BACHELOR THESIS

Sharing intangibles in the supply chain, when do I need a blockchain?

Author:	Pieter Miedema
Date:	18-06-2021
Location:	Oranjewoud
Company supervisor:	Maxime Bouillon
Organization:	Spark! Living Lab
University:	Hogeschool Windesheim, Zwolle

BACHELOR THESIS

Sharing intangibles in the supply chain, when do I need a blockchain?

Author:	Pieter Miedema
Student number:	s1118523
University:	Hogeschool Windesheim, Zwolle
Study:	Finance & Control
VOE-code:	BEvAFST.2021
Graduation period:	01-02-2021 until 18-06-2021
Name of the organization:	Spark! Living Lab
Supervisor of the organization:	Maxime Bouillon
University supervisors:	Bart Scholten & Frank Evers
Date:	18-06-2021

Preface

Since the cryptocurrency boom in 2017, one of the many, I became interested in cryptocurrencies and the technology behind these cryptocurrencies, blockchain. I hesitated to get into the cryptocurrency realm to hunt for the enormous gains shown on the news. But when the bear market kicked in, I gradually lost my focus and interest in this space.

Until I attended a meeting at my previous internship at Aegon N.V. where a colleague gave a presentation about Bitcoin. He did not focus on the big profits that were gained, but he gave an in-debt explanation of the blockchain technology behind it. Since that moment, I regained my interest in blockchain technology and figured out how I could learn more about this. I was delighted to hear that I could integrate this topic into my study by doing the minor Blockchain & Cryptocurrencies, Business, IT & Law at The Hague University. I became so fascinated by this topic that I did not want to stop learning about blockchain technology.

I would like to thank the people at Spark! Living Lab, especially Maxime Bouillon, for giving me the opportunity to graduate at their organization and learn more about blockchain technology. Also, to all the people who are not connected to Spark! Living Lab but with whom closely worked together, herewith I would like to thank you.

Finally, I want to thank Bart Scholten and Frank Evers for all the guidance and feedback from Windesheim and for keeping me on my toes.

I hope you enjoy your reading,

Pieter Miedema

Oranjewoud, 2021

Management summary

With a growing global interest and spending, blockchain technology is here to stay. This relatively young technique starts to find its way into different industries, and more people are interested in blockchain technology. This often results in phrases “we want something to do with blockchain”. This sounds impressive, but if blockchain technology will be applied for everything, it will most likely fail to reach its true potential.

From Spark! Living Lab, the question has emerged whether a blockchain is the best way to share and guarantee the validity of certificates in the Blockcert use case. This use case tries to digitalize certificates with blockchain technology. In this use case it is already decided to make use of blockchain technology, but without the question if blockchain technology was really necessary in this situation. This thesis aims to determine if blockchain technology is necessary for the current Blockcert use case and what criteria there are to have a viable blockchain use case. Therefore, the following research question is used:

“To what extent is blockchain technology really necessary to digitalize certificates in the current Blockcert use case and in similar use cases or are the alternatives recommended to create more transparency and more efficiency in data transferring?”

There are three parties in the supply chain of potatoes: farmers, Isacert (certification authority) and Lamb Weston Meijer (producer of potato-based products). Lamb Weston can only buy potatoes from certified farmers. Between these parties there is no central database to check if a farmer has a certificate or not, but certificates are shared via Excel sheets and emails. This means that certificates given out by Isacert can be falsified. Also, Lamb Weston doesn’t commit a second check upon the certificates that a farmer has, in other words there is mutual trust. The current process is old fashioned, error-sensitive and doesn’t give real-time insight in data.

Blockchain technology enables a decentralized network where non-trusting parties can interact with each other. They don’t need to trust each other, but only the network. Also, all the data that is stored on a blockchain is transparent and immutable. In other words: blockchain technology creates a robust and fraud-proof system. But there are some criteria to have a viable use case. There need to be data to share among participants on a network, there need to me more than one party on the network which adds data, among all the parties on the network need to be a lack of trust and there needs to be a need for disintermediation.

The results have shown that there are specific criteria that need to be met to justify the use of blockchain technology for a use case. But the current Blockcert use case doesn’t meet all the criteria. There is no lack of trust in this use case, only one party adds data, and there is no need for disintermediation. And if trust and disintermediation are not a point of concern, there will be nothing that a blockchain can do that a central database can’t do. Therefore, database technology is preferred over blockchain technology.

The Blockcert use case needs to get expanded with more actors who join the use case. If more certification bodies and producers get on board, the use case will meet all the criteria to use a blockchain. The criteria in this thesis can also be used to formulate new use cases in such a way that the use of blockchain technology can be justified. Eventually, the goal of Spark! Living Lab is to experiment if blockchain technology can add real value to supply chains.

Table of content

1. Introduction and organizational background

This chapter contains the preliminary part of this report. It is divided into two parts. First, some more information about Spark! Living Lab is given to outline the context of the research that will be conducted. Secondly, this introduction includes a reading guide with which the reader will be guided through this report.

1.1 Spark! Living Lab

The Dutch government has set the goal to have a completely circular economy by the end of 2050. This means that for the logistics sector there are set some ambitious goals to reach that goal. This means that there has to be a more efficient way of collaboration and a more effective use of resources (Rijksoverheid, 2016).

Data sharing in the supply chain is therefore a must. Where money and resources flow more and more efficiently through the supply chain, many parties lack reliable and accurate information/data (Schaaf, 2018). Spark! Living Lab aims to close that gap by researching blockchain- and Internet of Things (IoT) applications that provide more sustainable and circular supply chains (Spark! Living Lab, 2020). Living labs are defined as a research concept, defined as a user-centred, open-innovation ecosystem, often operating in a territorial context, integrating concurrent research and innovation processes within a public-private partnership (European Network of Living Labs, 2021).

Spark! Living Lab, started in early 2020, is founded by a consortium of 10 organizations as TNO, TU Delft, Windesheim, Blocklab and more. All participants in the consortium are showed in an overview below this paragraph. This project is part of a bigger research program called “Duurzame living labs” which is funded by the Dutch Organization of Scientific Research (NWO), the Ministry of Infrastructure and Water Management and the Taskforce for Applied Research (SIA) (Spark! Living Lab, 2020).

Fig. 1.1 Organizations taking part in Spark! Living Lab (Spark! Living Lab, 2020)

Currently, Spark! Living Lab is focussing on use cases in supply chain & logistics using blockchain and IoT. But also augmented reality, big data, autonomous robots, and artificial intelligence are main areas of focus, as long as the use case meets the requirements of data sharing technologies in supply chains. The projects where Spark! Living Lab can work on are:

- Track and trace, insight in accurate and reliable delivery schedules, origin, and certification on product level.
- Safe data exchange, a safe exchange of data with conservation of the level playing field.
- Process integration, better Purchase to Pay (P2P) and Order to Cash (O2C) process by using digital transport documents.
- Paper processes, digitalizing of documents without the risk of fraud.

1.2 Reading guide

This thesis is built up in a logical and clear order. The second chapter the problem definition, consists out of 3 parts: the reason for this research, the problem description with the goal of the research and the sub-questions and a theoretical framework. In this chapter the complete research will be explained and defined.

Chapter three covers the findings and results of the research, elaborated by each sub-question. Different aspects with pros and cons can be found per technique. Out of the answers to the sub-questions will flow a logical conclusion. This is covered in chapter four. Together with the conclusion of this research there are recommendations done based on the conclusion. These recommendations can be considered for future work. This report closes with the discussion, a critical reflection on the results and the quality of this research.

2. Problem definition

In this chapter, the problem definition, three parts are covered: the reason for the research, the problem description with the goal of the research and the sub-questions, and the definition of context.

2.1 Reason

From Spark! Living Lab, the question has emerged whether a blockchain is the best way to share and guarantee the validity of certificates in the Blockcert use case. This use case tries to digitalize certificates with blockchain technology. In the supply chain of potatoes there are three parties: farmers of potatoes, Isacert (certification authority) and Lamb Weston (producer of potato-based products). Lamb Weston processes the potatoes to frozen potato products for the retail and foodservice (Lamb Weston, 2021). Lamb Weston can only buy potatoes from certified farmers. Between those parties there is no central database. This means that, in worst case scenario, certificates given out by Isacert can be falsified. Also, Lamb Weston doesn't commit a second check upon the certificates that a farmer has, in other words there is mutual trust. The current process is old fashioned, error-sensitive and doesn't give real-time insight in data.

In this use case it is already decided to make use of blockchain technology, but the alternatives for using blockchain technology have not been properly researched. The main reason for this is because the consortium, mainly led by Lamb Weston, desired to use blockchain technology.

The reason for this research is when entrepreneurs and small & medium enterprises (SME's) want to innovate and make use of data sharing technologies there isn't an overview of what technologies can be used to share intangibles besides blockchain. In this research there will be two other alternatives investigated: X.509 certificates and database technology. The main reason why X.509 certificates are interesting, is the theoretical possibility of bringing the best of two worlds together. The cryptographic security of blockchain technology and the efficiency of a centralized system.

In the last semester, a feasibility study has been done by management engineering students, commissioned by Spark! Living Lab, to discover the possibilities to digitalize the certificates with the help of blockchain technology. The conclusion of this report said that blockchain technology can be used for this problem, but this was more because the client who initiated the use case wanted to use blockchain. In the coming semester a group of software engineering students from TU Delft will develop a proof of concept. Therefore, a running application needs to be designed and developed that can run in a test-environment to digitalize the certification process.

2.2 Problem definition

The goal of this research is to investigate if blockchain technology is really necessary for the Blockcert use case from Spark! Living Lab, this also applies to similar use cases. Also, an overview of two alternative technologies for sharing intangibles will be a goal of this research.

To achieve these goals, the following main question has been formulated: ***"To what extent is blockchain technology really necessary to digitalize certificates in the current Blockcert use case and in similar use cases or are the alternatives recommended to create more transparency and more efficiency in data transferring?"***

This question will be answered with help of the following sub-questions:

- How are certifications currently being shared through the supply chain in the Blockcert use case?
- When should blockchain technology be used for data sharing in the supply chain?
- What are the differences aspects of blockchain technology, X.509 certificates and database technology?
- What are the pros and cons from these techniques regarding the Blockcert use case?

2.3 Definition of concepts

In the definition of concepts an overview is given below to clarify the terms that are used in this research. Each term that needs explanation on what it means and how it is used or applied is clarified below.

Concept	Definition
Blockchain technology	A distributed and decentralized ledger for information-, value-, and data sharing without intervention of a trusted third party (IBM, 2021)
Certificates	Proof that a farmer successfully passed an audit by a certification body like Isacert.
Blockcert use case	Project where the application of blockchain technology can be applied in the supply chain of potatoes.
Data transferring	"Collection, replication, and transmission of large datasets from one organization or business unit to another." (Informatica.com, 2021)
X.509 certificates	Standard format for public key certificates digital documents that securely associate cryptographic key pairs with identities such as websites, individuals, or other intangibles (SSL.com, 2019).
Database technology	Storage, organization, and processing of data in such a way that the end user can make information out of it (Levy, 2018)
SME's	Small and medium enterprises

Fig. 2.1 Definitions of concepts used in the problem definition.

2.4 Research models

To find out if blockchain technology is necessary, several models can be used to decide whether or not a blockchain is needed. For this research, two models are chosen to decide if the current Blockcert use case needs a blockchain based solution. The models are decision trees where the Blockcert use case can be put in the model to find out if the case needs a blockchain.

The first model is the B. Suichies Model (Meunier, 2019). The difference between a public blockchain (Bitcoin and Ethereum) and a private blockchain (Hyperledger and Corda) are introduced here. The other model is the DHS model (Meunier, 2019). This is also a decision tree with questions about the storage and accessibility of data. This model shows for each outcome of the questions a good alternative which is preferable for each situation (Meunier, 2019). Both models are shown in the appendix of this report.

This thesis is based on desk research and is backed by multiple (scientific) papers. As opposed to the research plan, no interviews were conducted for sub-questions two and three. The literature which is gathered for this research was sufficient to answer these sub-questions.

	Theory	Research method	Sources
Sub-question 1: How are certifications currently being shared through the supply chain in the Blockcert use case?	Kwalitatieve data analyseren (Valk, 2017)	Qualitative deskresearch	Reports and possible additional interviews with Lambweston and Isacert. Encryption of interviews.
Sub-question 2: When should blockchain technology be used for data sharing in the supply chain?	(Wüst & Gervais, 2018) Suichies and DHL model	Qualitative deskresearch	Reports and papers from field experts. Document analysis
Sub-question 3: What are the differences aspects of blockchain technology, X.509 certificates and database technology?	Analysis of various reports	Qualitative deskresearch	Reports and papers from field experts. Document analysis
Sub-question 4: What are the pros and cons from these techniques regarding the Blockcert use case?	(Wüst & Gervais, 2018) Suichies and DHL model	Qualitative deskresearch	Reports and papers from field experts. Document analysis

Fig. 2.2 Visualization of the research- and data collection methods

3. Results

In this chapter, each sub-question is answered on the basis of the analysis that has been done. Each sub-question is a separate paragraph. The first paragraph covers the current situation in how certificates are being shared in the supply chain. The second paragraph describes in what situations blockchain technology is applicable. The third paragraph describes two alternatives to blockchain technology and the last one describes the pros and cons from these technologies regarding the Blockcert use case.

3.1 Current situation in sharing certificates

In the supply chain where this research is focussing on, there are three main players that are involved: A farmer who grows potatoes, a certification body who certifies farmers (Isacert) and a producer who buys certified potatoes from farmers to process it to frozen potato-products (Lamb Weston).

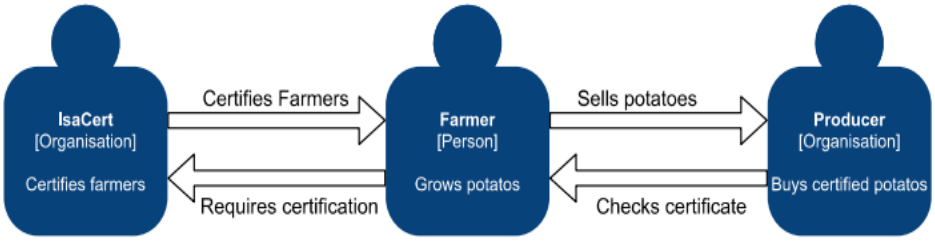


Fig. 3.1 High level overview of the actors in the supply chain (Galjaard, Zonneveld, Maquelin, & Hoonhout, 2021)

If Lamb Weston wants to buy potatoes from farmers to process it, they need to be sure that the specific farmer is certified with a VVA-certificate (food safety certificate). Due to food safety regulations, it is not allowed to buy uncertified potatoes. To obtain a certificate as a farmer you have to be audited by a certification body who is recognized by the Vereniging voor de Aardappelverwerkende Industrie (VAVI). In the supply chain where this research is focussing on the certification body is Isacert.

The current process starts with the certification body. Isacert calls the farmers from who they know their certificate will expire in the upcoming period. In that call an appointment will be made to audit a farmer on food safety measurements. After the audit is completed, the inspector will make up a report and he/she will pass it through to the certification manager. He/she decides to provide the certificate. If everything is correct, the certificate is sent by email to the farmer in PDF (Mussche, 2021). The certificate is stored on a central database from Isacert where only Isacert has access to.

Isacert sends an Excel file periodically to Lamb Weston with the certified farmers where they can buy potatoes from. This is not automated and integrated with Lamb Weston's ERP system. After the list is sent, an employee of Lamb Weston needs to look into this Excel file to see what is updated what needs to change in the system of Lamb Weston. These changes are made manually. There is also a problem that the Excel file is not complete. The list from Isacert contains around 70 growers, but Lamb Weston has 400 growers, so it is only a part of the growers. From the other growers, Lamb Weston needs to gather certification information separrately. For example, supervisors from Lamb Weston contact the farmers directly and they send their certificate directly to Lamb Weston (Peters, 2021).

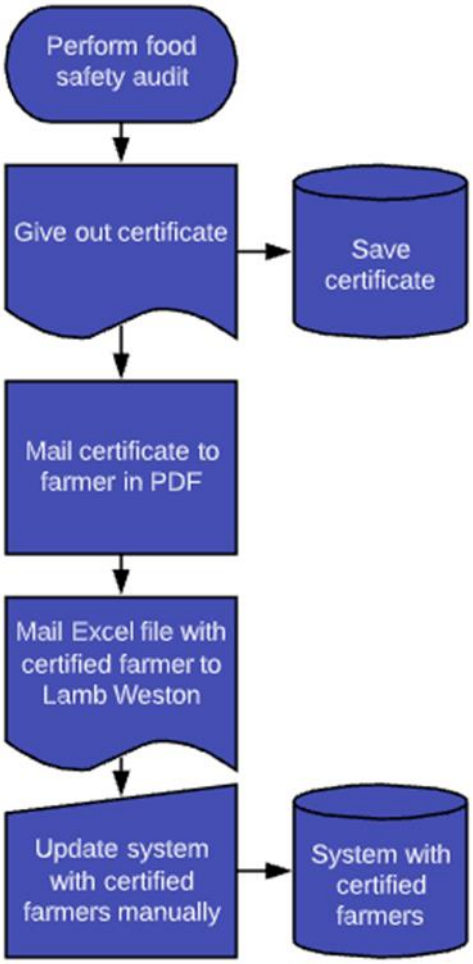


Fig. 3.2 Process flow of the current process of sharing food safety certificates.

To make the process of sharing certificates through the supply chain clearer, there is a process flow stated above to visualize the process. The next paragraph will focus on the overall- and the actor-specific downsides of the current process.

3.1.1 Downsides on the current process

In the current process, there are overall and specific challenges that each party encounters. What stands out the most is that most of the challenges are the result of cumbrous steps in the current process. This paragraph explains the challenges of retrieving certificates and informing the different actors in the supply chain. All the data for this part is collected out of two interviews. One with Dirk Peters, agriculturist at Lamb Weston and one with Frankwin Mussche, team leader agro-cultivation at Isacert.

From a farmer's point of view, they face many paperwork and administration to receive, store and share their food safety certificate. As mentioned in the previous paragraph, every time when Lamb Weston has incomplete certification information about a farmer, they contact the farmer directly to ask the farmer for their certificate. The farmer needs to dig in their administration to find the certificate and provide it to Lamb Weston directly (Cárdenas & Gerard, 2021).

The certification body in the supply chain, Isacert, acknowledges that around 10% of the certificate's requests are rejected and around 3-4% is rejected due to internal inconsistencies on the side of Isacert. This can be spelling errors but also logic errors. On top of that, Isacert sends Lamb Weston every month a report with the certified farmers. This is an expensive affair because an employee of Isacert needs to prepare and send the report while Lamb Weston is getting all the information for free. Another problem is that Isacert commits random checks on certified farmers. Around 10% of the audits are followed by a random audit to check if everything is really good. It is possible that a certificate will be revoked after this random audit. The problem is that it is still a paper certificate. So Isacert can withdraw a paper certificate, but a farmer still has the old paper certificate which is approved. And that one can still be used. A producer might think they have a valid certificate while it actually isn't. (Mussche, 2021).

For the last actor in the supply chain, Lamb Weston, also faces some major issues on the current state of the process in sharing certificates. Particular in planning the production for the factories of Lamb Weston. Every day the factory is planning the inflow of potatoes. But there is also a long term planning that is filled in weeks in advance. Since Lamb Weston is only allowed to buy from certified famers, the planning department in the factory needs to know the expiration dates of the certificates from the farmers. When the expiration date of a certificate from a farmer is passed in the planning period, the farmer will get blocked, and they can't get on the planning. Lamb Weston has two ways of refreshing the expiration date of certificates in their systems: (1) the periodically report of Isacert with updates on who is certified, but not every farmer is in this system, (2) or the supervisor calls the farmers, and they need to provide a valid certificate. This is also a very expensive affair because it costs much time and hours to get that information anyway (Peters, 2021). The main problem here is that Lamb Weston doesn't have real-time insight in where they can buy potatoes and were not. This is because they get information on a monthly basis, so Lamb Weston always has to act on possibly old data.

Because not even half of all the farmers are in the Excel sheet of Isacert, Lamb Weston spends much time contacting farmers and checking their certification status. This involves some risks of fraud of receiving incorrect information because the certificates are in this situation shared without a check from Isacert. However, Lamb Weston doesn't check if the information is correct because they don't expect fraud on behalf of trust towards the farmer. But Lamb Weston doesn't know if a farmer commits fraud because they never checked (Peters, 2021).

In short, a farmer only can sell potatoes when they are certified, and Lamb Weston can only buy potatoes from certified farmers. But certificates are shared via Excel sheets and emails. This means that, in the worst case scenario, certificates given out by Isacert can be falsified. Also, Lamb Weston doesn't commit a second check upon the certificates that a farmer has, in other words there is mutual trust. The current process is old fashioned, error-sensitive and doesn't give real-time insight in data.

To summarize this paragraph, below there is an overview with the downsides of the current process per actor. This to give an answer to the question "How are certifications currently being shared through the supply chain in the Blockcert use case?".

Actor	Downside
Farmer	(1) A lot of paperwork and administration.
Isacert	(1) Internal inconsistencies. (2) reports that are made are expensive, but are sent out for free. (3) revoked certificates can still be used by the farmers.
Lamb Weston	(1) No real-time insight in the certification status of farmers. (2) It is expensive to retrieve the certification status of farmers. (3) Risk of fraud of receiving incorrect certification data.
The whole supply chain	The current process is old fashioned, error-sensitive and doesn't give real-time insight in certification data.

Fig. 3.3 Downsides of the current process split by actor

3.2 Why even a blockchain solution?

This paragraph explains the fundamentals of blockchain technology and why it is so disruptive. In short, this technology is explained so the reader gets a good understanding of the technology were so many people heard of, but don't know what it is about. Thereafter the paragraph will be focussing on situations where a blockchain solutions can be used.

3.2.1 Blockchain fundamentals

In 2008 Satoshi Nakamoto, the name used by the person or people who designed Bitcoin and is or are still anonymous until today, published the whitepaper of Bitcoin, the first peer-to-peer electronic cash system. This was the first blockchain that could be used to serve as a public distributed and decentralized transaction ledger of the native coin bitcoin (BTC) (Nakamoto, 2008). The blockchain space was born.

Until today there is no universal and scientific definition of blockchain. To define the concept for this research, a definition stated by Imran Bashir, writer of the book "Mastering Blockchain" is taken. "*Blockchain is a peer-to-peer, distributed ledger that is cryptographically-secure, append only, immutable, and updateable only via consensus or agreement among peers*" (Bashir, 2018). This means that there is no intermediary involved, so every participant on the network interact directly to each other. The ledger is distributed which means that the ledger is spread among all participants on the network where each participant holds a copy of the ledger. At last, cryptography is used to secure the ledger. Therefore, the ledger is immutable and has only an append only function, data can only be added to the ledger in time-ordered sequential order (Bashir, 2018).

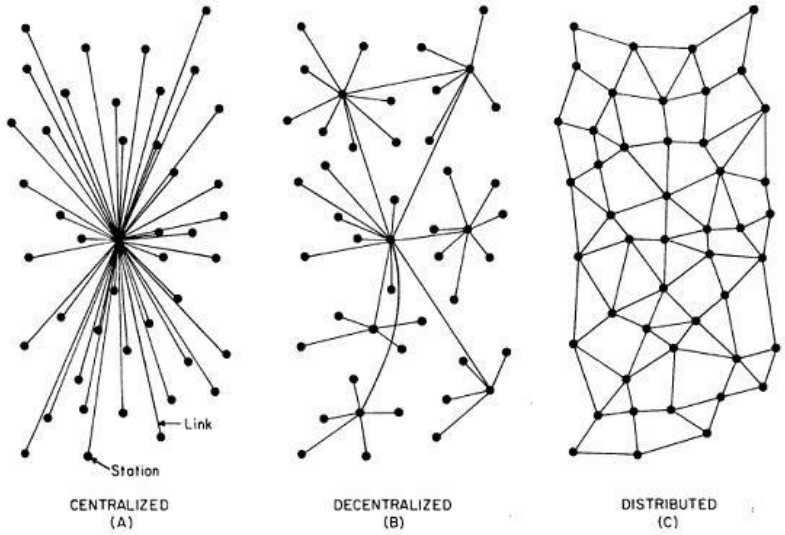


Fig. 3.4 Difference between centralized, decentralized, and distributed networks (Goyal, 2015)

But what is so disruptive about blockchain? The 1976 Nobel Memorial Prize winner in Economic Sciences said the following: "*I think that the Internet is going to be one of the major forces for reducing the role of government. The one thing that's missing, but that will soon be developed, is a reliable e-cash - a method whereby on the Internet you can transfer funds from A to B without A knowing B or B knowing A.*" (Friedman, 1999). With blockchain technology it is now possible to actually do this. By removing the intermediary, i.e., decentralize the ledger, secure the ledger with cryptography, and distribute the ledger among all participants, you create a robust and fraud-proof system. In a blockchain network, participants don't need to trust each other, but only the network (Shearer, 2018).

But how do transactions on a blockchain take place? A blockchain is decentralized by definition and therefore there is no central party who decides if a transaction is legitimate. If a participant on a blockchain network makes a transaction with another participant, it has to be approved by every other participant on the network. In other word, all participants need to reach consensus about all the transactions. As a solution to this there is a so called *consensus algorithm*. This decentralizes the control over the blockchain by forcing participants to cooperate in the enforcement of the consensus rules (Yafimava, 2019). This means for example that all the entities around the world agree beforehand, what kind of transactions are valid and what kind are invalid.

Consensus is the crucial part on a blockchain for making transactions. Participants on the network transact with the help of their public/private-key pair, comparable to a username and password on a regular network. Via this key pair, transactions get encrypted and decrypted. Together with other transactions between participants, the transaction gets stored in a block. When a block is filled with transactions, the block gets hashed. This means that all the data (transactions) in the block is transformed in an alphanumeric string via a mathematical function. When this is done, the block will be added to the existing chain of previous blocks. Every block starts with the hash of previous block, via this way all the blocks are linked to each other and so ensuring that the data on the blockchain is tamperproof (Rosic, sd).

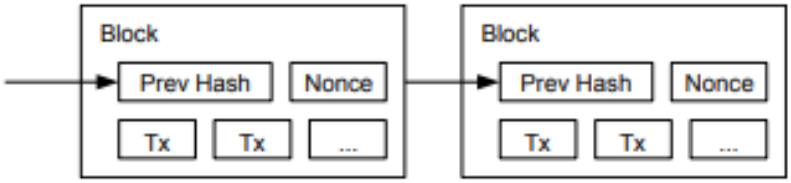


Fig 3.5 Simplified blockchain structure (Nakamoto, 2008)

At last, for understanding the rest of this research it is good to emphasize that there are two categories when we talk about blockchain. *Public/permissionless blockchains* are open and decentralized. Everyone can join the network by downloading the software or transacting on the network. There is no central entity which manages who join and leave the network. Examples off public blockchains are Bitcoin (BTC) and Ethereum (ETH). *Private/permissioned blockchains* are closed off for public, so you need permission from a central entity to join the network. Examples off private blockchains are Hyperledger and R3 Corda (Wüst & Gervais, 2018).

	Permissionless Blockchain	Permissioned Blockchain	Central Database
Throughput	Low	High	Very High
Latency	Slow	Medium	Fast
Number of readers	High	High	High
Number of writers	High	Low	High
Number of untrusted writers	High	Low	0
Consensus mechanism	Mainly PoW, some PoS	BFT protocols (e.g. PBFT [5])	None
Centrally managed	No	Yes	Yes

Fig. 3.6 Difference between public-, private blockchains and a central database (Wüst & Gervais, 2018)

3.2.2 Do I need a blockchain?

Since inception, blockchain technology drew attention of industry. In 2020 a cross-industry survey of almost 1500 senior executives by Deloitte revealed that 55% of them said blockchain technology will be critical for their organization and is in their top-five strategic priorities, and 26% said that blockchain technology will be important but not in the top-five strategic priorities (Deloitte, 2020). Also, the International Data Corporation (IDC) forecasted the worldwide spending on blockchain solutions on $4.3 billion, reaching $14.4 billion by 2023 (IDC, 2020).

It is clear that the role of blockchain technology is growing rapidly. This results in a shift that people tend to resort to blockchain technology for all kind of use cases, even projects that have nothing to do with blockchain technology. The phrase “we want something to do with blockchain” is often meaningless. Having a blockchain project sounds impressive and is good PR to show to the outside world (Greenspan, 2015). Therefore, in this part the criteria’s for using blockchain will be described. This is done on the basis of two decision models: B. Suichies Model and the DHS model. Also, other sources as scientific papers are consulted.

First, the most important thing to be aware of is that blockchain is about data/value sharing. If there is nothing to store or to share it is by default useless to even think about blockchain technology. So, the first criteria should be that there is something to share, you need to share it and you know why you are sharing it. Also, important to add is that the storage of the data needs to be in the right historical order.

Second, running a network based on blockchain technology is only valuable when more than one participant contributes data to the network. There need to be multiple writers on the network who make transactions which affects the current state of the network. If there is only one entity who adds data to the network, a blockchain solution doesn’t provide extra benefits and a central database is better suited (Wüst & Gervais, 2018).

Third, when it is established that there are multiple writers who add data to the network, there needs to be a lack of trust between those writers who have joined the network. Until the inception of blockchain technology, we have always needed a trusted third party (TTP) to maintain systems because we can’t trust random strangers not to abuse the system. If there is mistrust between the participants, the consensus algorithm on a blockchain network ensures that everyone plays by the rules (Filippi, Mannan, & Reijers, 2020). If all the writers trust each other and they assume that the other participants are not fraudulent and/or malicious, a shared database is a better solution.

The fourth criteria is all about the trusted third party (TTP). A trusted third party serves as intermediary who all writers trust if they don’t trust each other. Blockchain technology removes, as mentioned, the need for a trusted intermediary. No central party needs to verify all the transactions that are proposed on the network. The rules of the transaction are included in the consensus rules where all participants agreed upon. This process is called disintermediation (Greenspan, 2015). The question here is to determine if you *want* or *need* disintermediation. If there is nothing wrong with having a trusted third party, there is no need for a blockchain based solution for the use case.

A key point that most people don’t think about is that decentralized networks are way less efficient than centralized networks (Wüst & Gervais, 2018). Also, with regards to latency and throughput (how much data can be transferred in a certain timeframe), centralized networks perform much better than blockchains because in a blockchain network their need to be consensus first to update the current state. This tradeoff, decentralization versus throughput, should be considered as well.

At last, there are some more points to talk about before thinking about blockchain. Points to consider are the amount of data that need to be stored, setting up the network and the rules to reach consensus, picking validators, the rules of the transactions that are made on the network don't need to change frequently and jurisdiction about the technology. But one of most important aspects is that you need very specific knowledge in your organization. This means that you most likely need to hire an external party to help you building your desired blockchain network, and that while there is a huge shortage of well-trained and skilled staff who can develop and manage the complexity of such a decentralized network (Meijer, 2020).

To summarize this sub-paragraph, there is an overview with conditions that need to be met to justify the use of blockchain technology for a use case. This to give an answer to the question "When do I need a blockchain?". To involve the current Blockcert use case into this overview, an additional column is added.

Viable blockchain use case	Current Blockcert use case
There needs to be a shared state of data.	The current state on certification status needs to be shared through the supply chain.
More than one participant adds data.	Only Isacert adds data about the certification status.
There is a lack of trust between participants.	All the parties in the current situation trust each other being honest and not committing fraud.
There is a certain need for disintermediation.	No party feels the need to remove Isacert as gatekeeper of the certificates.
Accept decentralization/throughput tradeoff.	There is no need for high transaction throughput in giving out and revoking certificates.

Fig. 3.7 Conditions for a viable blockchain use case compared to the current Blockcert use case.

So, in short, blockchain technology enables a decentralized network where non-trusting parties can interact with each other. They don't need to trust each other, but only the network. Also, all the data that is stored on a blockchain is transparent and immutable. In other words: blockchain technology creates a robust and fraud-proof system. However, a decentralized network is very inefficient compared to a centralized network. The amount of throughput is much lower in a decentralized network. Also, a decentralized network is less capable of storing large amount of data, finding competent people to build such a network, and setting up the network are much harder compared to a centralized network.

3.3 Database technology

Blockchain technology is a disruptive and impressive technology, but if it will be applied to every use case, no matter the conditions, it will most likely fail to reach its true potential (Perera & Nanayakkara, 2020). The previous paragraph focussed on blockchain technology (decentralized network). This paragraph focusses on database technology (centralized network). There are many different types of databases, so to make this concept more scoped, database technology should be read as a centralized database. This means that the data is stored centrally and verified and validated users from various locations can access this data (Tawde, 2020).

3.3.1 Database fundamentals

Ever since people started to transfer assets to each other, there was a need to store information about those transfers. The oldest storage of that kind of information is found in the city of Mesopotamia, around 5000 years ago. Tablets of clay were used to record lists of goods received and traded. The tablets were safe-kept in temples that were considered the banks of the time (Frydel, 2018). With the emerge of computers and the internet the need to store data, maintain it and retrieve it later grew. With the rise of computers, databases changed fast making it an easy, cost effective and less space-consuming job to collect, index and maintain data (Berg & Seymour, 2021).

Databases use network architecture where a user can modify or read the data that is stored on a centralized server. As opposed to a blockchain network, a centralized database is controlled by a single authority, the trusted third party (Fig. 3.2). This party controls the database, controls who can join and authorizes the credentials of the participants. The database itself is stored on a single location, from this location the data within the database is managed. Most of the times this location is accessed via an internet connection (Yanowitz, 2018).

Often when you hear about databases, the term *relational database* is used. To be clear, a relational database is also a central database here, because the database is still stored centrally. The data is stored in related tables, divided in rows and columns. The software package to create and manage a relational database is called a Database Management System (DBMS). This systems makes sure that the data in a database is maintained (Oracle, 2021). Examples of relational databases are Microsoft SQL server, Oracle database and MySQL.

To communicate with the data that is stored on a database, Structured Query Language (SQL) is used. This is the standard language to interact with most information systems. The language offers a consistent mathematical language, based on relational algebra, to easily find outcomes based on a command which is called a query (Oracle, 2021).

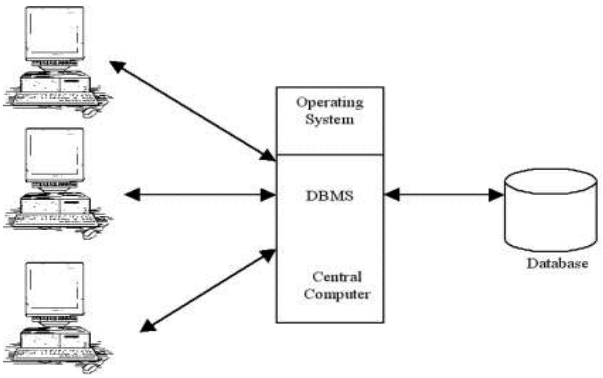


Fig. 3.8 Simplified schematic overview of a centralized database (Yanowitz, 2018).

3.3.2 Do I need a database?

More often you hear the term *data-driven society*. This term refers to the usage of data to make better and more efficient decisions. The fact that data plays a key role in our daily live can be seen in the amount of data in the world. It is predicted that the total amount of data in the world will grow from 59 zettabytes (ZB) in 2020 to 175 zettabytes in 2025 (IDC, 2020).

This actively demonstrates that companies and supply chains produce and have to deal with way more data than before. In 2018, a standard supply chain handled 50 times more data than in the five years before. This means that the supply chain nowadays is transformed through the power of data (DHL, 2020). Therefore, it is critical to have a database in which that data can be stored, managed, and analysed.

As opposed to blockchain technology, there are no hard criteria's for using a database. The only hard criteria for using a database according to the DHS model is the need for a shared, consistent data storage. Similar to the first criteria described in sub-paragraph 3.2.2, a database is useless if there is nothing to store. So, similar to blockchain technology there need to be data to store and share, you need to share it and you know why you are sharing it. Because of the less strict conditions compared to those described in previous paragraph, the focus here is more on the advantages and disadvantages of having a central database.

The biggest advantage of a database is the high level of efficiency. In the previous paragraph the decentralization versus throughput tradeoff is discussed. Central databases can handle a high amount of throughput because of their architecture, participants don't need to reach consensus. Also, in the amount of data that can be stored is a database better suited than a blockchain network. This is efficiency on a technical level, but a database provides also cost- and time-efficiency. When it comes to planning, execute, and implement a database, it will be cheaper and less time-consuming than adopt blockchain technology. Therefore, a database is an easy to set up, relatively cheap and scalable technology (Greenspan, 2016).

The benefit of a centralized database is the efficiency it reaches as long as the trusted third party being trustworthy. But there are some downsides as well. These downsides can be summarised in 3 main categories: exclusion, dishonesty, and a loss of records (Dilley, Poelstra, & Wilkins, 2017).

The trusted third party that controls the centralized database can *exclude* participants on a network. Exclusion means that you are not allowed to participate on the network, but neither can't access the full benefits of the network (Chaia, Goland, & Schiff, 2010). One of the consequences of the trusted third party owning the database, is that this party also owns and manages all the data. This gives this party a big advantage since data represents a lot of value nowadays.

When the trusted third party owns and manages the data in the database there is a risk of *dishonesty*. Corruption and abuse of power are two examples of this. Since there is only one party that can change data, there is risk that data is changed fraudulently or maliciously. Because of this risks, external and certified auditors are hired to audit the work of the trusted third party.

The most well-known example of a *loss of records* is a hack where a person or entity get access to a network illegally. The problem with centralized networks is that there is a "single point of failure". This point is a part in a network that when that point fails, the entire network will stop working (Yanowitz, 2018). In other words, the chain is as strong as its weakest link.

The usage of a database in the certification industry plays a big role. In fact, there is already a worldwide database system to store and share (food safety) certificates with involved parties. This is done via GlobalGAP, a non-governmental organization that sets standards for certification of agricultural products around the world. This organization aims to harmonise certification standards and procedures in a certification system for Good Agricultural Practises (GAP). GlobalGAP offers 16 standards for crops and livestock, more than 160.000 producers use GlobalGAP certification in 124 countries (GlobalGAP, 2021).

GlobalGAP uses an internet-based platform for certification-management and other services. Behind this internetportal runs a central database that 0stores and connects the audits and certification data of more than 200.000 farmers in 135 countries. This is the biggest source for validated certification data on food safety. More than 155 certification bodies, including Isacert, approved by GlobalGAP, use this database to register and store their clients' certification data (GlobalGAP, 2021).

This central database is worldwide accessible for everyone where everyone has its own rights in the database. Only approved certification bodies are allowed to change data about certificates. All other parties can only read the data. The database provides real-time insight in the data, so there are no delays in sharing a certificate (GlobalGAP, 2021).

	Register	GGN	Reg.No	Name1/Last Name	City	Country	Producerstatus	Trustee
select reset								
	No	4052852303002		Test Notif	Melbourne	Australia	Not confirmed	Eurepgap
	No	4052852231206		dafa	kölhn	Israel	Not confirmed	Eurepgap
	No	4052852164689		NotTest	Cologne	Afghanistan	Not confirmed	Eurepgap
	No	4050373841294		Buehler GmbH	Koeln	Germany	Not confirmed	Eurepgap
	No	4050373546205		T. Estuser	Testhausen	Germany	Not confirmed	Eurepgap
	No	4050373379780		PACHT: Canadasol	Almeria 04120	Spain	Not confirmed	Eurepgap
	No	4050373134228		Kartoffel Test Böhmer	n.a.	Germany	Not confirmed	Eurepgap
	No	4049928664976		PACHT: NIJARSTAR	Nijar (Almeria)	Spain	Not confirmed	Eurepgap
	No	4049928664969		PACHT: CAÑADASOL	Almeria	Spain	Not confirmed	Eurepgap
	No	4049928954329		Bioenergia do Brasil S/A	Lucélia - SP	Brazil	Not confirmed	Eurepgap

Fig. 3.9 Example of the GlobalGAP certificate database (GlobalGAP, 2021)

3.4 X.509 certificates

Now there are two data-sharing technologies covered, it is interesting to see if there is a technique which brings the best of those other technologies together. In this case, the cryptographic security of blockchain technology and the efficiency of a centralized system.

3.4.1 X.509 fundamentals

X.509 certificates are standards in cryptography for public key certificates. These are electronic documents that are used to prove the ownership of a public key. A certificate contains information about the key, the identity of the owner, and the digital signature of the party who verified the content of the certificate (Cooper, 2008).

The process where the public keys are connected to the identity of a party is called the Public Key Infrastructure (PKI). This contains a set of roles, agreements, hardware, software, and procedures. The PKI makes sure that information can be transferred securely through a network. This as an alternative for simple passwords and authentication methods. An infrastructure like this is often used for use cases where it is required to validate identity and the information that is being transferred. To connect a public key with an identity, there is a process of registration and issuance of the certificates. This is done via a Certification Authority (CA). This is an entity that controls and manages the certificates. A CA can be public or private (Gerck, 2000).

Like mentioned before, this technique makes use of cryptographic security. This is called asymmetric cryptography. This makes sure that only the recipient has access to the encrypted message. This process is executed via a public/private-key pair. The public key to encrypt the message, and the private key to decrypt the message. This process is shown below.

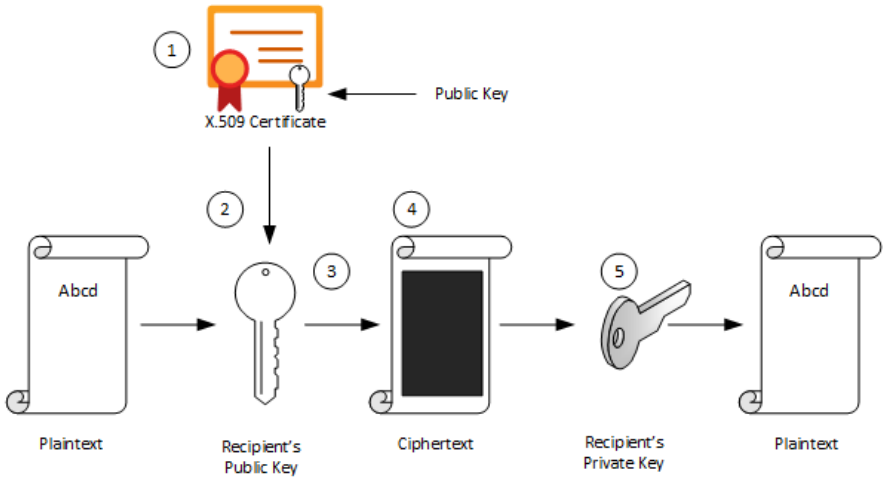


Fig. 3.10 Encrypting process via public/private key pair (Microsoft, 2021)

The recipient generates a public/private key pair and sends the public key to the CA. The CA will use this public key in the X.509 certificate which is generated. Thereafter, the CA will send its public key to the recipient. The sender of the message encrypts its data with an encryption algorithm with his own public key. After the encryption, the sender sends the message to the recipient so he can decrypt the message with his own key pair. The X.509 certificates make sure that the recipient is sure that he communicates with the right person, because he can see that the CA signed the certificate (Microsoft, 2021).

3.4.2 Do I need X.509 certificates?

What is unknown for most people, is that they encounter X.509 certificates on a daily basis. X.509 certificates are widely used for verified and safe internet usage, also known as Hypertext Transfer Protocol Secure (HTTPS). This protocol makes it possible to transfer private data securely on the internet. HTTPS avoids with the encryption of this data, with use of X.509 certificates, that this data can be intercepted becomes readable for a third party. HTTPS and X.509 certificates ensure a safe communication between two parties (Russel, 2020). Other widely used applications for these certificates are signed and encrypted emails, document signing, code signing by software developers and client authentication. It can be concluded X.509 certificates play an important role when trust is an important issue.

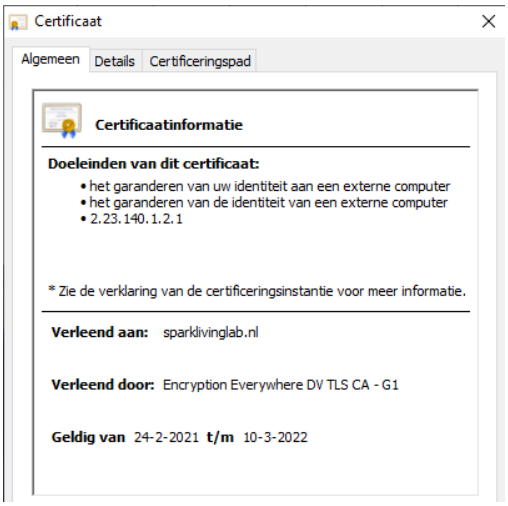


Fig. 3.11 Example of an X.509 certificate for the HTTPS protocol

X.509 certificates have in theory the potential to be used in various use cases. However, their design and architecture are not flawless, and even experts disagree on issues raised by X.509 certificates (Nilsen, 2016). There is one important issue with these certificates: they are not human readable (information that can be read by humans). There is no clear view on what has been certified and, in most cases, it has to be taken for granted that what is accepted, is correct.

Another issue is that the standards where X.509 relies on, is never completely defined, and disclosed. This left room for a wide interpretations of those standards by CA's. Each CA can set their own rules and procedures for making a certificate. Therefore, these certificates are not suitable for cross-verification, when clients of different CA's are users to one another (D. Cooper, 2008). In short, it can be that one X.509 certificate isn't the same as another certificate.

Like central databases, X.509 certificates rely on trusted third parties and are most of the times stored centrally. Therefore, this technique has the same risk categories of a centralized network, explained in paragraph 3.3.2. The only reasons to choose for these certificates are when there are trust-issues among parties. An X.509 certificate shows that the entity really is who they say they are. However, there are certain blockchain networks who are compatible with X.509 public key infrastructures. This would improve security of the certificates (Wang, 2019).

Advantages	Disadvantages
Secure infrastructure for interacting.	No consistent format.
	Not human readable.
	Still a trusted third party.

Fig. 3.12 Advantages and disadvantages of X.509 certificates

4. Conclusion and recommendations

With a growing global interest and spending, blockchain technology is definitely here to stay. This relatively young technique starts to find its way into different industries and more people are interested in blockchain technology. This results often in phrases “we want something to do with blockchain”. This sounds impressive, but if blockchain technology will be applied for everything it will most likely fail to reach its true potential.

4.1 Conclusion

From Spark! Living Lab, the question has emerged whether a blockchain is the best way to share and guarantee the validity of certificates in the Blockcert use case. This use case tries to digitalize certificates with blockchain technology. In this use case it is already decided to make use of blockchain technology, but the alternatives for using blockchain technology have not been properly researched. The main reason for this is because the consortium desired to use blockchain technology.

The following main question has been formulated: ***“To what extent is blockchain technology really necessary to digitalize certificates in the current Blockcert use case and in similar use cases or are the alternatives recommended to create more transparency and more efficiency in data transferring?”***

The answer to that question is: In the current Blockcert use case, blockchain technology is *not* necessary to implement. For the current situation, a central database is more suitable. This will be explained further.

The results have shown that there are certain criteria that need to be met to justify the use of blockchain technology for a use case. These criteria are explained in paragraph 3.2.2. As shown there, the current Blockcert use case doesn’t meet all the criteria.

A viable use case were blockchain technology can be applied characterizes itself by a situation where there needs to be a shared state of data. There need to be data to share among participants on a network. Then, it is important that more than one participant on the network adds data to it. If there is only one entity who adds data to the network, a blockchain solution doesn’t provide extra benefits. When there are multiple writers to the network, there needs to be a lack of trust between those writers. If there is mistrust between the participants, the consensus algorithm on a blockchain network ensures that everyone plays by the rules. If all the writers trust each other and they assume that the other participants are not fraudulent and/or malicious, a shared database is a better solution. Finally, there must be a certain need for disintermediation. No central party needs to verify all the transactions that are proposed on the network. The rules of the transaction are included in the consensus rules where all participants agreed upon. If there is nothing wrong with having a trusted third party, there is no need for a blockchain based solution for the use case.

In this use case there is not a lack of trust, only one party adds data, and there is no need for disintermediation. And if trust and disintermediation are not a point of concern, there will be nothing that a blockchain can do that a central database can’t do. Therefore, database technology is preferred over blockchain technology.

A central database, like the GlobalGAP database, however offers the best properties for the current Blockcert use case. In the current situation it is not a lack of trust that is an issue, but efficiency seems to be the problem when food safety certificates need to be shared among different parties. A central database hosted by Isacert would bring real-time data insight in certification data which will result in an efficiency improvement. Employees of both Isacert and Lamb Weston don't need to spend time anymore making expensive reports, updating systems manually and be busy with gathering certification data from the farmers directly. In short, this will result in net savings in man hours.

When the two models (DHS and B. Suichies) are consulted, you see that both models dissuade the use of blockchain technology undisputedly. According to the DHS model, the Blockcert use case requires a database to store and share the food safety certificates, while the B. Suichies model only shows that blockchain technology should not be used.

At last, X.509 certificates are being investigated for potential usage. This because in theory, this technique brings the best of blockchain- and database technology together: the cryptographic security of blockchain technology and the efficiency of a centralized system. However, the results showed that this technique was too complex regarding their properties. The only unique selling point for this technique was that it plays an important role when trust is an important issue. This is not the case for the current Blockcert use case. Therefore, X.509 certificates are deemed not suitable for this use case, the same reason why blockchain technology is not necessary in the current situation.

4.2 Recommendations

As said before, the question which emerged from Spark! Living Lab whether a blockchain is the best way to share and guarantee the validity of certificates in the Blockcert use case. As a result of this thesis, it turned out not to be necessary to use blockchain technology for this use case and that a central database would bring the same benefits. However, it was already decided to make use of this technique. Mainly because of the consortium that wanted to use blockchain technology. Therefore, the feasibility study that was done was influenced and steered in a way that the outcome would be that blockchain technology was suitable for this use case.

A recommendation for Spark! Living Lab in general would be to think critical from the start of a use case about the use of blockchain technology. Spark! Living lab is a young organization and this use case was one of the first one of its kind. The criteria in this thesis can be used to formulate a new use case in such a way that the use of blockchain technology can be justified. Eventually, the goal of Spark! Living Lab is to experiment if blockchain technology can add real value to supply chains.

As mentioned, the current Blockcert use case has already been formed around the use of blockchain technology. This thesis shows that for the current situation, blockchain technology is not necessary. And this semester, the first proof-of-concept is developed, running on blockchain technology. Therefore, it is recommended to continue to build upon the work done, but shape the use case in such a way that the use of blockchain technology can be justified. In this case that won't be very complex.

The project needs to get expanded with more actors who join the use case. If more certification bodies and producers get on board, the use case will meet all the criteria to use a blockchain. This application relies strongly on a network effect. The more actors join the network, the more relevant it will be for other parties in the future to join the network. To clarify this, there is an overview below to show the criteria to use blockchain technology, the current use case, and the use case if the project gets expanded.

Viable blockchain use case	Current Blockcert use case	Future Blockcert use case
Their needs to be a shared state of data.	The current state on certification status needs to be shared through the supply chain.	The current state on certification status needs to be shared through the supply chain.
More than one participant adds data.	Only Isacert adds data about the certification status.	There are multiple certification bodies who add data about the certification status.
There is a lack of trust between participants.	All the parties in the current situation trust each other being honest and not committing fraud.	Parties are competitors of each other. Therefore, they will not trust each other.
There is a certain need for disintermediation.	No party feels the need to remove Isacert as gatekeeper of the certificates.	When there are more certification bodies, it is unlikely that one of them will be the overall trusted third party.
Accept decentralization/throughput tradeoff.	There is no need for high transaction throughput in giving out and revoking certificates.	There is no need for high transaction throughput in giving out and revoking certificates.

Fig. 4.1 Conditions for a viable blockchain use case compared to the current and future Blockcert use case.

4.2.1 Implementation

This thesis shows that there are certain criteria that need to be met to justify the use of blockchain technology for a use case. Spark! Living lab is a young organization and the Blockcert use case was one of the first one of its kind. The current use case that started at Spark! Living Lab doesn't meet the criteria. Therefore, Spark! Living Lab can take learnings from this use case combined with the outcome of this thesis. This to refrain from the earlier mentioned phrase "we want something to do with blockchain".

The current process of a use case at Spark! Living Lab can be divided in four phases: the ideation phase where a use case gets ideated in a workshop or round tables with interested companies, the analyse phase where a potential use case gets discovered and a problem definition is formulated, the development phase where a prototype gets developed and an experiment gets designed and at last the experimental phase where an experiment will be done to test the prototype in different scenarios (Spark! Living Lab, 2020). Below this paragraph is a process overview of this current process.

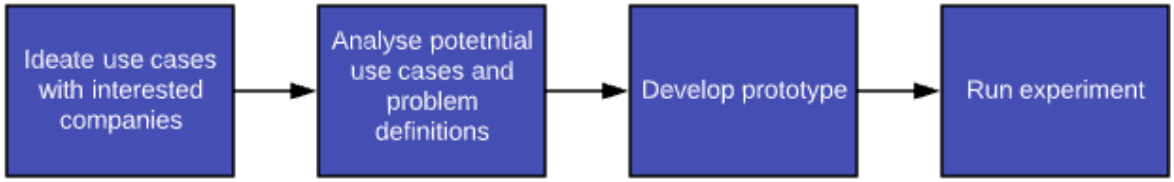


Fig. 4.2 Global process of a use case at Spark! Living Lab (Spark! Living Lab, 2020)

With the outcomes of this thesis, this process can be improved by implementing the criteria of a viable blockchain use case in this process. This check need to be implemented in the analyse phase of the process. This can be done in formulating a problem definition. This will ensure that a use case will be checked on those criteria, and that a use case ends up in adding true value with help of blockchain technology. It can happen that a use case will not meet all the criteria in the first place, like the Blockcert use case. In that case agreements can be made to form a use case in such a way that eventually the criteria can be met.

This action can't be taken by one person alone. It has to be done in consultation with every stakeholder of a potential use case. These stakeholders are the representative of Spark! Living lab for this use case and all the interested companies. All these parties need to align on how they justify the use of blockchain in a use case.

5. Discussion

For this research two models and scientific papers are used to research the necessity of blockchain technology in the Blockcert use case. In this use case, food safety certificates need to be stored and shared among the participants in the supply chain. The current method is old fashioned, error-sensitive and doesn't give real-time insight in data. This research aimed to find an answer if blockchain technology is really necessary to digitalize certificates in the current Blockcert use case or if database technology or X.509 certificates are better alternatives for this use case.

This study can be assessed as sufficiently valid. What needs to be measured has been measured to formulate a good conclusion that answers the main question of this research. The internal validity has been guaranteed because the right conclusions can be drawn from the chosen research method.

The results showed that the use of blockchain technology is not necessary for the Blockcert use case. This result is not surprising regarding the general properties of a blockchain. However, I gained definitely some new insights. During the minor, the focus was almost only about blockchain technology. Therefore, my it was possible that my mind was a bit troubled with the fact that this technology is so fascinating and innovative. This research brought me more clarity about database technology, and that this fits in almost every use case, while the use of blockchain technology is way smaller nowadays. I don't see that this state of mind had a negative influence on this research because I realized very quickly that this distinction was an important fact that was impossible to ignore.

Also at first glance, this research seems to be irrelevant and outdated because it focuses on a use case where it has already been decided to use blockchain technology. However, the opposite is true. This thesis will be highly relevant for Spark! Living Lab in the first place. With the outcomes of this thesis, they will be able to make their work even more relevant for their partners. Secondly, this is also highly relevant for anyone who will read this thesis to discover the possibilities of blockchain technology. In short, the outcomes of this thesis are not only applicable on Spark! Living Lab, but also for every use case in the future, regardless the organization who will discover new blockchain use cases.

There where some limitations on this research. Due to time, there has been choses to only focus on 2 alternatives of blockchain technology. For example, there are way more types of databases, and maybe there is a type of database which will suit the use case better than the traditional database that is described in this research. It is also possible that there is a better alternative that is not covered in this thesis.

A suggestion for a follow-up research upon this thesis is to take a deep dive into the alternatives for blockchain technology. This would be a more technical research. Other, more economical/social, research that can be held as a follow up, is the willingness of companies in The Netherlands to explore the possibilities of blockchain technology.

Bibliography

Bashir, I. (2018). *Mastering Blockchain: Distributed ledger technology, decentralization, and smart contracts explained.* Brimingham-Mumbai: Packt. Retrieved May 7, 2021

Berg, K., & Seymour, T. (2021). *History of Databases.* Minot: International Journal of Management & Information Systems. Retrieved May 11, 2021

Cárdenas, M., & Gerard, M. (2021). *Blockcerts.* Dronten. Retrieved April 30, 2021

Chaia, A., Goland, T., & Schiff, R. (2010). *Half the World is Unbanked.* Financial Acces Initiative. Retrieved May 18, 2021, from https://wagner.nyu.edu/files/faculty/publications/Half_the_world_is_unbanked.pdf

D. Cooper, S. S. (2008). *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.* Trinity College Dublin. Retrieved May 2021, from https://www.hjp.at/doc/rfc/rfc5280.html#sec_3.1

Deloitte. (2020). *Deloitte's 2020 Global Blockchain Survey.* Deloitte. Retrieved May 9, 2021, from https://www2.deloitte.com/content/dam/insights/us/articles/6608_2020-global-blockchain-survey/DI_CIR%202020%20global%20blockchain%20survey.pdf

DHL. (2020, October 9). *Logistics trend radar*. Retrieved May 17, 2021, from Website of DHL: https://www.dhl.com/global-en/home/insights-and-innovation/insights/logistics-trend-radar.html

Dilley, J., Poelstra, A., & Wilkins, J. (2017). *Strong Federations: An Interoperable Blockchain.* Ithaca: Cornell University . Retrieved May 18, 2021, from https://blockstream.com/strong-federations.pdf

European Network of Living Labs. (2021). *What is a living lab*. Retrieved February 4, 2021, from Website of the European Network of Living Labs: https://www.blockcerts.org/guide/recipient_experience.html

Filippi, P. D., Mannan, M., & Reijers, W. (2020). *Blockchain as a confidence machine: The problem of trust & challenges.* Technology in Society. Retrieved May 10, 2021, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3665447

Friedman, M. (1999). Interview National Taxpayers Union. (J. Berthoud, Interviewer) Retrieved May 7, 2021, from https://www.youtube.com/watch?v=mlwxdyLnMXM&t=0s

Frydel, M. (2018, February 15). *Ledger-nomics*. Retrieved May 11, 2021, from Website of Bytemycoin.com: https://bitemycoin.com/opinion/ledger-nomics/

Galjaard, J., Zonneveld, W., Maquelin, S., & Hoonhout, D. (2021). *Blockcert: Blockchain in the supply infrastructure.* Delft: TU Delft. Retrieved May 21, 2021

Gerck, E. (2000). *Overview of Certification Systems: X.509, CA,.* MCG. Retrieved June 6, 2021, from https://www.blackhat.com/presentations/bh-usa-99/EdGerck/certover.pdf

GlobalGAP. (2021). *The GLOBALG.A.P. Database*. Retrieved June 3, 2021, from Website of GlobalGAP: https://www.globalgap.org/uk_en/what-we-do/the-gg-system/GLOBALG.A.P.-Database/#:~:text=The%20GLOBALG.A.P.%20Database%20is%20a%20Internet-based%20platform%20for,validated%20farm%20data%20on%20food%20safety%20and%20sustainability.

GlobalGAP. (2021). *Who are we?* Retrieved June 3, 2021, from Website of GlobalGAP.org: https://www.globalgap.org/uk_en/who-we-are/about-us/Our-Core-Values/

Goyal, S. (2015, July 1). *Centralized vs Decentralized vs Distributed*. Retrieved May 9, 2021, from Website of Medium.com: https://medium.com/delta-exchange/centralized-vs-decentralized-vs-distributed-41d92d463868

Greenspan, G. (2015, November 22). *Avoiding the pointless blockchain project*. Retrieved May 10, 2021, from Website of Multichain.com: https://www.multichain.com/blog/2015/11/avoiding-pointless-blockchain-project/

Greenspan, G. (2016, March 17). *Blockchains vs centralized databases*. Retrieved May 17, 2021, from Website of Multichain.org: https://www.multichain.com/blog/2016/03/blockchains-vs-centralized-databases/

IBM. (2021). *What is blockchain technology*. Retrieved February 16, 2021, from Website of IBM.com: https://www.ibm.com/blockchain/what-is-blockchain

IDC. (2020, 22 June). *IDC Reports Worldwide Blockchain Spending to Slow Down to US$ 4.3 Billion in 2020*. Retrieved May 9, 2021, from Website of IDC: https://www.idc.com/getdoc.jsp?containerId=prAP46625520

IDC. (2020, May 8). *IDC's Global DataSphere Forecast Shows Continued Steady Growth in the Creation and Consumption of Data*. Retrieved May 17, 2021, from Website of IDC.com: https://www.idc.com/getdoc.jsp?containerId=prUS46286020

Informatica.com. (2021). *What is data transfer*. Retrieved February 16, 2021, from Website of Informatica.com: https://www.informatica.com/services-and-training/glossary-of-terms/data-transfer-definition.html

Lamb Weston. (2021). *Producten Lamb Weston*. Retrieved April 2, 2021, from Website of Lamb Weston: https://lambweston.eu/nl/producten

Levy, E. (2018, January 14). *Quick Guide to Database Technologies*. Retrieved March 1, 2021, from Website of Sisense.com: https://www.sisense.com/blog/quick-guide-database-technologies/

Meijer, C. d. (2020, February 29). *Remaining challenges of blockchain adoption and possible solutions*. Retrieved May 10, 2021, from Website of Finextra.com: https://www.finextra.com/blogposting/18496/remaining-challenges-of-blockchain-adoption-and-possible-solutions

Meunier, S. (2019, Augustus 4). *When do you need blockchain? Decision models.* Retrieved March 1, 2021, from Website of Medium: https://medium.com/@sbmeunier/when-do-you-need-blockchain-decision-models-a5c40e7c9ba1

Microsoft. (2021, February 21). *Information about public key cryptography and infrastructure with X.509 certificates*. Retrieved June 3, 2021, from Website of Microsoft.com: https://docs.microsoft.com/nl-nl/azure/iot-hub/tutorial-x509-introduction

Mussche, F. (2021). Interview certification process Isacert. (L. Gelsomino, C. Verhoef, & M. Ayşen, Interviewers) Retrieved April 29, 2021

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System.* Retrieved oktober 26, 2020, from Website of bitcoin.org: https://bitcoin.org/bitcoin.pdf

Nilsen, W. (2016, October 3). *IoT security: when X.509 certificate authentication may not work*. Retrieved June 3, 2021, from Website of Embedded.com: https://www.embedded.com/iot-security-when-x-509-certificate-authentication-may-not-work/

Oracle. (2021). *What Is a Relational Database?* Retrieved May 13, 2021, from Website of Oracle.com: https://www.oracle.com/database/what-is-a-relational-database/

Perera, S., & Nanayakkara, S. (2020). *Blockchain Technology: Is it Hype or Real?* Sydney: Elsevier. Retrieved June 9, 2021, from https://www.translateyar.ir/wp-content/uploads/2020/09/Blockchain-Technology.pdf

Peters, D. (2021). Interview certification process. (L. Gelsomino, C. Verhoef, & M. Aysen, Interviewers) Retrieved April 4, 2021

Rijksoverheid. (2016). *Nederland circulair.* The Hague: Rijksoverheid. Retrieved February 3, 2021, from Website of Rijksoverheid.nl: file:///C:/Users/pmied/Downloads/bijlage-1-nederland-circulair-in-2050.pdf

Rosic, A. (n.d.). *What Is Hashing? [Step-by-Step Guide-Under Hood Of Blockchain]*. Retrieved May 9, 2021, from Website of Blockgeeks.com: https://blockgeeks.com/guides/what-is-hashing/

Russel, A. (2020, July 13). *What is HTTPS*. Retrieved June 3, 2021, from Website of SSL: https://www.ssl.com/faqs/what-is-https/

Schaaf, H. v. (2018, August 2). *Blockchain zorgt voor een betrouwbare supply chain*. Retrieved February 4, 2021, from Website of Cargoledger.nl: https://cargoledger.nl/2018/08/02/blockchain-zorgt-voor-een-betrouwbare-supply-chain/

Shearer, C. (2018, February 2). *Building a Network of Trust using Blockchain Technology*. Retrieved May 7, 2021, from Website of Medium.com: https://medium.com/regen-network/building-a-network-of-trust-using-blockchain-technology-1745b295c6c7

Spark! Living Lab. (2020). Retrieved February 4, 2021, from Website of Spark! Living Lab.nl: https://sparklivinglab.nl/

SSL.com. (2019, september 23). *What is an X.509 certificate?* Retrieved March 1, 2021, from Webiste of SSL.com: https://www.ssl.com/faqs/what-is-an-x-509-certificate/

Tawde, S. (2020). *Types of databases*. Retrieved May 11, 2021, from Website of educba.com: https://www.educba.com/types-of-database/

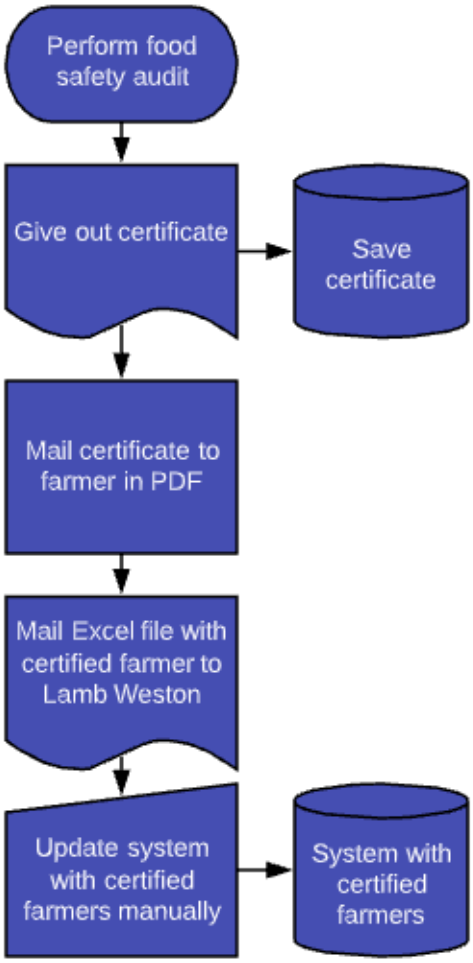
Wang, Z., Lin, J., Cai, Q., Wang, Q., Jing, J., & Zha, D. (2019). *Blockchain-based Certificate Transparency and Revocation Transparency.* Beijing. Retrieved June 3, 2021, from https://fc18.ifca.ai/bitcoin/papers/bitcoin18-final29.pdf

Wüst, K., & Gervais, A. (2018). *Do you need a Blockchain?* Zürich/London: Imperial College London. Retrieved May 9, 2021, from https://eprint.iacr.org/2017/375.pdf

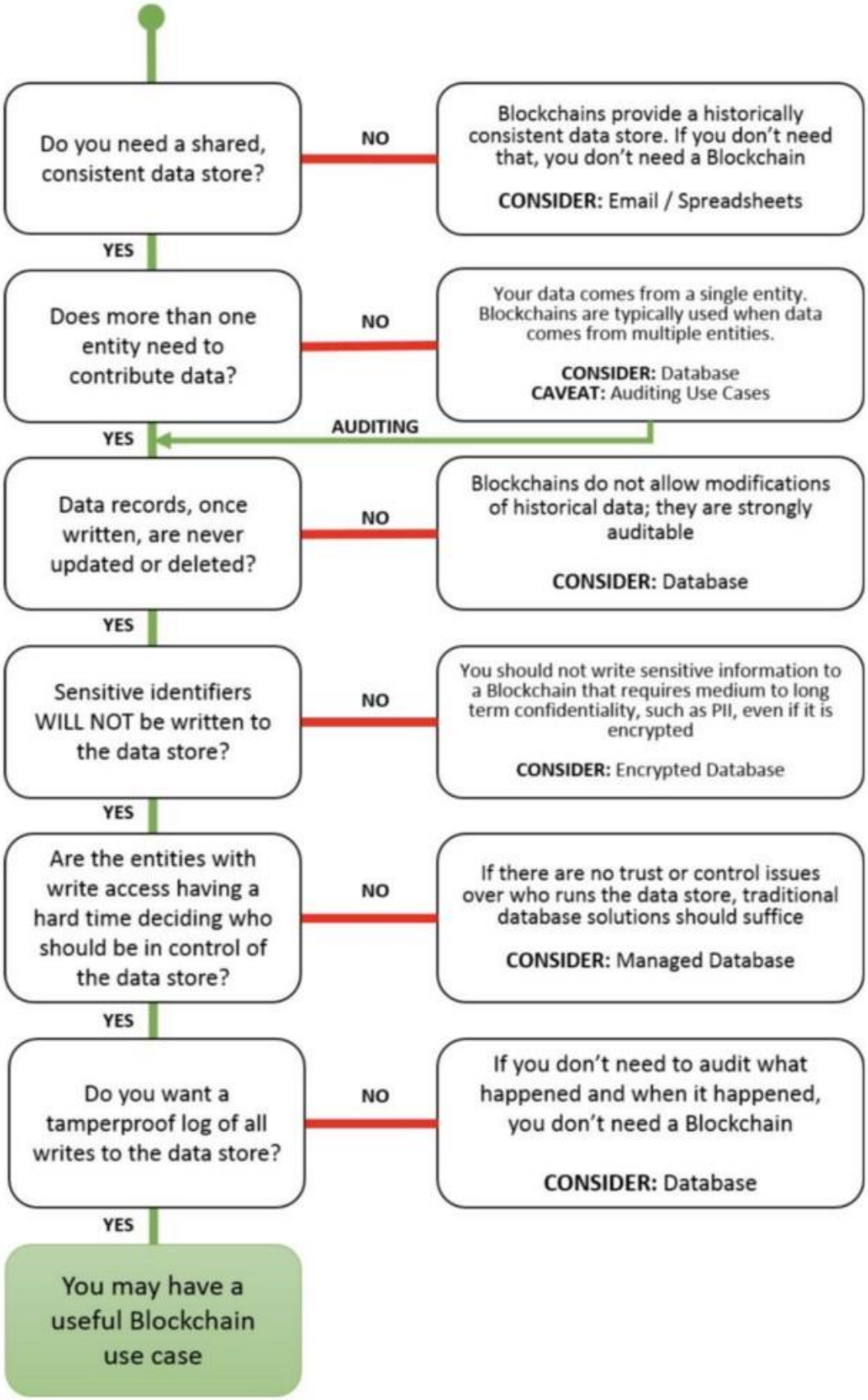
Yafimava, D. (2019, april 2). *Consensus in Blockchain: What You Need to Know*. Retrieved oktober 28, 2020, from Website of openledger.info: https://openledger.info/insights/blockchain-consensus/

Yanowitz, J. (2018, September 17). *Is Blockchain Better Than a Database*. Retrieved May 12, 2021, from Website of Medium.com: https://medium.com/blockworks-group/is-blockchain-better-than-a-database-d518743bdafa

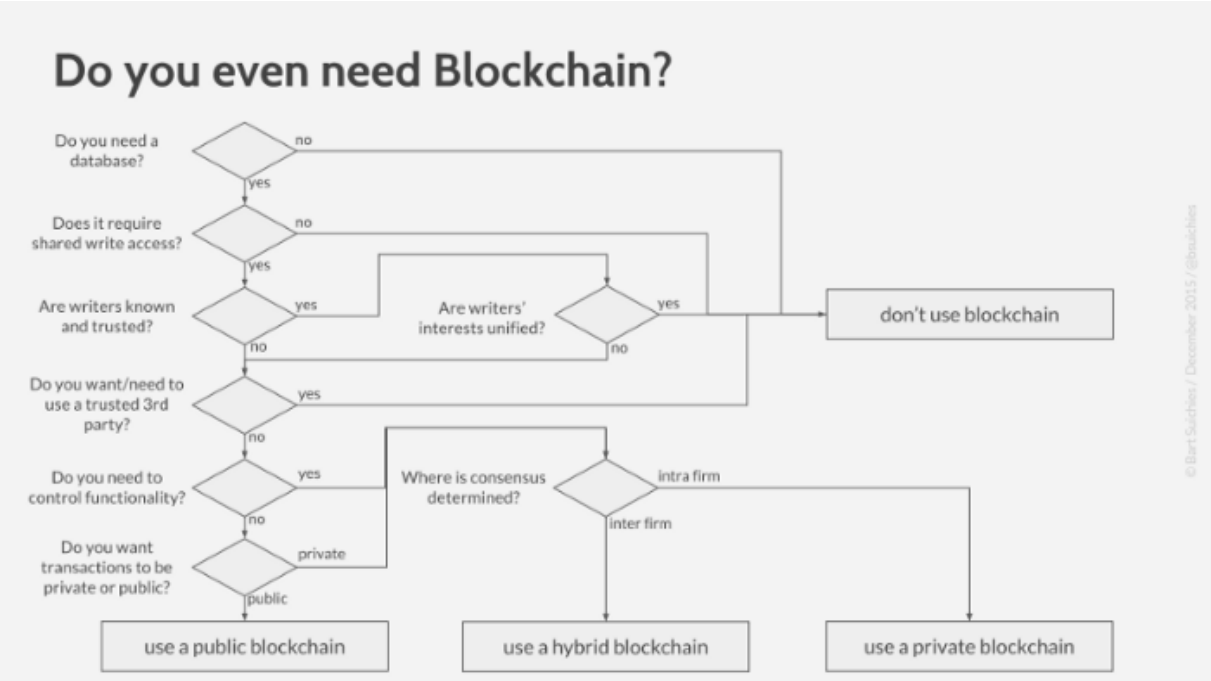
Appendix A Process scheme of the current situation



Appendix B DHS model



Appendix C B. Suichies model



Appendix D Interview Isacert

Transcript interviews current situation in sharing certificates Isacert (only the relevant passages):

L. Gelsomino: Roughly, how many certificates do you do in one year?

F. Mussche: About 10.000.

L. Gelsomino: That is in your entire company, or in your business unit?

F. Mussche: Yeah, in my business unit?

L. Gelsomino: So, on food safety?

F. Mussche: Yeah, there are around 300 about sustainability and all the others on food safety. And we make a distinction on Global Gap and on food safety. We do 2000 on Global Gap and 8000 on food safety.

L. Gelsomino: And can you guide us in the process on doing this certification. Do you get a request, or do you go to the farmer? Is there another process to follow? How does it work?

F. Mussche: Well, mainly the customers who did an audit last year, we call them to attend them that they need to plan an audit because the certificate will expire regarding the 1 year validity of the certificate. For that date we have to do an inspection. We make an appointment and then out auditor goes to the farmer and does the inspection, then it comes back to our offices. Someone checks the report on mistakes. If everything is alright, it will be sent to the certification manager. He takes the decision to provide the certificate. Then we will send the certificate by email to the farmer. And the Global Gap certificate is a global database so there we will upload the certificate and the report there. But in our operations with Lamb Weston, we work with food safety certificates and that is only a paper certificate, and we email it to them in PDF.

L. Gelsomino: How long does it takes to do this entire process?

F. Mussche: Well, it depends on the workload, but on average 28 days for the whole process.

L. Gelsomino: Clear, I understand. Chris, I see you have a question?

C. Verhoef: Yeah, I did not want to interrupt because Frankwin is giving valuable information. But you mentioned that when a certificate is made, it goes back to the head office to check if there were mistakes made. What kind of mistakes are we talking about and what is the result of rejection due to this mistakes?

F. Mussche: Well, it can be language. What is in the report goes to the customer. So, if there are some spelling errors, we don't want to send that out. Also, inconsistencies in the reports are not allowed. That has to be checked. Around 10% of the certificates are rejected and around 3-4% is rejected due to internal inconsistencies.

L. Gelsomino: To sum it up: you have a first check with some other than the auditor, and roughly 10% is rejected to inconsistencies and spelling mistakes by the certificate manager. However, only 3-4% get rejected because the certificate manger finds problems with the report in the grower.

L. Gelsomino: Okay, and the certificates you mail to the farmer. But If I understand correctly, we've spoken to Lamb Weston, you communicate that to Lamb Weston as well?

F. Mussche: Yes, we have a kind of database where we put the certificates in, and they get an email every month with a report with statements which farmer has a valid certificate and which not. And

they can see the certificates in a small portal, but it is not functioning very well. The famer can not see the certificate, but he gives permission to Lamb Weston to see the certificate.

C. Verhoef: Would you be open for the farmer to directly give the permission to Lamb Weston? Now it goes through you, so what if in an end result the farmer actually does it directly to Lamb Weston, and you are no longer the hold up, would that be good?

F. Mussche: It think that we would like that. Sometimes I am wondering who the owner of the information is. Is it the farmer, or are we? If you would say we are the owner, we could charge some money for it.

C. Verhoef: If you make the farmer owner of the data, it is automatically GDPR proof.

L. Gelsomino: The portal that you mentioned, that doesn't work very well. Can you elaborate on that? What is it that is not working?

F. Mussche: We have our own ERP-program, and it is not very well developed. So, it is very rudimentary, they can see some certificates, but that's all.

L. Gelsomino: What would you like to see in the perfect world with a perfect portal?

F. Mussche: I think it would be good for a partner like Lamb Weston to see what the phase of the audit is, is there already made an appointment, is the audit already been done etc. They also want to see the report, now they only see the certificates.

L. Gelsomino: All right that makes sense. One thing that is not super clear to me is what is actually your business model? Do you charge the farmer, or do you charge Lamb Weston?

F. Mussche: We charge the farmer. They pay us to get certified. Lamb Weston is getting all the information for free.

L. Gelsomino: You also mentioned that you would like to give Lamb Weston ideally information on the status of the audit. Is that also something that they ask you?

F. Mussche: In the end the only thing for Lamb Weston what matters, is that they want to know if a farmer is certified yes or no. But sometimes we are late with the appointment for the audit. In that case Lamb Weston wants to know what the status is. Because they also have to schedule their planning for when they receive potatoes.

L. Gelsomino: For Global Gap, what is the process there. Do you only upload the certificate on their system? And that is everything you need to do there?

F. Mussche: Yes exactly, and then we send the certificate to the farmer as well.

C. Verhoef: Are there cases were a certificate gets withdrawn?

F. Mussche: Yes, that happens. We do, alongside our audits, some random samples. 10% of our audits are followed by a random audit to check if everything is really good. This is an easy process. But the problem is that it is still a paper certificate. So, we can withdraw a paper certificate, but they still have the old paper certificate which is approved. And that one can still be used. Lamb Weston might think they have a valid certificate but actually it isn't. A major advantage of a digital system will be that this isn't possible anymore.

C. Verhoef: Are there cases that certificates are rejected by another party than Isacert, for example Lamb Weston rejecting the certificates.

F. Mussche: No that isn't possible. We are the ones that give out the certificate and judge about the food safety. Lamb Weston can find everything about it, but we make the decisions.

M. Ayşen: Yeah, I have a question. Sometimes you reject a certificate because of internal mistakes, how can you detect that mistakes?

F. Mussche: If we reject a certificate. A farmer has the possibility of appeal, and everybody uses it because without the certificate you can't sell the potatoes in Holland, and even in countries where it is not necessary, they get a lower price. And via that way we discover our mistakes. We can't understand how it is our mistake.

L. Gelsomino: Thank you, it was very useful to have this call. So, thank you and we will definitely stay in touch. Thank you very much.

Appendix E Interview Lamb Weston

Transcript interviews current situation in sharing certificates Lamb Weston (only the relevant passages):

D. Peters: When growers want to supply potatoes to us, they need to participate in an external food safety program. In this program they are checked on around 70 points. This to prevent food safety issues. So, to become a food safe grower, they need to participate. Then they get audited every year, and when they get this audit, they get a certificate to proof that they passed When we have this certificate then they are allowed to supply to us. When they don't have a valid certificate, they will be blocked, and they can't provide potatoes to us.

L. Gelsomino: So essentially growers undergo some kind of certification, and they are audited once a year. Do they get audited by you or a third party?

D. Peters: Yes exactly, but they get audited by an external party. And this party is also member of this project, and it is Isacert.

L. Gelsomino: All right, and is the certification from Isacert, is it shared with your competitors? Is that a standard or is it something that only you ask?

D. Peters: No, the certificate and the food safety program can be joined by all growers so they can supply potatoes. We all share the same certificates. There are different certificates. The main one is VVAK, or we have Global GAP. This project will focus on VVAK.

L. Gelsomino: And does it happen often that a supplier does not get his certification?

D. Peters: Well, it works like this: we have a planning, so every day our factory is planning potatoes to come in. But they also have a long term planning that they filled in a few weeks before. Every certificate has an expiration date, after this date a certificate is not valid anymore. These expiration dates are in our system, so when the planning department makes a new planning, and the expiration date is passed, these growers will be blocked, and they can't get on the planning. So, in that way they are blocked. We have two ways of refreshing the expiration date. (1) A weekly report of Isacert with updates on who is certified, but not everybody is in this systems. (2) The supervisor call the farmers and they need to provide a valid certificate

L. Gelsomino: So Isacert and Global GAP send you messages with new certificates? Is this automated integrated messages in your ERP?

D. Peters: No, we get an excel from Isacert. We have to look into it and to see what is updated and manually we have to change it in our system. But the problem is that the list from Isacert contains around 70 growers, but in total we have 400 growers, so it is only a part of the growers. From the rest we get our information in a separate way. The growers have to send it to our department.

L. Gelsomino: For this growers, do you trust them that they send the correct information?

D. Peters: Yes, we do because we don't expect fraud because on the certificates there are number on which we can check with the auditor if it is correct. But we don't do that. So, we don't even know if a farmer commits fraud because we never checked. We completely trust the grower that he has a correct certificate. We have a feeling our growers are correct, but we can't prove it. Our customers don't ask us to prove us like this, but we see it happening that customers want more and more to know what is happening on that side. In the future we think we need to prove much more than we have to do now.

M. Ayşen: If I understand it correctly the farmers don't have to have certificates from the third party you have an agreement with. They can get it from everywhere.

D. Peters: Partly true, we have selected some auditors where they can participate in a food safety program. They can participate with 6 certification bodies.

L. Gelsomino: Do you know what these audit checks with the growers. In general terms do they check hygiene or quality of the products?

D. Peters: The focus is on food safety, so what they check if according to a complete handbook. According to that handbook there are around 70 measures they have to take. For example, an auditor checks if a farmer administrates how they use their pesticides and in what use. Another example is that growers store their potatoes, an auditor check if a grower doesn't use light bulbs of glass. Also, a farmer needs to administrate which potatoes come from which fields.

L. Gelsomino: And this is the targeting use case you are discovering, spoken of blockchain.

D. Peters: Yes, this is one way, to get to know if a certificate is valid and genuine, but another thing that is a problem for us is that what we see, is that Isacert is the biggest certification body we have. A lot of growers certify via Isacert. A lot of them get audited and get a new certificate in the period of August and October. And then you see a huge spike in workload in Isacert. We notice is that they can't renew a certificate in time for growers. A certificate is expired, and we are not allowed to process the potatoes of these growers only because Isacert is not able to renew it in time. And we were thinking maybe with blockchain, can we speed up the whole process of certification.

C. Verhoef: Do you also have problems with certificates when you are trying to validate the certificate across borders?

D. Peters: Well, we don't ship potatoes normally, we only ship potatoes to our factory and then we produce fries. We don't export potatoes.

C. Verhoef: Do you then need a separate certificate for your fries, or does the VVA certificate from the farmer also counts for your fries?

D. Peters: Yes, our plants are also certified. Some customers demand that certificates.

L. Gelsomino: Do customers ask for both certificates at one time?

D. Peters: Yes, sometimes they do. We have customers that demand BRC certification. So, the plants are BRC certified. But at the same time, they demand that our growers are certified. Sometimes we get some questions about our growers. Then we have to supply where these potatoes are coming from together with the certification of the growers.

L. Gelsomino: To give us an idea, how many tons are we talking about per year?

D. Peters: Lamb Weston processes in four factories and there we process around 1 million tons of potatoes so 1 billion kilograms. In the UK around 200.000 tons and in Austria around 150.000 tons. You have to imagine that when you look at the fry market, then 90% of the fries that are consumed worldwide is coming from north America/Canada or northwestern Europe.

L. Gelsomino: Thank you, it was very useful to have this call. So, thank you and we will definitely stay in touch. Thank you very much.

Appendix F Justification research methods

In this appendix, each sub-question will be evaluated and described. The actual research methods are described here. This thesis is based on desk research and is backed by multiple (scientific) papers. As opposed to my research plan, no interviews were conducted on by sub-questions two and three. The literature which is gathered in this research was sufficient to answer these sub-questions.

- How are certifications currently being shared through the supply chain in the Blockcert use case?

Research design: This sub-question served as starting point for this research. The first sub-question is answered with the help of desk research and field research. Previous reports and semi-structured interviews from Spark! Living Lab are used to give a clear overview of the current situation. The reason for this is to get the data straight from the persons who are working in the supply chain which is covered in this research. The method for this sub-question that is used is a document analysis. As said, the previous reports and interviews are analysed for information that could be used for answering the first sub-question. Because al the information of Spark! Living Lab is stored at one place, this information was easily accessible.

Data collection: Data that is collected from the sources of Spark! Living lab is all secondary data. The interviews were already taken and they only needed to be transcribed. Also the reports that were made are secondary data. however, these had to be properly checked for reliability and quality.

- When should blockchain technology be used for data sharing in the supply chain?

Research design: At this part of the research there is investigated what blockchain technology is and when do you need a blockchain. After this, the knowledge is applied to the Blockcert use case. For this, desk research is done to gather data to answer this question. Multiple (scientific) papers and two decision models are used to gather representative insights. Therefore, the method for this sub-question that is used is a document analysis on the (scientific) papers.

Data collection: All the data out of the (scientific) papers that are used is secondary data. The papers are all checked on reliability. This is done by checking the authors and fact-checking the statements that are made. For answering this question, multiple sources are used. Therefore, all the statements made in this report are backed by multiple sources to make sure that all the statements are fundamentally strong and unbiased.

- What are the differences aspects of blockchain technology, X.509 certificates and database technology?

Research design: This question is answered in the same way as the previous question. At this part of the research there is investigated what blockchain technology is and when do you need a blockchain. After this, the knowledge is applied to the Blockcert use case. For this, desk research is done to gather data to answer this question. Multiple (scientific) papers and two decision models are used to gather representative insights. Therefore, the method for this sub-question that is used is a document analysis on the (scientific) papers.

Data collection: All the data out of the (scientific) papers that are used is secondary data. The papers are all checked on reliability. This is done by checking the authors and fact-checking the statements that are made. For answering this question, multiple sources are used. Therefore, all the statements made in this report are backed by multiple sources to make sure that all the statements are fundamentally strong and unbiased.

- What are the pros and cons from these techniques regarding the Blockcert use case?

Research design: This question is answered in the same way as the previous question. At this part of the research there is investigated what blockchain technology is and when do you need a blockchain. After this, the knowledge is applied to the Blockcert use case. For this, desk research is done to gather data to answer this question. Multiple (scientific) papers and two decision models are used to gather representative insights. Therefore, the method for this sub-question that is used is a document analysis on the (scientific) papers.

Data collection: All the data out of the (scientific) papers that are used is secondary data. The papers are all checked on reliability. This is done by checking the authors and fact-checking the statements that are made. For answering this question, multiple sources are used. Therefore, all the statements made in this report are backed by multiple sources to make sure that all the statements are fundamentally strong and unbiased.

Appendix G Link main- and sub-questions to learning goals

This appendix contains the justification of the learning goals for the study Finance & Control. These learning goals will be linked to the main- and sub-questions of this research. In this way it is proven that the research topic fits in well with the learning goals for the study Finance & Control.

Learning outcome 2: learning outcome 2 is focussed on delivering a contribution to the design on a control system aimed at control and monitoring the strategic goals of an organization. With this research several methods of data sharing in the supply chain are investigated. I advised which method suits the best for the Blockcert use case and helped designing and developing a working application for sharing and storing digital certificates.

Learning outcome 4: This learning outcome is about advising how to organise the information supply and processes focussed on managing risks in an organization. With this research to data sharing technologies it is investigated how to share data in the most transparent and efficient way in the Blockcert use case supply chain.

Learning outcome 6: This learning outcome is focussed on advising about the best design of retrieving data and business processes, focussed on effectivity and efficiency. With this research several methods of data sharing in the supply chain are investigated. I advised which methods suits the best for the Blockcert use case and helped designing and developing a working application for sharing and storing digital certificates.