers, processors, distributors, and end-buyers must follow. This influence can be top-down, coming from an end-buyer of certification standards, or bottom-up with a brand created by or with fishers. Depending on the values of the brand it is possible to influence the entire supply chain and for instance incorporate sustainability criteria into their product specifications.

Relationship dynamics

Relationships in the seafood industry are usually long lasting and built on trust, especially between fishers and their buyers (first receivers). It is not uncommon that those relationship tend to be both business and personal in nature. If the relationship is harmonious and healthy, this proximity is an added value to the supply chain and makes it more flexible. However, if the buyer starts to press or exploit the seller, the latter will feel trapped and the supply chain will be very difficult to influence.

Consolidation (vertically integrated vs. dispersed)

A vertically integrated supply chain means that a single actor controls most major steps in the supply chain, from fishing activities to the end product. The orientation of the product towards sustainability, and the ability of the supply chain to modify will depend on the motivation of that single actor. A dispersed supply chain is a supply chain where every function is performed by an independent entity, working to make a profit. In short supply chains and supply chains with differentiated products (see product differentiation) this can be a great advantage to easily modify the supply chain by working together for a common benefit. However, as a supply chain lengthens, the margins get slimmer and the different actors are more focused on cutting costs which can lead, at times, to committing fraud.

Market access (bottleneck vs. open access)

Many remote, artisanal fisheries involve a large number of fishers selling to a few middlemen who control the supply-chain relationships. Such bottlenecks limit the power of the fishers to negotiate the price and make changes to their fishing habits. With the middleman holding significant power, the fisher will be dependant on him/her to recognise the added value of the potential change the fisher would like to apply. Some fishers have more open access, either because they may be nearer to the end market and could bypass the middleman or because they have a highly sought-after product, and therefore more potential

buyers. In those cases, the fisher controls the price as well as the potential modifications he/she would like to make to his/her fishing activity.

In general, the pros and cons of using a blockchain-based traceability system for seafood are the same as for food products in general. But we saw that seafood supply chains can be very diverse and that some models are easier to change than others. We will link the relevance of blockchain-based implementation to the different attributes listed above in the Table 8.

Table 8 Relevance of blockchain-based systems on some characteristics of the seafood supply chain

Characteristic of the seafood supply chain	Relevance of blockchain-based implementation
Product differentiation, whether a product is considered as a commodity or differentiated according to geography, quality, vessel, or individual fish.	Whatever traceability system used, if the data entry is manual there is no guarantee that the stated differentiated attribute is the actual attribute. However, in a blockchain-based system everyone would see the entry in the system which could make the detection of a false attribute easier. If the entry is made automatic (geographical coordination of the boat, weight of the fish, vessel out fishing) then the entry can be trusted and will be immutable once recorded, which is not the case for a traditional traceability system. A differentiated product will then fit well with a blockchain-based system, which in this case could also provide consumer access to the recordings in the database, should that level of transparency be desired
Brand presence top-down or bottom-up	Will not be improved by a blockchain-based system but in case of implementation, if the standards of the supply chain are ruled by a top-down system meaning that the brand dictate the supply chain, the implementation of a blockchain-based system will depend on whether the brand sees a potential profit. If the standards are ruled by a bottom-up system, the change to a blockchain-based system can be led by the fisher who sees an added-value from sharing information on his/her work and effort to the customer.
Relationship dynamics	Will not be improved by a blockchain-based system but of course the better the relationship between supply chain actors, the easier it would be to get them on board as the blockchain should be applied on the supply chain as a whole to be efficient.
Consolidation (vertically integrated vs. dispersed) whether a single actor controls the major steps of the chain or if all entities along the chain work for themselves	We saw that a long supply chain with all entities working for themselves can be a trigger for food fraud as everyone will try to cut the cost where they can. In that case blockchain will help to detect the fraud more easily than with a traditional system as every step is recorded and immutable, and a mismatch with a previous block will be easily spotted.
Market access (bottleneck vs. open access)	Will not be improved by a blockchain-based system. However, the action of the middleman would be recorded in the blockchain which would at least ensure the fisher that the middleman is not cheating with it to pressure him/her.

We can see based on this analysis that the implementation of a blockchain-based system would not improve management dynamics and power relations in the supply chain regarding brand presence, relationships dynamics and market access, but would on the other hand have a positive impact on the product differentiation and to prevent or at least allow for detecting food fraud more easily. But when we analyse the supply chain itself and the different forms the supply chain can have, we don't analyse the profitability of the supply chain nor the satisfaction of the end customer, both which are important in order to have a successful product. In the next section we will see that this is an area where blockchain can have an impact.

6.3 Norwegian seafood trust example

In 2020 a project started in collaboration between Atea, Norwegian Seafood Association, and IBM to create a national seafood tracking network: the Norwegian seafood trust (NST, <https://norwegianseafoodtrust.no/>). They have engaged with Nova Sea and Kvarøy Arctic, two salmon producers in Northern Norway, and Biomar, one of the biggest aquaculture feed producers in Norway. The goals of the NST are to provide the Norwegian seafood industry with:

- An advantage in the market
- Increased value creation of Norwegian products and services
- Create consumer safety in a competitive market in the future
- Leverage each other's expertise
- Share experiences and knowledge

The motivation at the start of the project was to find solutions to the societal challenges that seafood is facing: lack of consumer trust in the product, desire to know more about the condition of production, type of feed given, environmental impact, condition of transport and processing, freshness of the product and many more. On the producer side there is frustration: a lot of care and work is put in place in the production, but nothing is reflected on the final product despite the information existing. The NST project was designed to bring this information to the consumer by using information available but not used to their fullest so far with the help of a blockchain based system. While Norwegian seafood association and Atea bring the local knowledge, IBM has designed a blockchain system adapted to the seafood industry: IBM food trust, <https://www.ibm.com/blockchain/resources/food-trust/seafood/>.

IBM food trust is a tailor made blockchain, built in four modules to achieve different goals regarding traceability:

Consumer module shares the journey of your seafood, along with product details and/or sourcing information. Connects seafood consumers to specific permissioned information that helps influence buying decisions such as origin, ingredients, quality, and sustainability practices. Objective: building consumer demand and brand trust.

Insights capabilities module provide supply chain visibility to help identify and address inefficiencies. It provides near real time supply chain data, including seafood temperature and location within the cold chain. Leveraging blockchain and IoT technology, it enables better temperature control for improved shelf life and decreased waste, as well as dynamically optimising inventory management and product rotation. Objective: improving cold chain management and reducing waste.

Trace module allows food system members to securely and transparently trace the location and status of food products on the supply chain. Enables end-to end supply chain visibility. Know the provenance of seafood and its status as it travels from catch to fork for improved food integrity. Objective: establishing proof of origin and preventing mislabelling.

Documents module allows users to prove sustainability and provenance with ease by securely managing certificates throughout the entire supply chain. Allows users to upload, manage, edit, and share any documents along the supply chain. Improve information management, certify provenance, ensure authenticity, and demonstrate production standards – regardless of the type of document used. Objective: supporting sustainability and quality standards.

Seven common issues are found in the food production: supply chain efficiency, brand trust, food safety, sustainability, food freshness, food fraud and food waste. Table 9 shows who those issues can be improved with a combination of the four suggested modules.

Table 9 Improvements brought by blockchain within food production (IBM Food Trust)

Issues	Problems	Improvements by blockchain	Modules
Supply chain efficiency	Manual paper-based processes that makes it difficult and time-consuming to identify issues and manage inventory, to match supply and demand, and identify waste hot spots, and; waste due to poor coordination across the food chain network.	Easily identify process inefficiencies, eliminate bottlenecks and optimise the supply chain for continuous growth; real-time demand forecasting: all food system participants can know the provenance, real-time location and status of their food products. With better data, companies can develop more accurate supply and demand forecasting models, localise the sourcing of ingredients and restructure contracts.	Insights, Trace, Documents
Brand trust	The trend shows that consumers want to know more than just the nutritional information – they want to know the food's origin, when it was grown and how. Trust in the seafood. 30% of shoppers switch brands after a product recall.	Full transparency, top-to-bottom visibility into the food chain enables brands to quickly and proactively manage damaged products without disrupting the entire supply chain. When consumers and supply chain partners know that brands are transparent about the quality and origin of their foods, it builds brand equity and trust, creating differentiation. By tracking each step of the supply chain and sharing data on an immutable ledger, participants can ensure the quality of goods.	Trace, Consumer, Documents
Food safety	Not all companies can quickly identify the cause of a food safety incident, and tracing food across the supply chain can take a long time. Gaps in supply chain monitoring create vulnerabilities. Food safety regulators demand state-of-the-art practices and modern technologies to ensure food safety.	Transparency by knowing the provenance, real-time location and status of any food product. If a food safety issue is reported, it is immediately clear who is impacted and who should take action.	Trace, Documents, Insights
Sustainability	More and more people are willing to change food consumption habits to reduce their environmental impact. With the global world population growing, companies are looking for ways to decrease their ecological footprints.	With end-to-end transparency users can guarantee provenance and gain a clearer view of where inefficiencies and lack of sustainability exist across the entire supply chain. Farmers, producers and other food actors can automatically digitize and easily share audits, certificates and other records, proving that they utilise and promote sustainable and ethical practices. Increase trust.	Consumer, Trace, Documents
Food freshness	Food travels far before reaching a plate because of globalisation. Due to the complexity of the food chain, fresh products spend a good percent of their shelf life in transit. A complex supply chain along with gaps in it decrease the velocity of travel and increase challenges to maintaining food freshness. Poor visibility on part of the supply chain creates product loss and decreases margin.	Track how fresh food really is and how long it's been traveling allows for better understanding of the remaining shelf life. Full visibility into the food chain enables companies to know exactly the conditions under which the product was shipped, for example with regards to temperature data and inventory levels. It allows proactive decisions to optimise and improve efficiencies in the supply chain.	Trace, Documents, Consumer
Food fraud	Food fraud regulators demand good practices and technology to help bring organisations up to standard and ultimately create a more transparent food system. Complex supply chains create blind spots to identify at what level food fraud can happen.	End-to-end traceability increases surveillance on each link of the food chain, enabling real-time traceability and creates accountability. Secure data-sharing between food chain actors eliminates the possibility for participants to move fraudulent foods unknowingly. Improvement of transparency allows fewer opportunities for fraudsters to penetrate the supply chain and permanent records enable better management of material safety and quality standards.	Trace, Insights, Documents
Food waste	Reducing food waste remains complex and requires effort across the supply chain. Consumers that are unsure about the quality of their food will contribute to food waste.	End-to-end traceability helps to maximise the shelf life, optimise partner networks and increase recall response efficiency, helping reduce waste. More visibility on the supply chain helps identify opportunities to reduce food waste.	Insights, Trace, Documents

The decision of opting for a blockchain-based solution can be based on different needs like improving the overview of the supply chain to ensure better management and optimising profits or a desire for communicating the work done and the effort put in the sustainable seafood production to the end customer. With the module system proposed by IBM food trust, companies interested in one of these improvements can create a blockchain-based system that corresponds to their needs. Nevertheless, we can see in Table 10 that two modules, Trace and Documents, are mentioned as an improvement across all the potential issues of the food production.

Table 10 Summary of suggested modules according to aimed improvement in food production

	Consumer	Insights capabilities	Trace	Documents
Supply chain efficiency		x	x	x
Brand trust	x		x	x
Food safety		x	x	x
Sustainability	x		x	x
Food freshness	x		x	x
Food fraud		x	x	x
Food waste		x	x	x

Kvarøy Arctic have presented their experience with the Norwegian Seafood Trust (IBM Blockchain, 2020) and their implementation of the blockchain-based solution by IBM. We will describe their case study in the next section.

6.3.1 Kvarøy Arctic experience of IBM food trust

Kvarøy Arctic is a small-scale family-owned salmon producer with 26 employees based around the island of Kvarøy in northern Norway. They have six licences and produce 8 tonnes of salmon per year which represents 0.6% of Norway's yearly production. Their focus, driven by their customers, is on producing sustainable and environmentally friendly high-quality salmon. To meet the needs of their customers, they implemented some changes to their production. These include producing fish without using chemicals or antibiotics, nets without copper treatment, creating their own feed that is sustainable with natural colorant, and using algae oil to reach higher omega 3 compounds in the salmon while at the same time reducing the amount of fish used in the feed, which gives them a fish inn: fish out-ratio of 0.48:1.

Their decision to implement blockchain technology came about as a response to their customers, who wanted more information about how the feed is produced, and who pushed for a more transparent and traceable production. For Kvarøy Arctic it was important to address this demand and show that they have no secrets and that everything they do can be shared. They got on board with the NST in 2020, making them the first salmon producer in Norway to use IBM's blockchain solution, believing that it was a good platform to share what they are doing and how they are doing it with their customers. A feature of great importance for them was that the data was collected automatically. This was not the case for all data when they started the IBM food trust solution, but after a software system change, they reached that goal. They have control over most of the supply chain which certainly made the implementation of the blockchain through the whole production easier. They achieved full traceability from the eggs to the fish in the store, which was already a great achievement, but in addition it allowed them to gather more data to understand better how their salmon is produced. Those data already existed but were not being used. Still at an early stage of the blockchain, they can now select what data to share with their customers and are working with them to know what information they would like to have access to, which will be done through a simple QR code that can be scanned with a phone camera.

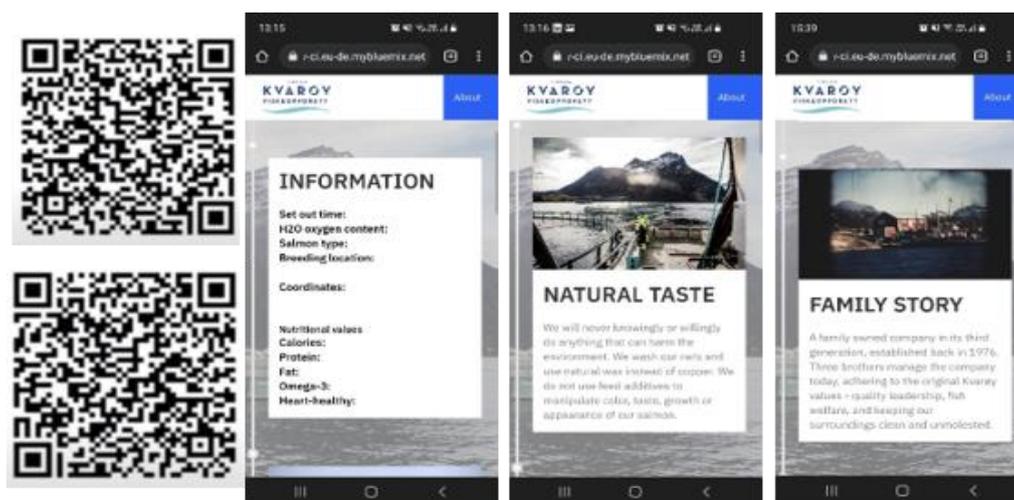


Figure 5 Kvarøy Arctic QR code and webpage (in construction) linked to those

Figure 5 gives us an example of what kind of information can be found when scanning the QR code on the packaging of Kvarøy Arctic salmon in shops. They can provide information on both the production and nutrition of the salmon, as well as other information they would like to share with their customers such as the history of the company, their values of sustainability, environment, and quality, whether they are global, or even very specific information such as them washing their nets using natural wax instead of copper.

6.4 How authorities may use data recorded in a blockchain-enabled system

The costs associated with implementing and maintaining a blockchain-based traceability system largely fall on the food businesses; this includes the additional costs associated with a blockchain-based system as compared with a traditional system. Some of the benefits associated with a blockchain-based system are significant for the authorities, as indicated in Table 11.

Table 11 Costs and benefits of blockchain-based systems for authorities

Comparison criteria	Traditional electronic traceability system	Electronic traceability system based on blockchain technology
Suitability of database	Authorities can only access claims in relation to state of variables	Authorities can access the entire set of transformations that led to the current state, which makes it easier to see the origin of the stated claim
Data quality and veracity	Authorities need separate and external checks to test the data quality and veracity	Some degree of quality and veracity is provided by the blockchain-based system itself
Immutability, integrity and transparency	It is difficult for authorities to know if recorded data has been subsequently overwritten	The immutability of the database means that the authorities know that the data has not been overwritten
Confidentiality	Not an issue for authorities	
Trust	Not really an issue for authorities (except for trust in data quality and veracity, which is better in a blockchain-based system)	
Robustness	Not an issue for authorities	
Speed and efficiency	Not an issue for authorities	
Interoperability	Lack of interoperability makes it more difficult to identify discrepancies, and to do mass-balance accounting which is sometimes necessary to identify fraud	Better interoperability and better access to comparable data from different systems makes it easier to identify discrepancies, and to do mass-balance accounting

As indicated, the costs associated with blockchain-based systems (speed, efficiency, and confidentiality in particular) are not particularly relevant for authorities, whereas some of the benefits (recording of transactions and not only variable states, immutable database, interoperable systems) are significant for authorities. From this follows that authorities should be proponents of blockchain-based food traceability systems and should encourage FBOs to adopt them.

7 Conclusions and recommendations

The overall recommendation is that unless confidentiality or speed are of paramount importance, to base an electronic food traceability system on blockchain technology is a good solution. The main reason for this conclusion is the question of interoperability and data sharing. While it is technically possible to achieve this between existing systems, in practice a lack of interoperability has been one of the main bottlenecks preventing data access from farm to fork. Rather than continuing to hope for the widespread adoption of standards to support interoperability, it is probably more realistic to hope that many actors in the supply chain will adopt blockchain-based traceability systems, which in itself will increase interoperability.

It is worth emphasising that blockchain-based implementations will not solve all, or even most of the problems associated with traditional electronic traceability systems. This includes:

- Data quality and veracity — still a problem in blockchain-based implementations.
- Food fraud — still a challenge in blockchain-based implementation, although if food fraud is detected, it will be easier to identify who made the fraudulent statement.
- Need for standards – while standards for EDI are less relevant when using blockchain-based systems, standards that define what the recorded data elements and values mean (ontologies) will be needed more than ever. The increased interoperability will mean increased access to data recorded in a different part of the supply chain; a standard is needed to define what the data element names mean, and what the recorded values signify.

But keeping those challenges in mind, blockchain technology seems a suitable solution and would improve the connection between actors of the supply chain, provide a better overview and avoid black spots, which would lead to a better management of the production, less food waste and a closer contact with end-customers if sharing information with them is a desire.

8 References

- Abeyratne, S.A. & R.P. Monfared (2016). Blockchain ready manufacturing supply chain using distributed ledger. *International Journal of Research in Engineering and Technology*, **05**, pp. 1–10.
- Bermeo-Almeida, O., M. Cardenas-Rodriguez, T. Samaniego-Cobo, E. Ferruzola-Gómez, R. Cabezas-Cabezas & W. Bazán-Vera (2018). Blockchain in Agriculture: A Systematic Literature Review. Springer, Cham, pp 44–56.
- Blasetti, R. (2017). Blockchain For Business, Should You Care? Available at: <https://blockgeeks.com/blockchain-for-business/> [Accessed December 30, 2018].
- Borit, M. & P. Olsen (2016). Seafood traceability systems: Gap analysis of inconsistencies in standards and norms (FAO/FIAM/C1123). Rome.
- Carson, B., G. Romanelli, P. Walsh & A. Zhumaev (2018). Blockchain beyond the hype: What is the strategic business value? Available at: <https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/blockchain-beyond-the-hype-what-is-the-strategic-business-value> [Accessed December 30, 2018].
- Casino, Fran, et al. (2021) Blockchain-based food supply chain traceability: a case study in the dairy sector. *International Journal of Production Research* 59.19 : 5758-5770.
- Ciaian, P. (2018) Blockchain technology and market transparency. Available at: https://ec.europa.eu/info/sites/info/files/law/consultation/mt-workshop-blockchain-technology-and-mt_ciaian_en.pdf [Accessed December 30, 2018].
- Collak, V. (2018) Blockchain In Supply Chain -- How To Use The Distributed Ledger To Trace Products. Available at: <https://www.forbes.com/sites/forbestechcouncil/2018/05/22/blockchain-in-supply-chain-how-to-use-the-distributed-ledger-to-trace-products/#4e64ffc2351c> [Accessed December 16, 2018].
- Egels-Zandén, N., K. Hulthén & G. Wulff (2014). Trade-offs in supply chain transparency: the case of Nudie Jeans Co. *Journal of Cleaner Production*.
- Food and Agriculture Organization (FAO) (2019). E-agriculture in action – blockchain in agriculture – opportunities and challengers. Sylvester ed, available at: <http://www.fao.org/3/CA2906EN/ca2906en.pdf> [Accessed 18 February 2022].
- Fox, M. et al. (2018). The seafood supply chain from a fraudulent perspective. Springer. Future of Fish. Available at <https://www.futureoffish.org> [Accessed October 25, 2021]
- Galvez, J.F., J.C. Mejuto & J. Simal-Gandara (2018). Future challenges on the use of blockchain for food traceability analysis. *TrAC Trends in Analytical Chemistry*, **107**, pp. 222–232.
- Hochfelder, B. (2018) HSBC, Cargill successfully complete blockchain trade-finance transaction. Available at: <https://www.supplychaindive.com/news/hsbc-cargill-blockchain-pilot/523554/> [Accessed December 17, 2018].
- Hofstede, G.J. (2004) Hide or confide?: the dilemma of transparency. *Reed Business Information*, 's-Gravenhage.
- Howson, P. (2020). Building trust and equity in marine conservation and fisheries supply chain management with blockchain. *Marine Policy*, 115, 103873.
- IBM. IBM Food Trust: A new era in the world's food supply. Available at [IBM Food Trust - Blockchain for the world's food supply | IBM](#) [Accessed October 19, 2021].
- IBM. Seafood on blockchain. Available at [Seafood on blockchain - IBM Food Trust | IBM](#) [Accessed October 24, 2021].
- IBM Blockchain (2020). IBM Food Trust: Blockchain for Seafood. Available at [IBM Food Trust: Blockchain for Seafood - YouTube](#) [Accessed October 20, 2021].
- Kamilaris, A., A. Fonts & F.X. Prenafeta-Boldú (2018). The Rise of the Blockchain Technology in Agriculture and Food Supply Chain. Available at: https://www.researchgate.net/profile/Andreas_Kamilaris/publication/327534824_The_Rise_of_the_Blockchain_Technology_in_Agriculture_and_Food_Supply_Chain/links/5b93d0ada6fdccf

- d5428b0f2/The-Rise-of-the-Blockchain-Technology-in-Agriculture-and-Food-Supply-Cha [Accessed December 17, 2018].
- Kim, H.M., M.S. Fox & M. Grüninger (1999). An Ontology for Quality Management — Enabling Quality Problem Identification and Tracing. *BT Technology Journal*, **17**, pp. 131–140.
- Knudsen, C. (2020). Lakseprodusenter skal bruke blokkjedesporing: Kan øke salget med opptil 1,3 milliarder. *Online journal E24*. Available at <https://e24.no/hav-og-sjoemat/i/dOylyq/lakseprodusenter-skal-bruke-blokkjedesporing-kan-oeke-salget-med-opptil-13-milliarder> [Accessed October 24, 2021]
- Kosba, A., A. Miller, E. Shi, Z. Wen & C. Papamanthou (2016). Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts. In: 2016 IEEE Symposium on Security and Privacy (SP). *IEEE*, pp 839–858.
- Lansiti M. & R.K. Lakhani (2017) The Truth About Blockchain. Available at: <https://hbr.org/2017/01/the-truth-about-blockchain> [Accessed December 30, 2018].
- Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G.M. and Savage, S. (2013) A fistful of bitcoins. In: Proceedings of the 2013 conference on Internet measurement conference - IMC '13. ACM Press, New York, New York, USA, pp 127–140.
- Nakamoto, S. (2008) Bitcoin: A Peer-to-Peer Electronic Cash System. Available at: <https://bitcoin.org/en/bitcoin-paper> [Accessed December 30, 2018].
- Nova Sea (2021). Nova Sea joins Norwegian Seafood Trust to track salmon from feed to food. Available at [Nova Sea joins Norwegian Seafood Trust to Track Salmon from Feed to Food - Nova Sea](#) [Accessed October 23, 2021].
- Nugent, T., D. Upton & M. Cimpoesu (2016). Improving data transparency in clinical trials using blockchain smart contracts. *F1000Research*, **5**, p. 2541.
- Olsen, P. & M. Borit (2013). How to define traceability. *Trends in Food Science and Technology*, **29**, pp. 142–150.
- Olsen, P. & M. Borit (2018). The components of a food traceability system. *Trends in Food Science and Technology*, pp. 143–149.
- Olsen, P. Borit, M. Syed, S. (2019). *Applications, limitations, costs, and benefits related to the use of blockchain technology in the food industry*. Tromsø: Nofima.
- Reef resilience Network. Structure of Seafood Supply Chain. Available at <https://reefresilience.org/coral-reef-fisheries-module/making-sense-of-wild-seafood-supply-chains/structure-of-seafood-supply-chains/> [Accessed October 25, 2021].
- Renn, O. (2008). Risk governance: coping with uncertainty in a complex world. Earthscan.
- Sønstebj, S. – IBM (2021). Blockchain stories: giving Norwegian seafood a competitive edge. Available at [Blockchain stories: Giving Norwegian seafood a competitive edge IBM Supply Chain and Blockchain Blog](#) [Accessed October 17, 2021].
- TraceFood (2008). GTP:Defining traceable units. Available at: www.tracefood.org [Accessed October 24, 2015].
- Underwood, S. (2016). Blockchain beyond bitcoin. *Communications of the ACM*, **59**, pp. 15–17.
- Venås Kjeldsen, T. - ATEA (2020). Mer bærekraftig med blockchain-teknologi. Available at ["https://www.atea.no/siste-nytt/mer-baerekraftig-med-blockchain-teknologi/"](https://www.atea.no/siste-nytt/mer-baerekraftig-med-blockchain-teknologi/) [Accessed October 17, 2021].
- Wang, H., Z. Zheng, S. Xie, H.N. Dai & X. Chen (2018). Blockchain challenges and opportunities: a survey. *International Journal of Web and Grid Services*, **14**, p. 352.
- Wust, K. & A. Gervais (2018). Do you Need a Blockchain? In: 2018 Crypto Valley Conference on Blockchain Technology (CVCBT). *IEEE*, pp. 45–54.
- Zheng, Z., S. Xie, H. Dai, X. Chen & H. Wang (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. In: *2017 IEEE International Congress on Big Data (BigData Congress)*. *IEEE*, pp. 557–564.