Blockchain for Agriculture and Food

Findings from the pilot study

Lan Ge, Christopher Brewster, Jacco Spek, Anton Smeenk, and Jan Top

WAGENINGEN
UNIVERSITY & RESEARCH

TNO innovation for life

Blockchain for Agriculture and Food

Findings from the pilot study

Lan Ge, Christopher Brewster, Jacco Spek, Anton Smeenk, and Jan Top

With inputs from Frans van Diepen, Bob Klaase, Conny Graumans, and Marieke de Ruyter de Wildt

This study was carried out by Wageningen Economic Research and TNO in collaboration with RVO, AgroConnect, VAA ICT Consultancy, NVWA, AgriPlace, OTC Holland, Floricode, BC3, GS1, Control Union, SKAL, and PPM Oost. The research was commissioned and financed by the Dutch Ministry of Agriculture, Nature and Food Quality within the programme 'Voedselagenda'.

Wageningen Economic Research
Wageningen, November 2017

REPORT
2017-112
ISBN 978-94-6343-817-9

Ge, Lan, Christopher Brewster, Jacco Spek, Anton Smeenk, and Jan Top, 2017. *Blockchain for Agriculture and Food; Findings from the pilot study.* Wageningen, Wageningen Economic Research, Report 2017-112. 34 pp.; 4 fig.; 2 tab.; 18 ref.

This report documents experiences and findings from the public private partnership (PPP) project 'Blockchain for Agrifood' that was started in March 2017. The project aims to contribute to a better understanding of the blockchain technology (BCT) and its implications for agrifood, especially how it can impact specific aspects of supply chains and what is needed to apply BCT in agrifood chains. A second aim of this project is to conceptualise and develop a proof of concept in an application based on a use case concerning table grapes from South Africa where BCT could be applied. This has been done by building a demonstrator that keeps track of different certificates involved in the table grapes supply chain. The code of this demonstrator is published at Github.[1] Furthermore, the project explored issues regarding the relevance, applicability and implications of BCT for the agrifood sector through literature study and stakeholder consultation.

Key words: blockchain, agriculture, food

This report can be downloaded for free at https://doi.org/10.18174/426747 or at www.wur.eu/economic-research (under Wageningen Economic Research publications).

P.O. Box 29703, 2502 LS The Hague, The Netherlands, T +31 (0)70 335 83 30,
E communications.ssg@wur.nl, http://www.wur.eu/economic-research. Wageningen Economic Research is part of Wageningen University & Research.

Wageningen Economic Research Report 2017-112 | Project code 2282300245

Cover photo: Shutterstock

[1] https://github.com/JaccoSpek/agrifood-blockchain

Contents

Executive summary

This report documents experiences and findings from the public private partnership (PPP) project 'Blockchain for Agrifood' that was started in March 2017. The project aims to contribute to a better understanding of the blockchain technology (BCT) and its implications for agrifood, especially how it can impact specific aspects of supply chains and what is needed to apply BCT in agrifood chains. A second aim of this project is to conceptualise and develop a proof of concept in an application based on a use case concerning table grapes from South Africa where BCT could be applied. This has been done by building a demonstrator that keeps track of different certificates involved in the table grapes supply chain. The code of this demonstrator is published at Github[2]. Furthermore, the project explored issues regarding the relevance, applicability and implications of BCT for the agrifood sector through literature study and stakeholder consultation.

The project took an agile multi-actor approach i.e. with lean and active stakeholder participation. The main focus was on obtaining hands-on experience with the development of blockchain applications in agrifood and insight into perspectives of key stakeholders.

Understanding BCT

BCT is not a single technology. BCT uses a combination of technologies that have a considerable history in computer science and in commercial applications. These component technologies include public/private key cryptography, cryptographic hash functions, database technologies especially distributed databases, consensus algorithms, and decentralised processing. The fundamental purpose is to achieve database consistency and integrity in a context of a distributed decentralised database.

Key technical choices of BCT include: 1) Permission design, i.e., whether permission is needed to access the blockchain; 2) Choice of consensus algorithm, i.e., how a new block is added to the blockchain; 3) Whether or not to use smart contract, i.e., whether to use the blockchain as a virtual machine where programs representing business processes are run; 4) Whether or not to use cryptocurrency, i.e., whether the consensus algorithm and smart contract operations depend on an artificial currency or not . For BCT implementation, technical choices often result from the governance model chosen for the ecosystem of participants.

Relevance and implications of BCT for agrifood

An increasing demand in society for greater information about food reflects the need for more transparency and the lack of trust. At the same time, more and more food products and beverages are branded and accompanied by a variety of certification schemes, with an increasing risk of fraud (selling unqualified product with high-quality labels or claims) and adulteration.

In the current situation, much of the compliance data and information is audited by trusted third parties and stored either on paper or in a centralised database and these approaches are known to suffer from many informational problems such as the high cost and inefficiency of paper-based processes and fraud, corruption and error both on paper and in IT systems. These information problems, indicating that current transparency and trust systems have not been able to solve or at times even have exacerbated the problems of low transparency and trust in agrifood chains, pose a severe threat to food safety, food quality, and sustainability. In particular, food integrity has become a

[2] https://github.com/JaccoSpek/agrifood-blockchain

major concern. Food integrity refers to the fairness and authenticity of food in food value chains both at the physical layer and the digital layer, where the digital layer should provide reliable and trustworthy information on the origin and provenance of food products in the physical layer.

Blockchain technology provides a means to ensure permanence of records and potentially to facilitate the sharing of data between disparate actors in a food value chain. This potential may lead to an exciting paradigm shift facilitating transparency and trust in food chains that ensures food integrity.

Proof of Concept (PoC)

This PoC pilot has demonstrated that it is feasible to put basic information concerning certificates on a blockchain with a permissioned ledger and a smart contract. Compared to traditional situations with centralised databases, the PoC demonstrator shows how a blockchain can be used to ensure that different parties share the same layer of information on the validity and provenance of certificates that is tamper-proof. This feature can potentially increase the value of certificates.

There are several limitations to the PoC demonstrator. First, the amount of data and information that is shared is very limited. For the sake of simplicity, our demonstrator focused on one smart contract with all participants able to read and write. All participants in a smart contract (under this architecture) have access to all data, and thus in a real world deployment, multiple smart contracts would need to be deployed for the different contractual relationships in order to keep business confidentiality. An important aspect that would need to be addressed is the interaction between smart contracts and the feasibility of data flows between smart contracts. The limitations of the PoC demonstrator, however, have little impact on its value in improving the understanding of BCT, but rather suggest directions for further research. To obtain better insight into the added value of BCT in more real life cases, these issues should be addressed in further research and exploration.

State-of-the-art developments

At the moment (October 2017), few would question the relevance of BCT to agrifood. The main question is rather on the added value of BCT compared to existing IT solutions or other non-IT solutions (i.e. new organisational models) in real life cases.

BCT is still in an early stage of development. Innovation in blockchain architectures, applications and business concepts is happening at a fast pace; it is often characterised by decentralised, open source development, and it is perceived as being disruptive to traditional players in many industries. The rapid but unpredictable direction of blockchain innovation makes it particularly hard for commercial organisations and government agencies to make strategic decisions on how to respond to BCT.

Future research and policy recommendations

Given the rapidly increasing level of digitalisation and demand for data and product integrity, the agrifood sector is in a unique position to explore the potential of BCT. BCT can for example help value chain partners in improving transparency and efficiency of business transactions, compliance processes and tracking and tracing of food products. BCT can also help NGOs and impact investors in supporting inclusive business models. Although the application of BCT in agrifood is currently still in its infancy, it can be expected that more initiatives will be taken by various organisations. Left uncoordinated, this can result in the waste of resources and missed opportunities for businesses and society as a whole.

From a policy perspective, the following recommendations can be made:

- Facilitate and encourage the growth of the ecosystem of blockchain-minded parties in agrifood chains;
- Support and stimulate blockchain as part of the digitalisation strategy to improve transparency, efficiency, competitiveness and sustainability of the agrifood sector;
- Design a clear regulatory framework for blockchain implementations;
- Provide government investment in research and innovation so as to develop the evidence for the added value of the technology.

With special attention to:

- Development of guidelines for proof of concept (PoC) projects and large-scale implementation;
- Development of standards and knowledge base regarding BCT implementation;
- Awareness raising of new governance and organisational modes implied by BCT and its implications for business and policy through knowledge dissemination;
- Investment in ecosystem development for blockchain implementation around themes such as transparency, food integrity, and traceability in agrifood chains.

1 Introduction

This report documents experiences and findings from the public private partnership (PPP) project 'Blockchain for Agrifood' that was started in March 2017. The project reflects a joint exploration and learning process on blockchain technology (BCT), a new technology that is considered by many to be disruptive to many sectors but has undoubtedly the feature of a 'technology hype' that is still going through the early phases of the hype cycle[3].

In view of the ongoing hype of the blockchain technology (BCT), this study aimed to:

- contribute to a better understanding of the blockchain technology and its implications for agrifood, especially how it can impact specific aspects of supply chains and what is needed to apply BCT in agrifood chains.
- conceptualise and develop a pilot use case on table grapes from South Africa where blockchain could be applied.
- explore other applications of blockchain technology for agrifood with key stakeholders in the agrifood sector and identify the following:
  - State-of-the-art (technology and policy perspective)
  - Opportunities and challenges
  - A list of potential applications
  - Research agenda

The remainder of this report consists of 5 chapters. Chapter 2 provides more background information on the technology and this project. Chapter 3 highlights the relevance of the technology to agrifood. Chapter 4 describes the Proof of Concept-the demonstrator application in the use case. Chapter 5 presents the main findings of this pilot study. Chapter 6 discusses the findings and offers policy recommendations.

[3] See e.g., http://www.gartner.com/technology/research/methodologies/hype-cycle.jsp

2 Background and methodology

2.1 Blockchain as an emerging technology

The last three years have seen an explosion of interest in Blockchain Technology (BCT) with a great many companies and research institutions focusing on potential applications of this technology across a range of financial, industrial and social sectors. However, the technology has also been surrounded by a great deal of exaggeration and hype resulting in misplaced expectations and misunderstandings. BCT is still in an early stage of development, with considerable potential for real-life commercial applications. Innovation in blockchain architectures, applications and business concepts is happening at a fast pace; it is often characterised by decentralised, open source development, and it is perceived as being disruptive to traditional players in many industries. The rapid but unpredictable direction of blockchain innovation makes it particularly hard for commercial organisations and government agencies to make strategic decisions on how to respond to BCT. Furthermore, since the technology is borderless, it is difficult to regulate at a national level.

In the Netherlands, industrial interest in BCT was first documented at the end of 2014, as a number of Dutch banks started their first modest experiments with bitcoin payments. Banks worldwide have indicated decentralised cryptocurrencies (such as, but not limited to Bitcoin) have the potential to disrupt or even replace traditional banking payment services, and Dutch banks have made similar statements.[4] As BCT progressed beyond Bitcoin, it became clear that BCT is not only able to disintermediate financial transactions, but can also disintermediate many other kinds of information transactions. This sparked interest in other industries in the Netherlands, such as the broader financial services industry (insurance, pensions), logistics, energy, healthcare, telecommunications, industrial manufacturing and many more.

2.2 Background of the project

A number of authors have proposed that the food and agriculture sector may also be a fruitful area for the application of BCT and this is of particular importance in the Netherlands. BCT was considered of great relevance to the agrifood sector because agrifood transactions are fraught with a number of information management problems. The Italian organic food scandal (2011) and the horsemeat scandal (2013) plus the ongoing problem of food certification authenticity are some examples. BCT provides immutable permanent transactions and distributed data access which have the potential to facilitate data exchange and reduce the opportunities for fraud or adulteration.

The social enterprise Provenance (www.provenance.org) in the UK has been a leader in proposing the application of BCT to agricultural supply chains (mostly concerning the recording of certification). Other potential areas of application may include tracking and tracing, improving trust in data sharing, and insurance. However, a great deal of work needs be undertaken translating the theoretical applicability of BCT to its use in real world scenarios. There remain many technical challenges such as scalability and throughput, suitability for data querying, and the digital to physical interface. Issues which arise are not just purely technical (e.g. throughput of transactions) but also concern legal status and governance. More generally, many questions have to be asked such as ‘What problems does BCT solve?’, ‘What problems does BCT create?’ and closely related to these questions ‘Who benefits?’. What impact will this new technology have on the digital ecosystems for transparency and trust in agrifood? Will this new kind of trust and transparency revolutionise the way agrifood chains are organised? What knowledge and expertise are needed in order to harness the power of the

[4] See e.g., https://www.coindesk.com/ideation-realization-dutch-bank-harness-blockchain/

blockchain? These questions can only be answered by the joint exploration of key stakeholders with a pilot use case.

A stakeholder workshop was held in November 2016 on the possibilities and challenges of blockchain for agrifood. Stakeholders expressed great interest in and enthusiasm for BCT. A steep learning curve was expected and a pilot study was considered necessary to improve understanding of the technology and its implications.

The use case of table grapes from South Africa was considered suitable for the pilot as it involves information problems supposedly addressed by BCT. From a vineyard under the South African sun, table grapes travel a long way before reaching the plates of European consumers. There is a lot that the end consumers (and therefore traders and retail) would like to know about the table grapes. For example, are they safe to eat? Are they produced in a sustainable way? In what kind of soil did the plants grow? What type of fertiliser was applied? What were the labour conditions on the farm? Can we be assured for their safety and sustainability if they carry such a certificate? How can we be sure that the certificate is authentic? Are the claims valid? In view of these questions, our pilot project was designed to determine in what way blockchain technology could help.

Thanks to a previous public private partnership (PPP) research project FarmDigital (www.farmdigital.nl), a lot of details about the chain and network were already known so that the project could focus on the application of blockchains in this use case. A detailed description of the use case can be found in Appendix 1.

2.3 Issues explored in the pilot study

At the start of the project (i.e., March 2017), the full range of potential applications of BCT and the corresponding challenges were unknown. Although the technology and its ecosystem have developed rapidly, there are still many unsolved issues and problems which need to be addressed before the full potential of BCT and related technologies can be realised, including:
- the resolution of issues of privacy and security in digital transactions and data-exchange
- the choice between alternative designs and implementations for BCT
- the relation to and interaction with existing (legacy) database and network technology
- the lack of a regulatory framework for BCT while there are strong data privacy regulations (GDPR)
- the issues concerning performance (speed, reliability) and scalability (capacity of the blockchain)
- the potential costs of developing and maintaining the network.

With these general issues in mind, the project explored the following issues in the use case:
- Which issues/problems related to information exchange exist in the specific use case?
- Which BCT platform to apply in this case? Based on what criteria?
- Which features of the platform chosen are most relevant for the use case?
- Which technical and organisations context features will have to be taken into account in this use case?
- Which stakeholders are affected by BCT in this case?
- What steps are needed to implement BCT?
- Does the technology impose specific requirements on the hosting infrastructure?

2.4 Methodology and process

The project took an agile multi-actor approach i.e. with lean development and active stakeholder participation. The main focus was on obtaining hands-on experience with the development of blockchain applications in agrifood and insight into perspectives of key stakeholders. Project activities include the following:
- Literature study: this includes peer-reviewed articles and documents from the 'grey literature' such as reports as well as popular blogs and news items.

- Architecture and business process modelling (using the program ArchiMate).[5]
- Requirements analysis and software (demonstrator) development
- Stakeholder consultation in the form of workshops and interviews
- Joint learning in the forms of:
  - Design meetings
  - Roundtable discussions
  - Meetups
  - Presentation and discussions at seminars and conferences

When making the technology choices for BCT implementation in the pilot, the following aspects were taken into account:

- Feasibility, which is determined by the costs (including minimum required hardware, licensing costs, programming costs etc.) and complexity of the technology;
- Convenience, which is determined by the availability of software, experience, easy of deployment, etc.;
- Performance (number of participants allowed, speed and processing time etc.).

Furthermore, technological choices are often conditioned by the choice of governance models. This is particularly relevant to the choice of permissioned vs. permissionless blockchain that is explained in Section 3.1.

[5] http://www.archimate.nl/

3 Relevance of BCT to Agrifood

3.1 Principles of BCT

BCT uses a combination of technologies that have a considerable history in computer science and in commercial applications. These component technologies include public/private key cryptography (Rivest et al. 1978), cryptographic hash functions (Preneel 1994), database technologies especially distributed databases, consensus algorithms (Vukolić 2015) and decentralised processing. The fundamental purpose is to achieve database consistency and integrity in a context of a distributed decentralised database, where the database nodes are either controlled ('permissioned') or uncontrolled ('unpermissioned'), the prime example of the latter being Bitcoin.

BCT arose out of technology developed in the creation of Bitcoin (Nakamoto 2008). Bitcoin, as conceived by Satoshi Nakamoto, was an attempt to create a 'cryptocurrency' outside the control of government, a currency that would operate purely on the Internet (Grinberg 2011). Bitcoin was built on a number of key elements:

- A distributed file called a 'blockchain' spread over all computers participating in the system.
- Proof of work - in order to write on the 'blockchain' each node needed to complete a complex mathematical procedure (a process which eventually came to be called 'mining') in order to have the 'right' to write on the blockchain.
- Digital signatures - in order to know which person (using an identity expressed as a number) performed an operation each operation is signed using public-private keys.
- Chained hashes - this technology is widely used in version control and allows each documented to be 'hashed' into a digital 'summary'. A sequence of such hashes are used to construct the blocks in the blockchain.
- Byzantine consensus - the Bitcoin protocol claims to have solved the problem of 'byzantine consensus' which prevents 'double spend' of Bitcoins.

This enables the creation of a distributed database (a 'ledger') which can be used to record transactions of Bitcoins from one person (represented by their public key) to another. This database is immutable and ensures the impossibility of conflicting transactions.

Much has been written on the significance of Bitcoin in and of itself and its potential to transform various sectors mostly related to finance (Frisby 2014, Scientist 2017). Bitcoin led to a huge number of look-alike cryptocurrencies, and most public discussion has centred around the potential for illegal or illicit uses (such as the purchase of drugs on the Silk Road website). In keeping with the 'libertarian' origins of Bitcoin, it has been remarked that one of the major events which propelled Bitcoin to widespread adoption was the blockade of WikiLeaks by Visa and MasterCard, so Bitcoin was seen as a viable alternative payments medium which bypassed centralised control.

However, various people realised that the underlying technology of Bitcoin may have far greater interest. The Bitcoin software provides an 'unpermissioned' ledger for the recording of financial transactions but equally that ledger could be used to record non-financial transactions just like any ordinary database can. As the Ethereum White paper states:

> 'alternative applications of blockchain technology include using on-blockchain digital assets to represent custom currencies and financial instruments ("colored coins"), the ownership of an underlying physical device ("smart property"), non-fungible assets such as domain names ("Namecoin"), as well as more complex applications involving having digital assets being directly controlled by a piece of code implementing arbitrary rules ("smart contracts") or even blockchain-based "decentralised autonomous organisations" (DAOs)' (Buterin and et al., 2014-2016).

This realisation, which the has been ascribed to multiple authors, has led to a flowering of efforts to use initially the Bitcoin Blockchain for various non-cryptocurrency purposes, and then the creation of alternative platforms or systems (such as Ethereum and Hyperledger cf. below). Together with the realisation that blockchain technology could have a variety of other applications, there arose a number of start-ups seeking to find opportunities to exploit this technology. The start-ups have grown in number in areas ranging from finance to insurance, from logistics and now to agriculture and food.

The key principles of BCT can be outlined as follows:

- *Blocks in the blockchain*
  Each block in a blockchain contains a) an ordered set of records or transactions, and b) a hash of the previous block in its header (starting from an initial block called the 'genesis' block). This means its hash depends on the hash of its parent and so on in turn. This is key to blockchain security and guarantee of permanence since any change in the data of one block would affect all other blocks that follow. Such a change would require a new consensus process (typically involving 'proof of work' although not necessarily). A chain of such blocks forms a blockchain.
- *A peer-to-peer network*
  A blockchain depends a network of peers or 'nodes' who usually provide the computing power to achieve consensus for example by 'mining' if consensus is achieved by 'proof of work'.
- *A distributed immediately replicated file*
  Each blockchain is replicated across all 'nodes' or computers in the peer to peer network of that blockchain. The presence or absence of a particular node (e.g. being off-line) does not affect the operation of the blockchain as a whole, and this ensures guaranteed 'uptime'.
- *Consensus algorithm*
  In order for a new set of transactions to be written to a block, the block must be validated by a consensus algorithm. There are various such algorithms, the most common one being 'proof of work' where a node must solve a cryptographic puzzle thus entitling it to validate the new block (and in blockchains based on crypto-currencies to earn a 'coin'). The major issue with 'proof of work' is that it does not scale well in terms of the number of transactions. Other consensus algorithms include Byzantine fault-tolerant replication (Vukolić, 2015) and 'proof of stake' (currently being developed actively within the Ethereum project).
- *Cryptographic signatures*
  All transactions in a blockchain are cryptographically signed with public key cryptography to prove identity, authenticity and enforce read/write access rights.
- *Permissioned vs. unpermissioned blockchains or ledgers*
  As discussed in Walport (2016) blockchains (or as some people call them 'distributed ledgers') can be unpermissioned or permissioned. An unpermissioned blockchain has no single owner fulfilling the ideal that there is no central control. The best example is Bitcoin but the core Ethereum blockchain is also unpermissioned. A permissioned blockchain has a set of owners who control read/write/mining rights and thus operate the consensus algorithm. The Hyperledger Fabric works like this.
- *Smart contracts*
  Taking the distributed database concept one step further, Buterin proposed that a blockchain should be a virtual machine, a distributed computer that could run simple programs, so called 'smart contracts'. This raises the prospect of writing autonomous pieces of software which run independently of human intervention so called 'distributed autonomous organisations'.

Further details on the different technologies developed are provided below in Section 5.1.

3.2 Transparency and trust in agrifood: food integrity

The present-day supply chains are faced with many issues that have to do with the reliability of information: consumer trust, supply chain transparency, product quality, logistic issues, environmental impact, personal consumer data, fraud, food safety, etc. (Trienekens et al. 2012, Ge and Brewster 2016).

Consumers are increasingly concerned about the safety and sustainability of food and require more information on agrifood chains. The length and complexity of modern agrifood chains, however, have created a distance between consumers and producers that makes it infeasible for consumers to address their concerns and questions directly to the growers. Increasing demand for food information reflects the need for transparency and lack of trust. At the same time, more and more food products and beverages are branded and accompanied by a variety of certification schemes, with an increasing risk of fraud (selling unqualified product with high-quality labels or claims) and adulteration.

In the current situation, much of the compliance data and information is audited by trusted third parties and stored either on paper or in a centralised database and these approaches are known to suffer from many informational problems. Notable problems are:

- The high cost and inefficiency of paper-based processes.
- Fraud, corruption, error both on paper and in IT systems.
- Integrity of digital records (problems due to human error and data tampering).
- Double-spend of certificates.

These information problems have resulted in low transparency and trust in agrifood chains and pose severe threat to food safety, food quality, and sustainability. In particular, food integrity has become a major concern. Food integrity refers to the fairness and authenticity of food in food value chains both at the physical layer and the digital layer, where the digital layer should provide reliable and trustworthy information on the origin and provenance of food products in the physical layer.

Blockchain technology provides a means to ensure permanence of records and potentially to facilitate the sharing of data between disparate actors in a food value chain (although this is an open question). This potential may lead to an exciting paradigm shift facilitating transparency and trust in complex supply chains (Bessems and Bril 2017).

4 The Proof of Concept

A main aim of this project is to conceptualise and develop a proof of concept application based on a use case concerning table grapes from South Africa where BCT could be applied. This has been done by building a demonstrator (Spek et al. 2017) that keeps track of different certificates involved in the table grapes supply chain. The demonstrator has been built on a detailed analysis of the table grape supply chain and the interactions between farmers, certifiers, auditors, and table grape traders so as to enable a digital representation of a box of grapes to be associated with digital certificate.

The use case is described in detail in Appendix I, but can be summarised as follows: Organic table grapes are produced on a farm in South Africa, which consequently needs a certification authority, which is accredited by an accreditation authority, to confirm this is the case. This certification authority issues signing authority of an organic certificate to the farm, enabling the farm to certify the individual boxes of grapes it produces. These boxes of grapes are identified using a unique identification number (e.g. a bar-code). After certifying these grapes, they are shipped to a reseller in Europe, where they are sold to a supermarket and eventually to a customer. All the parties involved in this chain are able to verify the validity of the organic certificate issued by querying the blockchain. When the grapes change ownership, this is recorded in the blockchain as well and this enables anyone to check the provenance chain of the grapes. If the farm uses some kind of unauthorised pesticide, and this is discovered during an audit, then the auditor is able to revoke any certificate issued by the farm. This is recorded on the blockchain so anybody validating the certificate is able to see this. An auditor is also able to revoke accreditations on the level of an accreditation-body (the party issuing accreditations to certificate-bodies).

Architecture

The prototype has been built using Hyperledger Fabric (v0.6) and a reasonably complex 'Smart Contract' ('Chaincode' in Fabric terminology) which allows the relevant parties to update and query the data on the blockchain in view of their role and access rights. The fundamental architecture common to all blockchain systems assumes a shared distributed ledger. Hyperledger Fabric is designed for permissioned blockchains (cf. Section 5.1) and provides a membership management module for adding members to the blockchain. In view of the need to control participation in any given blockchain due to considerations of business confidentiality, this was considered the only possible choice among existing BCT Fabrics.

In Hyperledger Fabric, a member can be of different types, there are end-users, peers, and validators. End-users are users that have permission to execute transactions on the blockchain. Peers are nodes that keep a copy of the ledger. Validators also keep a copy, but also validate the incoming transactions and can participate in the consensus algorithm of the blockchain.[6]

As a distributed ledger, all nodes (peers and validators) have a complete copy of the whole blockchain but that does not mean all nodes have identical access to all data. Note that the approach adopted here does not involve hashing the data before placing it on the chain. The reason that in Hyperledger only certain participants have access to data is that smart contracts run inside a Docker container with their own key-value store (RocksDB for Hyperledger v0.6). Thus a smart contract can be designed to provide the smart contact participants access to the data within that database. However, all queries to the data must essentially be predefined in the functions written in the code.

For this demonstrator, we have also developed an API that allows for easy interaction with the blockchain. This API was developed using NodeJS. End-users can interact with the blockchain using a front-end application, which was also developed for this demonstrator. This (demo) front-end was

[6] For the purposes of the demonstrator, and to enable testing, the 'noops' consensus mechanism was chosen (i.e. accept all transactions) and thus the demonstrator ran on one node. Multiple nodes would have slowed down the system and in Hyperledger v0.6 the relevant consensus algorithm's implementation (PBFT) was known to be problematic.

developed using Angular.io (screenshot is shown in Figure 4.1). The basic architecture was designed as a set of Docker[7] containers which interact with each other as shown in Figure 4.2.

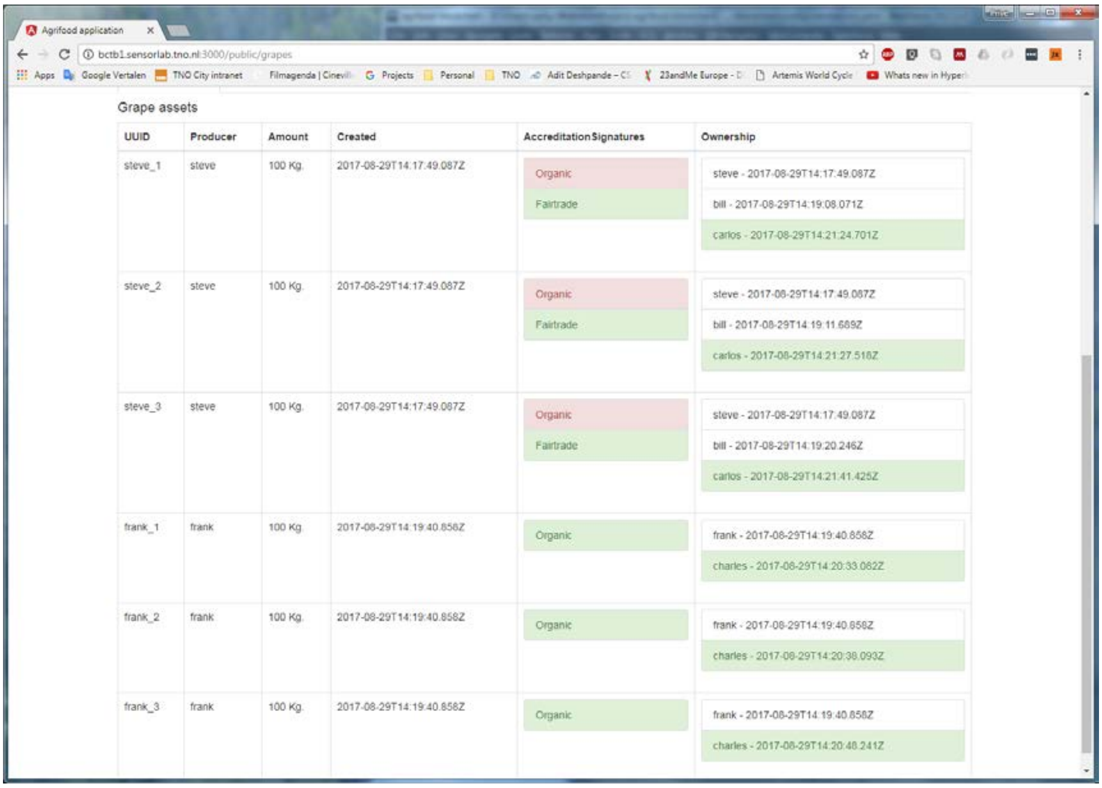

Figure 4.1 *Screen shot from demonstrator showing transaction history of grape shipments.*

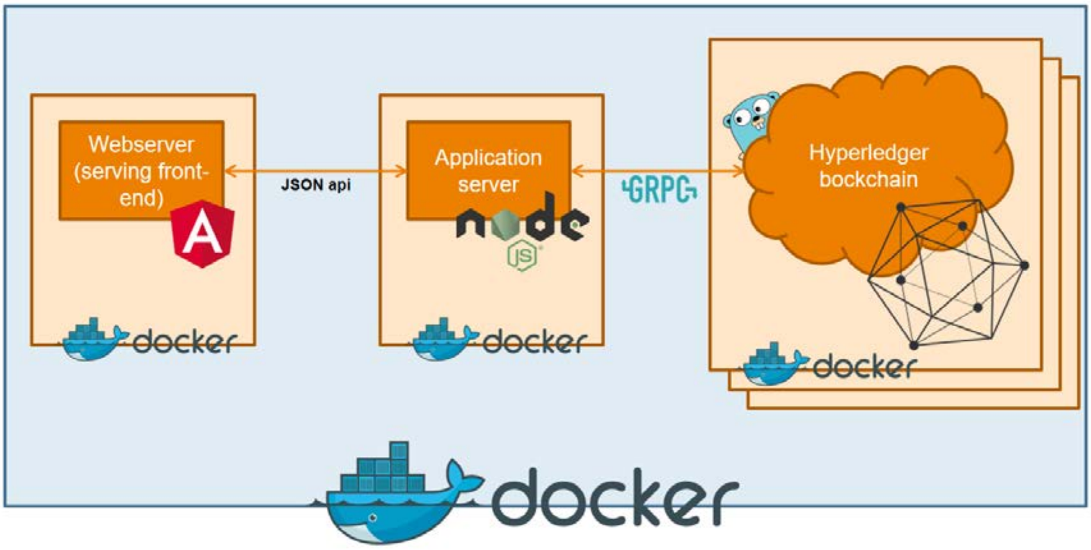

Figure 4.2 *Architecture of demonstrator*

A significant advantage of this architecture is that it allows easy launching of the demonstrator and thus can be deployed and extended without too much effort.

The source of the demo is publicly available at: https://github.com/JaccoSpek/agrifood-blockchain

7 Docker is a software technology providing containers, promoted by the company Docker, Inc., See more at: https://www.docker.com/what-docker

5 Findings from the pilot study

5.1 State-of-the-art: technological perspective

Alternative designs and implementations for BCT
The last three years (2014-2017) have seen a plethora of different blockchain software stacks (or 'fabrics') being developed reflecting a number of different design decisions both in terms of technical architecture and in terms of the governance of the software development (cf. Table 5.1).

Given the roots of blockchain technology in the libertarian Bitcoin initiative, most blockchain projects have started as a group of independent hackers setting up an open source initiative backed by a number of start-ups and as time passed larger more powerful software companies. The poster child here is Vitalik Buterin who wrote a white paper proposing the Ethereum project (Buterin and et al., 2014-2016), and with a number of collaborators launched this by advanced sale of the Ethereum cryptocurrency Ether (ETH) to owners of Bitcoin. This sale provided a working capital of USD 20m with which the Ethereum team undertook the development (Gerring, 2016). Other projects have been started by small companies or start-up (e.g. BigChainDB) or with the backing of open source groups (e.g. Hyperledger) and large companies (e.g. IBM's backing of Hyperledger). Most of these initiatives have provided their designs in the form of blogs or whitepapers published directly on the Internet rather than as academic papers reflecting the communities where these ideas sprang from.

Key technical choices include the following:

1. *Permission design*
   Bitcoin and Ethereum assume open, unpermissioned ledgers reflecting certain universalist ambitions, while Hyperledger (and most other fabrics) propose multiple blockchain each for a different commercial sector or community.
2. *Choice of consensus algorithm*
   Bitcoin and Ethereum, on the one hand, use a 'proof of Work' consensus algorithm, while Hyperledger and BigChainDB use much simpler voting methods. Hyperledger uses PBFT ('Practical Byzantine Fault Tolerance') (Castro et al., 1999; Strukhoff, 2017) which ensures high speed database consistency and is proven technology. There is considerable talk about the use of 'proof of stake' (where voting power is proportionate to the participant's investment) and there are plans to implement this in Ethereum (Buterin, 2017).[8]
3. *Smart contract*
   The inclusion or not of smart contract functionality is a core technical choice. Both Ethereum and Hyperledger ('chaincode') have emphasised the ability to run smart contracts on their technology stack. Bitcoin strictly does not have smart contract capability and BigChainDB avoids this functionality entirely. Smart contracts can be written in different computing languages. Ethereum provides 'Solidity' as a contract language, Hyperledger uses Go.
4. *Cryptocurrency*
   The use of a cryptocurrency is in fact partly dependent on the consensus algorithm chosen. If a 'proof of work' algorithm is chosen then of necessity, there has to be a cryptocurrency to incentivise participants to undertake 'mining'. However, there are cryptocurrencies (e.g. Ripple (Schwartz et al. 2014)) that use a simple voting method for their consensus algorithm.

[8] A number of less widely used blockchain 'fabrics' use versions of Proof of Stake including Peercoin, NXT

Table 5.1 *Example of Blockchain applications*

Name	Application	Smart contract execution	Smart Contract language	Consensus
BigChainDB (https://www.bigchaindb.com/)	Blockchain Database	N/A	N/A	Federated voting
Corda (https://www.corda.net/)	Smart contract	JVM	Kotlin, Java	Pluggable (RAFT, BFT, etc.)
Dfinity (https://dfinity.network/)	Smart contract	EVM	Solidity, Serpent, LLL	'Blockchain Nervous System' - Randomised POS
Monax (https://monax.io/)	Smart contract	EVM	Solidity	Tendermint (BFT)
Ethereum (https://www.ethereum.org/)	Smart contract, Cryptocurrency	EVM	Solidity	Ethash (PoW)
Hyperledger Fabric (https://hyperledger-fabric.readthedocs.io/en/latest/)	Smart contract	Dockers	Golang, Java	Pluggable (default PBFT)
MultiChain (https://www.multichain.com/)	Digital tokens			Randomised round-robin (mining diversity)
Ripple (https://ripple.com/)	Smart contract	-	-	Ripple Consensus Ledger (PoS)
Hyperledger Sawtooth (https://intelledger.github.io/)	Smart contract	TEE	Python	Proof of Elapsed Time
Stellar (https://www.stellar.org/)	Smart contract	Dockers	JavaScript, Golang, Java, Ruby, Phython, C#	Stellar Consensus Protocol
Tezos (https://www.tezos.com/)	Smart contract	Dockers	Tezos Contract Script Language	Proof of Stake

The leading blockchain technology stacks (or 'fabrics') include the following:

Ethereum (https://www.ethereum.org/)
One of the most influential fabrics is the *Ethereum Platform*, an initiative of Vitalik Buterin and Gavin Wood, which was funded by approximately USD 20m of bitcoin (Gerring 2016). The vision for Ethereum (Buterin and et al. 2014-2016; Wood 2015) was to create a blockchain-based distributed virtual machine which would allow 'smart contracts' to run as 'distributed autonomous' entities. This vision was a significant step in extending the vision as to what BCT was for and how it could be used. A 'smart contract' for Ethereum was a small piece of code that would be run 'on' the blockchain and crucially would function entirely independently without any possibility of censorship, downtime, fraud or third party interference. This enabled the vision of 'distributed autonomous organisations' which would be entities entirely specified in the smart contract code which could run without human interference, and because the blockchain has guaranteed up-time without any possibility of stopping. The creation of the Ethereum Virtual machine as a Turing complete virtual machine was a core innovation, capable of running any programme given enough resources ('gas') to run. Ethereum uses a cryptocurrency 'ETH' which is publicly traded on cryptocurrency exchanges, and an internal 'metering unit' called 'GAS'. Gas provides a means to provide transaction charges (including running smart contracts) and also allocate incentives for running the Ethereum VM. Ethereum currently uses a 'proof of work' mechanism for consensus but as noted above has plans to switch to a 'proof of stake' methodology.

Ethereum has had considerable mainstream success in being adopted by companies such as Microsoft and (initially) IBM to provide the underlying system for their own BCT offerings. A large proportion of blockchain start-ups and services are based on the Ethereum platform.

Hyperledger (https://www.hyperledger.org/)
The Hyperledger project was founded by the Linux Foundation with the intention of developing cross-industry collaboration in the area of BCT and with a focus on supporting business transactions. This

has meant a chief focus on *permissioned* blockchains. Many major technology companies and financial institutions were among founder members, although the most important and visible is IBM. Hyperledger is designed to be highly modular with the ability to plug in different alternative components for the same basic functionality. IBM has contributed 'Hyperledger Fabric' which is the most used blockchain technology stack after Ethereum. Following the modular design, Hyperledger Fabric (https://www.hyperledger.org/projects/fabric) allows components, such as consensus and membership services, to be plug-and-play. It allows for 'smart contracts' called 'chaincode'. The basic consensus mechanism is PBFT and there is no cryptocurrency because the design philosophy is for permissioned blockchain setups for specific business sectors. Apart from modularity and chaincode, key features of Hyperledger Fabric include:

- *Identity*
  A membership identity service that manages user IDs and authenticates all participants on the network
- *Privacy*
  Private channels which are restricted messaging paths that can be used to provide transaction privacy and confidentiality for specific subsets of network members.
- *Efficiency*
  Hyperledger Fabric uses a division of labour to assign different roles to different nodes claiming a consequent far greater efficiency of execution.

Partly due to the backing of IBM, Hyperledger has received widespread support and is being used in many different projects, including its use by Walmart in the pork supply chain (del Castillo 2016; Higgins 2017). We chose to use this technology for the Proof of Concept as reported above because of its identity management features and the ability to programme chaincode so as to allow access to certain kinds of data to the smart contract by different participants.

BigChainDB
In contrast to Ethereum, Hyperledger or other blockchain fabrics, BigChainDB (https://www.bigchaindb.com/) does not build a full stack of Blockchain technologies, but rather offers an overlay onto existing database technologies to 'blockchain-ify' them. 'BigchainDB is designed to merge the best of database and blockchain worlds: scale and querying from the database side, and decentralisation, immutability, and assets from the blockchain side' (McConaghy 2017). BigChainDB starts with an initial open source database (initially RethinkDB, now substituted with MongoDB) and have added blockchain characteristics including decentralised control, immutability, and creation and movement of digital assets (McConaghy et al. 2016). The main objective has been to overcome the widely recognised scaling problem that most blockchain projects suffer from. BigChainDB claims to be able to achieve over 1M transactions per second with this approach. The project sees itself as providing a technological component in a more conventional technology stack as shown in Figure 5.1.

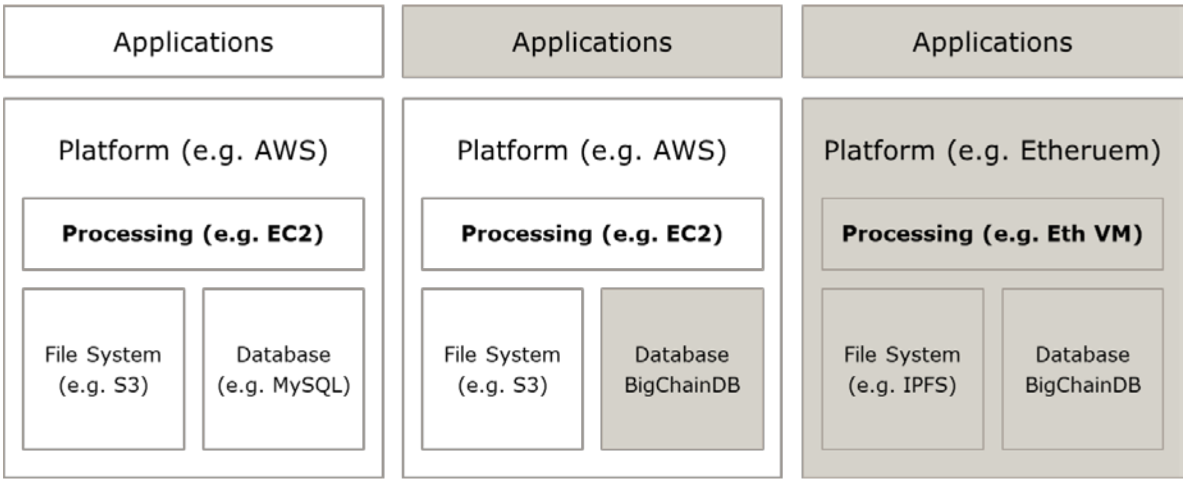

Figure 5.1 *Technology stack of BigChainDB.*
From McConaghy et al. (2016)

This means in part that BigChainDB explicitly excludes having a virtual machine or other mechanism for running ‘smart contracts’. In their approach, such a functionality would be provided by Ethereum or some other similar technology. The BigChainDB stressed three characteristics as being important:

- Decentralised control i.e. where no single entity controls the network.
- Immutability i.e. where data once written cannot be changed or tampered with
- Transfer of digital assets, i.e. the ability to create an asset and transfer this without central control.

A BigChainDB instance consists of a number of nodes all of which contain parts (but not all) of the complete database. Decentralised control is achieved by this DNS-like federation of nodes which have voting rights in the validation of blocks. Voting operates on a layer above the actual database and in order to achieve speed each block of transactions is written before being validated by a quorum of nodes. Nodes vote to validate a transaction and at validation time ‘chainify’ the block as each block provides a hash id of the previous block. Immutability is achieved through a combination of shard replication, disallowing reversions, database backups and cryptographic signing of all transactions (McConaghy et al. 2016, pp.12–13).

Scalability and Privacy of the BCT application

Two important aspects of the BCT application are scalability and privacy. Both issues present challenges in general for BCT applications.
Scalability refers to the capacity of the blockchain in terms of users and transactions.

Issues related to scalability of Bitcoin

The blockchain on which Bitcoin is based has some fundamental limitations (Greenspan 2015):

- *Limited transaction speed*
  Today the Bitcoin network is restricted to a sustained rate of 7 tps (transactions per second) due to the bitcoin protocol restricting block sizes to 1MB and the average block creation time of 10 minutes. Note that Visa has a peak tps of 56,000 transactions per second.
- *Limited payload size*
  As all blocks since the genesis block must be locally stored, the total size of a blockchain can become really huge. Keeping the payload limited helps managing the size. The current size of the Bitcoin blockchain is over 100Gb.
- *Transaction cost*
  Creating a new block does cost a notable amount of energy. Miners, creating a new block must be rewarded for their effort. Currently mining for Bitcoin consumes over 16TWh per year.
- *Irrelevant data*
  Institutions deploying over the bitcoin network need to process and store a large quantity of information that is of no interest to them. When a new bitcoin node is launched, it first downloads, verifies and stores the entire history of all bitcoin transactions.
- Increasing the block size or the transaction speed increases the risk of multiple forks on the block chain, which over time have to consolidate to a single branch.

For BCT to be successful and be widely adopted, the technology must be able to handle substantially greater data throughput than it currently can. Unless Bitcoin developers increase the block-size limit, Bitcoin will never be able to compete with the other payment providers. This issue of scalability affects all BCT ‘fabrics’ in one form or another.

Ethereum does not have a block-size limit, and had a much quicker block-rate of 1 block every 10-20 seconds (Ehrsam 2017). Nonetheless, the throughput of Ethereum, however, is limited by the gas-limit of the blocks (gas is best expressed as computational power needed to execute a smart-contract, analogous to gas used to drive a car). The gas-limit is set by the miners of the blocks by setting a new gas-limit on the mined block. The new gas-limit can only deviate by a certain amount from the previous block. So the network dynamically keeps a sensible block-size limit. Expressing the Ethereum throughput limits in transactions per second is not very meaningful, since transactions in Ethereum can contain a lot more data than just a simple value transaction. But Ethereum also suffers from throughput scaling limitations. These are limitations all blockchains have to deal with, since it’s a limitation intrinsic to the blockchain technology. These are the limitations caused by the consensus algorithms and the peer-to-peer network latency, and a number of solutions are being investigated and developed. As noted above, there are plans in Ethereum to move to a 'Proof of Stake' consensus algorithm partly to improve scalability (Buterin 2017).

Hyperledger Fabric claims significantly better scalability in part because it operates as a permissioned ledger and secondly does not depend on 'Proof of Work' but rather uses PBFT. Hyperledger is supposed to handle approximately 500 transactions per second, and recent developments may lead to over 1,000 transactions per second (Fujitsu 2017). Our proof of concept needs to be stress tested to determine in practice what actual throughput and performance is.

Issues related to privacy and security
One of the key features of BCT has been the supposed ease with which total transparency is achieved. All transactions in Bitcoin are visible because every node has a complete copy of the bitcoin blockchain and thus a complete record of all transactions. This is part of what makes possible the claim that bitcoin (and correspondingly all blockchain systems) are 'trustless' systems - due in part because of the automation of transactions between parties and partly because of the total transparency One of the key features of BCT has been the supposed ease with which total transparency is achieved. All transactions in Bitcoin are visible because every node has a complete copy of the bitcoin blockchain and thus a complete record of all transactions. This is part of what makes possible the claim that bitcoin (and correspondingly all blockchain systems) are 'trustless' systems - due in part because of the automation of transactions between parties and partly because of the total transparency (Goswami 2016). From a business perspective, total transparency is not tenable since much of the business is dependent on varying degrees of opacity (Shrier et al. 2016, Goswami 2016).

This problem of transparency was one reason the Proof of Concept chose to use Hyperledger because data could be wrapped within a smart contract and made available or 'visible' only to the participants in the at smart contract. This ensures that business confidentiality is retained. However, access to data has to be written into the smart contract from the start, and thus it is impossible to give post-hoc access to data to a new actor.

A further significant issue with regard to privacy is the EC's General Data Protection Regulation (GDPR). First, open unpermissioned blockchains like Ethereum are entirely decentralised and distributed which means there is no single entity with legal responsibility for data processing on the blockchain. In a permissioned blockchain like Hyperledger, in theory at least there is an entity responsible for participation in the Blockchain. Second, blockchains are designed to be immutable, but in accordance with the GDPR data needs to be completely removed if the relevant individual requests it. Furthermore, specific parts of the GDPR depend on the location where data is being processed, and obviously on the blockchain data is being processed everywhere and nowhere. These issues will have to be addressed by a combination of changes in regulation and developments in technology.

Standards and the relation to and interaction with existing information systems
BCT, as a technology, is often promoted as a solution to problems of interoperability between systems (Korpela 2017). The fundamental idea is that if there is a common database, a backbone, that all participants in an industry (or a supply chain) can access, read and write to, then all past frustrations with the absence of interoperability can be overcome. This perspective is, in our view, very optimistic for a number of reasons.

Interoperability with legacy systems
Even if we could conceive a universal database (or even a sectoral one) accessible to all participants, there is a large installed base of legacy systems with which any BCT system would need to be able to communicate. This is of course a challenge for any new technology but particularly so for a technology with claims to universal application. Currently, the majority of BCT applications and services are designed from scratch without taking into account the installed base of existing systems, the necessary middleware and the mapping of data. One prominent exception is Ripple (a blockchain based payments system with its own cryptocurrency) which has integrated its service across multiple ledgers and legacy systems (de Castillo 2017).

Interoperability between blockchain systems
It has gradually dawned on the blockchain community that there will not be 'one blockchain to rule them all'. There are many aspects of interoperability and standardisation which need to be considered as a consequence, as well a variety of use cases. Buterin (2016) lists as potential use cases:

- Portable assets
- Payment-versus-payment or payment-versus-delivery (or atomic swaps)
- Cross-chain oracles
- Cross-chain contracts

Equally there exist a variety of aspects of BCT which will need to be standardised in order to achieve an effective ecosystem. Buterin (op. cit.) discusses a range of such technological issues for blockchain interoperability. Furthermore, there exist a number of initiatives by standards organisations (ISO, UNCEFACT, W3C) and others (Hyperledger foundation) to develop standards for BCT interoperability at the protocol or smart contract level. As noted by Underwood (2016), data should be able to be processed on Hyperledger but reside on an Ethereum blockchain. Such interoperability has not yet been widely addressed. In this area, there is considerable work to be done.

5.2 State-of-the-art: stakeholder perspectives and acceptance

Key stakeholders
The distributed nature of the BCT means that the implementation of BCT inevitably involves multiple stakeholders. Key stakeholders in the pilot use case include the following:

- Producers of table grapes, this include growers and growers' organisations
- Traders (exporters and importers of table grapes)
- Logistics companies
- Product standard organisations (e.g., certification scheme owners)
- Data/Information standard organisations (e.g., UN/CEFACT)
- Certification organisations
- Supervisory authorities, this include for example accreditation authorities and food safety authorities
- Financial service providers (e.g., banks and investors)
- ICT services and solution providers

In implementing a BCT solution, these stakeholders are the 'usual suspects' for which the costs and benefits of BCT must be assessed. However, the adoption of BCT may change the business ecosystems by introducing new players and changing the position of existing players in the ecosystem. Unusual suspects in the adoption of BCT include parties that indirectly make use of the information exchanges such as insurance companies, or third party identity management providers. Furthermore, the novelty and promises of BCT makes it increasingly popular among start-ups who will seek to disrupt existing players.

Knowledge and engagement of key stakeholders
This project has had active participation of various stakeholders. The growing interest of various stakeholders is also evidenced by their presence at physical and virtual meeting and meetups. Questions and comments raised during numerous interviews and meetings showed high diversity in the level of knowhow in blockchain and expectations of the technology. Based on their general level of know-how and engagement in BCT research and implementation, stakeholders can be divided into four groups (Figure 5.2), where a large number of stakeholders show high-level of engagement in this project.

Many blockchain aspirants are familiar with the problems in the agrifood chain and encouraged by the promises of BCT but often lack the know-how and can have unrealistic expectations of the technology. This is in stark contrast with 'blockchain onlookers' who know too well about the challenges and limitations of the technology to promote the application of it to real life cases. It is generally agreed that the main challenge at the moment is to identify the right use cases and demonstrate the added value of BCT for different businesses and parties.

A considerable level of scepticism among stakeholders with low know-how of BCT exists, partly due to the way blockchain is portrayed as a panacea to all information problems, partly due to a number of technical issues that remain to be resolved. Due to its foundational nature, the adoption of BCT is likely to be a long process (Iansiti and Lakhani 2017).

The main concerns of our stakeholders include the following:

- The reliability of data that is put into the blockchain, often put as the 'Garbage in- Garbage out'-phenomenon;
- Environmental impact of mining;
- How to deal with different blockchains that will arise;
- The validity and consistency of smart contracts;
- The effectiveness of BCT in preventing fraud in the food chain.

Most of these concerns can in time be solved or alleviated by technological advancement (e.g., the use of machine-generated data) or institutional arrangements (e.g., the development of standards for blockchains and smart contracts). While the use of BCT is expected to discourage data tampering, it can never prevent people from putting false or erroneous information in the system or hiding information from the blockchain. BCT alone will therefore not eliminate fraud in the food chain. However, when more and more data are available and linked to BCT, it will become easier to detect and trace fraud due to the possibility of using cross-checks and the immutability of records. This may then significantly lower the likelihood of fraudulent information from entering the information system.

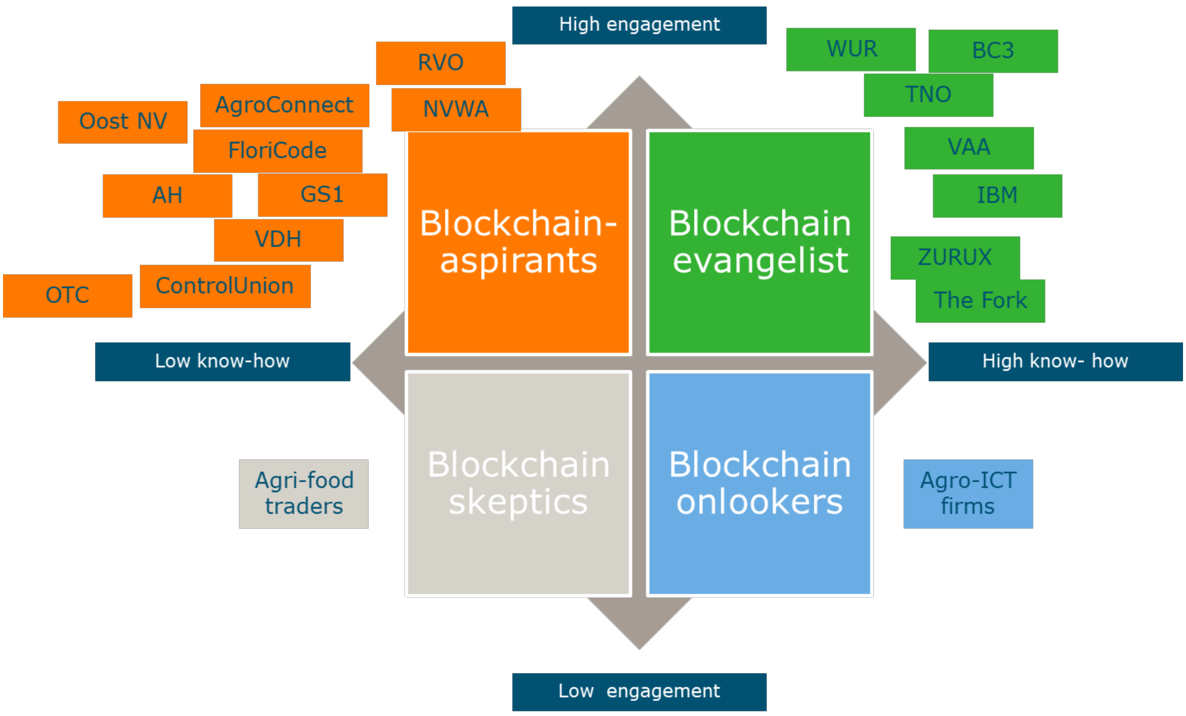

Figure 5.2 *Level of knowhow and engagement of key stakeholders in the ecosystem of the pilot*

5.3 Feasibility and added value of BCT as shown by the Proof of Concept

The demonstrator showed the conceptual feasibility of using the technology to solve a specific problem within the agricultural supply chain viz. the tracking of food certificates and the real time updating of these should validity change. We showed by the design of the architecture that such a system can both provide the relevant data to the relevant participants, can keep business confidentiality, and can propagate data effectively between the participants using blockchain technology. Thus the demonstrator showed that blockchain technology could be used successfully in such a context.

Furthermore, given the experimentation undertaken, it was shown that a medium size server (e.g. on the cloud) could function adequately as a node for the purposes of this type of use case. There is no need for special hardware, and all the software infrastructure (in this case Hyperledger Fabric) is open source and free.

5.4 Opportunities and challenges

Opportunities and learning objectives

Technological advancement is seldom neutral. BCT will be no exception. As discussions and consultations with stakeholders have made clear, BCT will create different opportunities and challenges for different stakeholders or organisations, depending on their current position in the market and in the value chain of food information.

To obtain insights into their views and stimulate discussions and joint learning, individual interviews, roundtable sessions and informal meetups have been organised on the opportunities and challenges. Table 5.2 shows the key opportunities, challenges and learning objectives as identified by the stakeholders in this pilot study.

Table 5.2 *Opportunities, Challenges and learning objectives for different stakeholders*

Stakeholders	Opportunities	Challenges	Learning objectives
Food producers	• Added value to food products with credence attributes due to increased transparency and assurance of provenance information • Fairer price and lower costs due to the removal of intermediaries • Better access to global market • Access to alternative financing arrangements • Direct contact with consumers	• Organising BCT implementation • Access to established blockchain • Getting the right conditions into smart contracts	• General knowledge of BCT • How to benefit from BCT
Certification bodies	• Increased value of certificates due to the improved transparency and reliability of certificates • Lower transaction costs due to efficient process • Risk based auditing	• New competencies needed • Potential threat to current business model	• How BCT can enhance the chain of custody and efficiency of certification processes
Governmental organisations (RVO, NVWA)	• Reliable data • Efficient regulatory processes • Lower transaction costs	• New competencies needed • Existing national and international regulatory framework	• Understanding the social implications of BCT • Identifying key use cases
Retail/Trader	• Improving transparency and traceability • Access to more information on the provenance of food products • Providing reliable information to consumers • Improving brand image	• Compatibility with existing systems • Compliance of other players in the supply chain • Privacy concerns • Traceability and provenance of compound products • Scalability of BCT	• Understanding the potential of BCT • Identifying and prioritise key use cases
Producers of digital equipment (e.g. sensors)	• Increasing market for hardware products • Increasing potential to capitalise on data captured	• Interoperability • New competence needed	• How to design blockchain-ready products
Standard organisations on sustainability (e.g., Organic)	• Potential to reduce transaction costs due to removal of intermediary processes	• Harmonisation of standards • Choice of indicators	• How to use BCT to improve compliance to standards
Standard organisations on information standards (e.g., GS1)	• Enhancing the implementation of standards through BCT	• Compatibility with existing standards	• How to take into account the implications of blockchain in norm setting
Knowledge institutions	• Deriving more value of existing data and information systems in agrifood domain • New research opportunities	• Identifying the right problems and partners • Establishing research consortium for trial and exploration	• How BCT can be used to enhance knowledge generation and dissemination
Agro-ICT companies	• Increasing market potential for providing software solutions	• Identifying the right use cases and users	• How to apply BCT to create new value proposition
Blockchain start-ups	• Initiating new business opportunities • Supporting social innovation with distributed governance models	• Finding the right funder and partners	• How to build minimum viable ecosystem for BCT implementation

Potential applications

Based on the inventories and discussions during meet-ups, the key areas of application are the following:

- Registration of holdings, animal, plant and transactions;
- Tracking and tracing of products with credence attributes (i.e., qualities that are not directly observable by users or end consumers). This can potentially enhance the developments in true pricing (or true cost accounting) that aim to convey information on the externalities of food production;
- Transfer of import & export certificates (e.g., SPS certificates);
- Inclusive development by ensuring access of smallholders to better market and better payments or financing possibilities (e.g., FairFood, AgriLedger);
- Creating opportunities of automating business processes triggered by a conditioned transaction (in case using smart contracts);

Challenges

At the moment, few blockchain applications concerning real life cases have gone beyond the phase of 'Proof of Concept' or small-scale pilots. Scalability is likely to be a major issue in real-life implementation of BCT. Larger-scale implementation of BCT concerns both technological scalability (number of nodes, amount of data and number of transactions) and social scalability (the number and types of users). Adoption of BCT by parties in the agrifood chain is key to solving the social scalability issue. More specifically, the following questions must be addressed:

- How to link physical flows to information flows?
- How to establish minimum viable ecosystem?
  - How to cope with the rapid tempo and dynamics in the implementation process
  - How to strike the balance between creating widespread support and forming committed parties.
  - How to collaborate with international parties

5.5 Research needed

Despite all the attention received, BCT is still in its relative infancy. There is a wide range of technical and socio-economic challenges which need to be addressed before the technology can really have an impact on the business sector (as it is widely claimed). Because agrifood is a sector with impacts across society and the environment, almost all aspects of research concerning the fundamentals of BCT are relevant to this sector. Areas of future research need to address the issues already briefly described in Sections 5.2 and 5.3. We would focus for the purposes of agrifood sector particularly on the following:

- Use cases or problem areas where there is a business case for key stakeholders for applying blockchain with viable business models and governance. Food integrity and inclusive development are two key themes in this regard.
- Scalability (technological – throughput in in terms of number of transactions).
- Digital to physical interface: connecting BCT applications with precision agriculture, big data, sensors and IoT platforms, connecting to electronic readable labels (identifiers of physical goods) such as RFID, barcode or 2D grid codes and event recording. The recorded event can be included in a blockchain on this product/supply chain;
- Semantic models and data models – specifically the integration of existing data models with BCT so as to enable wider interoperability.
- Querying of data on the blockchain, and access management.

6 Discussion and policy recommendations

6.1 Discussion

Added values and limitations of BCT for agrifood applications

At the moment (October 2017), few would question the relevance of BCT to agrifood. The main question is rather on the added value of BCT compared to existing IT solutions or other non-IT solutions (i.e. new organisational models) in real life cases. This PoC pilot has demonstrated that it is feasible to put basic information on certificates on a blockchain with a permissioned ledger and smart contract. Compared to traditional situations with centralised databases, the PoC demonstrator shows how blockchain can be used to ensure that different parties share the same layer of information on the validity and provenance of certificates that is tamper-proof.

There are several limitations to the PoC demonstrator. First of all, the amount of data and information that is shared is very limited. As with most PoC pilots, the project has not yet been able to demonstrate how the system would perform when handling a very large number of transactions (as is the norm in the food supply chain). Given the limited scope of the project, it remains to be determined what the resource consequences and throughput capacity of our system would be. Furthermore, our demonstrator focussed on one smart contract with all participants able to read and write. This is for the sake of simplicity. In practice, however, multiple smart contracts would need to be deployed for the different contractual relationships and so as to keep the transaction data visible only to the relevant subset of participants (or businesses). An aspect that would need to be addressed is the interaction between smart contracts and the feasibility of data flows between smart contracts. Finally repeated errors in smart contract design have shown that testing, validation and rigorous semantics are essential if significant damage is to be avoided in business relations. The limitations of the PoC demonstrator, however, have little impact on its value in improving the understanding of BCT, but rather suggest directions for further research. To obtain better insight into the added value of BCT in more real life cases, these issues should be addressed in further research and exploration.

Organising blockchain-ready agrifood chain

As a new technology, BCT is far from being well understood by both technology developers and other parties in the ecosystem. During the development of the pilot, a number of lessons or observations have been learned with regard to the technology itself and how stakeholders view the technology:

- BCT is not a panacea to all problems. It may not necessarily outperform existing systems or offer added value to existing businesses;
- A blockchain cannot store as much data as people would expect from ‘putting data on the blockchain’. In many use cases, only references to databases are stored in the blockchain;
- The mechanics and social-economic implications of the technology are still not well understood among most stakeholders. As a results, most stakeholders are not ready yet for a paradigm shift towards blockchain-ready food chain.

The adoption of new technologies often takes time and besides the novelty and complexity of the technology, chances play an important role as well. The implementation and adoption of BCT is likely to be even a lengthier processes due to its foundational nature (Iansiti and Lakhani 2017). The implementation of BCT implies the organisation of a social-economic order through code rather than through institutions—this requires joint effort and concerted actions of different parties that by default have no trustful relationships among each other. To move forward, it is important to have dialogues among each other to achieve better understanding of each other’s interests and stakes and identify common grounds for applying BCT. Experience in this project shows that meetups where different use cases are presented and discussed by various stakeholders are a good mechanism to grow the ecosystem of BCT in agrifood.

6.2 Policy recommendations

Given the rapidly increasing level of digitalisation and demand for information and product integrity, the agrifood sector is in a unique position to explore the potential of BCT. Although the application of BCT in agrifood is currently still in its infancy, it can be expected that more and more initiatives will be taken by various organisations. Left uncoordinated, this can result in the waste of resources and missed opportunities for businesses and society as a whole.

From a policy perspective, the following recommendations can be made:

- Support and stimulate development of BCT applications as part of the digitalisation strategy to improve transparency, efficiency, competitiveness and sustainability of the agrifood sector;
- Facilitate and encourage the growth of the ecosystem of blockchain-minded parties in agrifood chains;
- Design and implement a clear regulatory framework for blockchain implementations in agrifood domain;
- Provide government investment in research and innovation so as to develop the evidence for the added value of the technology.

With special attention to:

- Development of guidelines for proof of concept (PoC) projects and large-scale implementation;
- Development of standards and knowledge base regarding BCT implementation;
- Awareness raising of new governance and organisational mode implied by BCT and its implications for business and policy through knowledge dissemination;
- Ecosystem development around blockchain implementation around themes such as transparency, food integrity and traceability in agrifood chains.

The competiveness of farming and agrifood SMEs is a key policy issue for the Netherlands. To harness the power of BCT requires the adoption of BCT by many SMEs in farming and agribusiness. Most SMEs are however too small or lack the expertise to invest in BCT by themselves. Furthermore, given the current development of BCT, the uncertainties are too high to develop a convincing business case for individual parties. It is therefore important to address the application issues in public research agendas. The main focus of research is not on the BCT technology itself, but on the application of it to suitable use cases.

References and websites

Bessems, P. and W. Bril (2017). *Blockchain organiseren - fundamenten voor een nieuwe sociaaleconomische orde*, Mijnmanagementboek.

Frisby, D. (2014). *Bitcoin: The Future of Money?*, Random House.

Ge, L. and C.A. Brewster (2016). 'Informational institutions in the agrifood sector: meta-information and meta-governance of environmental sustainability.' *Current Opinion in Environmental Sustainability* 18: 73-81.

Greenspan, G. (2015). 'MultiChain Private Blockchain — White Paper.' https://www.multichain.com/download/MultiChain-White-Paper.pdf.

Grinberg, R. (2011). 'Bitcoin: An innovative alternative digital currency.'

Iansiti, M. and K. R. Lakhani (2017). 'The Truth About Blockchain.' *Havard Business Review* January-February: 118-127.

McConaghy, T., R. Marques, A. Muller, D. De Jonghe, T. McConaghy and G. McMullen, et al. (2016). BigChainDB: A Scaleable Blockchain Database. Ascribe GmbH Available at: https://www.bigchaindb.com/whitepaper/. [Accessed May 11, 2017].

Nakamoto, S. (2008). 'Bitcoin: A Peer-to-Peer Electronic Cash System.' www.bitcoin.org.

Preneel, B. (1994). 'Cryptographic hash functions.' *Transactions on Emerging Telecommunications Technologies* 5(4): 431-448.

Rivest, R. L., A. Shamir and L. Adleman (1978). 'A method for obtaining digital signatures and public-key cryptosystems.' *Communications of the ACM* 21(2): 120-126.

Scientist, N. (2017). *The End of Money: The story of bitcoin, cryptocurrencies and the blockchain revolution (New Scientist Instant Expert)*, John Murray Learning.

Trienekens, J. H., P. M. Wognum, A. J. M. Beulens and J. G. A. J. van der Vorst (2012). 'Transparency in complex dynamic food supply chains.' *Advanced Engineering Informatics* 26(1): 55-65.

Vukolić, M. (2015). *The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication.* International Workshop on Open Problems in Network Security, Springer.

Walport, M. (2016). Distributed Ledger Technology: Beyond Blockchain. Government Office for Science Available at: https://www.gov.uk/government/publications/distributed-ledger-technology-blackett-review.

Korpela, K., J. Hallikas, and T. Dahlberg (2017). Digital Supply Chain Transformation toward Blockchain Integration. In *Hawaii International Conference on System Sciences (HICSS) 2017*. https://doi.org/10.24251/HICSS.2017.506

Underwood, S. (2016). Blockchain Beyond Bitcoin. *Communications of the ACM*, *59*(11), 15–17. https://doi.org/10.1145/2994581

Buterin, V. (2016). *Chain interoperability*. r3cev.com. Retrieved from https://www.r3cev.com/s/Chain-Interoperability-8g6f.pdf

del Castillo, M. (2017, June 2). Interoperability Boost: Ripple Sends Blockchain Transaction Across 7 Ledgers - CoinDesk. Retrieved 4 September 2017, from https://www.coindesk.com/interoperability-boost-ripple-sends-blockchain-transaction-across-7-different-ledgers/

Websites

Buterin, V. (2017). Proof of Stake FAQ. Ethereum Wiki. Available at: https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ

Buterin, V., et al. (2014-2016). Ethereum White Paper - A Next-Generation Smart Contract and Decentralized Application Platform. https://github.com/ethereum/wiki/wiki/White-Paper.

Castro, M., B. Liskov, et al. (1999). Practical Byzantine fault tolerance. in OSDI (usenix.org), 173–186. Available at: https://www.usenix.org/events/osdi99/full_papers/castro/castro_html/castro.html.

del Castillo, M. (2016). Walmart Blockchain Pilot Aims to Make China's Pork Market Safer - CoinDesk. CoinDesk. Available at: http://www.coindesk.com/walmart-blockchain-pilot-china-pork-market/ [Accessed June 21, 2017].

Ehrsam, F. (2017) *Scaling Ethereum to Billions of Users – Fred Ehrsam – Medium* [online]. Available from: https://medium.com/@FEhrsam/scaling-ethereum-to-billions-of-users-f37d9f487db1 (Accessed 28 August 2017).

Fujitsu (2017). Fujitsu Speeds Up Transaction Processing on the Blockchain – CoinSpeaker. (2017, July 31). Retrieved 28 August 2017, from https://www.coinspeaker.com/2017/07/31/fujitsu-speeds-transaction-processing-blockchain/

Gerring, T. (2016). Cut and try: building a dream - Ethereum Blog. Ethereum Blog. Available at: https://blog.ethereum.org/2016/02/09/cut-and-try-building-a-dream/ [Accessed May 11, 2017].

Goswami, D. (2016). Unchaining Blockchain: The Ultimate Transparency Tool? | Government Innovators Network. Retrieved 6 November 2016, from https://www.innovations.harvard.edu/blog/unchaining-blockchain-ultimate-transparency-tool

Higgins, S. (2017). Walmart: Blockchain Food Tracking Test Results Are 'Very Encouraging' - CoinDesk. CoinDesk. Available at: http://www.coindesk.com/walmart-blockchain-food-tracking-test-results-encouraging/ [Accessed June 21, 2017].

McConaghy, T. (2017). BigchainDB 2017 Roadmap – The BigchainDB Blog. The BigchainDB Blog. Available at: https://blog.bigchaindb.com/bigchaindb-2017-roadmap-d2e7123f9874 [Accessed May 11, 2017].

Schwartz, D., N. Youngs and A. Britto (2014). The Ripple protocol consensus algorithm. Ripple Labs Available at: https://ripple.com/files/ripple_consensus_whitepaper.pdf.

Shrier, D., J. Larossi, D. Sharma, and A. Pentland (2016). Blockchain & Transactions, Markets and Marketplaces. cdn.resources.getsmarter.ac. Retrieved from http://cdn.resources.getsmarter.ac/wp-content/uploads/2016/08/mit_blockchain_transactions_report.pdf

Strukhoff, R. (2017). Hyperledger Fabric's Chaincode, Practical Byzantine Fault Tolerance, and v1.0 - Cloud Foundry Live | Altoros. Cloud Foundry Live | Altoros. Available at: https://www.altoros.com/blog/hyperledger-fabric-chaincode-practical-byzantine-fault-tolerance-and-v1-0/ [Accessed August 14, 2017].

Wood, G. (2015). Ethereum: A Secure Decentralised Generalised Transaction Ledger - Homestead Revision. Personal Website. Available at: http://gavwood.com/paper.pdf.

Fujitsu (2017). Fujitsu Speeds Up Transaction Processing on the Blockchain – CoinSpeaker. (2017, July 31). Retrieved 28 August 2017, from https://www.coinspeaker.com/2017/07/31/fujitsu-speeds-transaction-processing-blockchain/

Adi Ben-Ari, AppliedBlockchain https://appliedblockchain.com/outstanding-challenges-in-blockchain-2017/

Experience of pilots by Dutch government: https://www.ictu.nl/nieuws/resultaten-blockchainpilots-overheid-en-blockchainlab\

Introductions in Dutch:

- http://www.bitcoinevangelist.nl/
- http://innovators.kpmg.nl/nl/blogs/the-blockchain-promise/
- http://tegenlicht.vpro.nl/bijlagen/2015-2016/bitcoin-evangelie/blockchain.html

Blogs:

- http://www.martijnbolt.com/nl/home/
- https://blog.blockchain.com/
- https://bitsonblocks.net/2017/03/07/three-common-misconceptions-about-smart-contracts/

Information about the Pilot:

- https://time.tno.nl/en/articles/pilot-project-shows-that-blockchain-and-agri-food-are-a-fertile-combination/

Appendix 1 Use case description

To prove the added value of using blockchain technologies in the agrifood sector, this project implemented a simple use-case around the certification and provenance of table grapes from South Africa.

Goals

The goal of this proof-of-concept application is to show and further explore the added value of using blockchain in the agrifood sector. This use-case should address the following functions:

- *Provenance*
  Using the blockchain it should be possible to track the provenance of products from the buyer all the way back to the producer (audit-trail, chain of custody).
- *Issuing and validation of certificates*
  Certification authorities can issue certificates to products. These should be registered on the blockchain so it will be possible for all participants of the blockchain to verify the validity and issuer of a certificate. It should be possible for a certification authority to authorise other companies to issue certificates on their behalf (for example, once a farm is certified as organic, it can certify its own grapes as organic on behalf of the certifying authority). Certifying authorities can also revoke certificates issue by them or on their behalf.
- *Audit of certificates*
  Auditing organisations should be able to revoke certificates, but are also able to bar a certification organisations form issuing certificates when there is fraud or any other unethical behaviour. Results of audits should also be visible on the blockchain.

General description of the use-case

To achieve these goals using a blockchain implementation, we've designed a use-case that needs all the goals to be implemented.

The use-case is focused around the grapes supply chain. The grapes in our use-case are produces on a farm in South Africa. This farm produces organic grapes, so it needs a certification authority to confirm this is the case. This certification authority then issues a certificate to the farm, enabling the farm to certify the individual boxes of grapes it produces. These boxes of grapes are identified using a unique identification number (e.g. a bar-code).

After certifying these grapes, they are shipped to a reseller in Europe, where they are sold to a supermarket and eventually to a customer. All the parties involved in this chain should be able to verify the validity of the issued organic certificate.

Also, when the grapes change ownership, this should be recorded in the blockchain as well (except of course for the end-consumer), this would enable anyone to check the provenance chain of the grapes: How did they end up in the supermarket.

When it turns out the farm used some kind of unauthorised pesticide, and this is discovered during an audit. The auditor should be able to revoke any certificate issued by the farm. This should be recorded on the blockchain so anybody validating the certificate will be able to see this.

Roles in this use-case

Name:	General role	Role on the blockchain
Farmer	Produces table grapes and certifies the table grapes using a signing certificate received from a certificate authority	• Creates table grape-assets (boxes) in the blockchain • Certifies the table grape-assets using a certificate obtained from a certificate authority • Transfers the table grape-assets to other parties (shippers, resellers etc.)
Standard organisations		
Certificate authority	Trusted party that issues a certain type of certificate for table grapes (or allows other parties to certify product) Is also responsible for checking the conditions of the certificate	• Certify table grape-assets • Allow other parties to certify table grape-assets • Revoke certificates on assets • Revoke certification authority of other parties (it previously allowed)
Auditor	Other trusted party that checks the certification authority or farmer to see if they operate correctly	• Revokes certificates • Revoke certifying authority of any certificate authority • Publish audit certificates of table grape-assets • Publish audit certificates of farms • Publish audit certificates of certificate authorities
Trader	Buys and sells large quantities of table grapes	• Receive and transfer ownership of the table grape-assets • Check certificates • Check provenance
Shipper	Distributes the table grapes between parties	• Receive and transfer ownership of the table grape-assets • Check certificates • Check provenance
Supermarket	Sells the table grapes to the consumer	• Receive and transfer ownership of the table grape-assets • Check certificates • Check provenance
Customer	Buys table grapes in small quantities from sellers	• Check certificates • Check provenance
Shipper	Distributes the table grapes between parties	• Receive and transfer ownership of the table grape-assets • Check certificates • Check provenance

Wageningen Economic Research
P.O. Box 29703
2502 LS The Hague
The Netherlands
T +31 (0)70 335 83 30
E communications.ssg@wur.nl
www.wur.eu/economic-research

Wageningen Economic Research
REPORT
2017-112

To explore the potential of nature to improve the quality of life

Wageningen Economic Research
P.O. Box 29703
2502 LS Den Haag
The Netherlands
E communications.ssg@wur.nl
www.wur.eu/economic-research

Report 2017-112
ISBN 978-94-6343-817-9

The mission of Wageningen University and Research is "To explore the potential of nature to improve the quality of life". Under the banner Wageningen University & Research, Wageningen University and the specialised research institutes of the Wageningen Research Foundation have joined forces in contributing to finding solutions to important questions in the domain of healthy food and living environment. With its roughly 30 branches, 5,000 employees and 10,000 students, Wageningen University & Research is one of the leading organisations in its domain. The unique Wageningen approach lies in its integrated approach to issues and the collaboration between different disciplines.