TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Indrek Jõgi 174865IDDR

Method for choosing distributed ledger technology in supply chain management

Diploma thesis

Supervisor: Alexander Horst Norta
PhD

Tallinn 2021

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Indrek Jõgi 174865IDDR

Hajutatud pearaamatu tehnoloogia valiku meetodika tarneahela juhtimises

Diplomitöö

Juhendaja: Alexander Horst Norta
PhD

Tallinn 2021

Author's declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Indrek Jõgi

17.05.2021

Abstract

Global trade is highly reliant on supply chains that are becoming increasingly complex. In the course of the coronavirus pandemic the inherent weaknesses of current supply chain management solutions have been made evident in the form of disruptions and delays. Distributed Ledger Technology (DLT) is a potential candidate in the efforts to provide innovative solutions that are capable of tackling these present-day challenges. DLT provides an immutable data store that can be shared securely between stakeholders to foster collaboration and to track and trace the provenance of different items along supply chain processes. While the use of DLT for supply chain management (SCM) solutions is gaining momentum around the globe, the wider adoption of the technology still lags due to the lack of expertise about the technology and its successful implementation.

This thesis addresses the existing DLT expertise gap in SCM by proposing an assessment method that allows to identify DLT stacks that can be used for building decentralised applications (DApp). Current literature on the subject contains methods for general purpose DLT identification based on platform features and qualities. The proposed assessment method approaches technology identification by presenting a decision process that is guided by SCM specific criteria that can be used to match technologies to use case specific requirements. This allows to partially compensate DLT expertise with domain specific knowledge, while also aiming to make the assessment method compatible with other tools and methods. In order to evaluate the utility of the assessment method, it is used in a case study to design and develop a proof of concept (POC) SCM DApp. The usability of the method is evaluated by gathering feedback from conducting expert interviews where the assessment method is presented as a web-based decision support tool.

This thesis is written in English and is 50 pages long, including 7 chapters, 19 figures and 17 tables.

Annotatsioon

Hajutatud pearaamatu tehnoloogia valiku metoodika tarneahela juhtimises

Rahvusvaheline kaubandus sõltub tarneahelatest, mis muutuvad järjest keerukamaks. Koroonaviiruse pandeemia käigus on ilmnenud tarneahelate praeguste juhtimislahenduste nõrkused katkestuste ja viivituste näol. Üheks võimaluseks luua innovatiivseid lahendusi, mis suudaksid vastata neile ajakohastele väljakutsetele, on hajutatud pearaamatu tehnoloogia (HPT). HPT võimaldab muutumatut andmetalletust, mida saab osapoolte vahel turvaliselt jagada ning mis võimaldab soodustada koostööd ja jälgida erinevate kaubaartiklite liikumist tarneahela protsesside käigus. Samal ajal kui HPT kasutamine tarneahela juhtimises ülemaailmselt hoogustub, takistab selle tehnoloogia laiemat kasutuselevõttu erialase kompetentsi puudumine HTP ja selle eduka juurutamise kohta.

Lahendusena HPT erialase kompetentsi puudujäägi kompenseerimiseks tarneahela juhtimisel pakub lõputöö välja hindamismetoodika, millega saab tuvastada HPT-pinusid, mis sobivad detsentraliseeritud rakenduste (Däpp) väljatöötamiseks. Antud teemal koostatud teadustöödes on kirjeldatud üldotstarbelisi meetodeid HPT tuvastamiseks platvormi tunnuste ja omaduste järgi. Lõputöö raames väljapakutud hindamismetoodika on lähedane tehnoloogia tuvastusele, kirjeldades otsustusprotsessi, mis lähtub tarneahela juhtimise spetsiifilistest kriteeriumitest ja mille abil on võimalik sobitada tehnoloogiaid kasutusjuhtumi erinõuetega. Selline lähenemine võimaldab osaliselt asendada HPT erialase kompetentsi valdkonnapõhiste teadmistega, seades ühtlasi eesmärgiks tagada hindamismetoodika ühilduvus teiste tööriistade ja metoodikatega. Hindamismetoodika kasulikkust hinnati juhtumiuuringus, mille käigus projekteeriti ja töötati välja tarneahela juhtimise Däpi prototüüp (proof-of-concept, POC). Metoodika kasutatavust on hinnatud ekspertintervjuudest saadud tagasiside abil, kus hindamismeetodit on kirjeldatud kui veebipõhist otsustustoe rakendust.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 50 leheküljel, 7 peatükki, 19 joonist, 17 tabelit.

List of abbreviations and terms

BiTAS	Blockchain in Transport Alliance Standards Council
BPS DSS	Blockchain Platform Selection Decision Support System
DApp	Decentralised Application
Däpp	Detsentraliseeritud rakendus
DAOM	Decentralized Agent Oriented Modelling
DLT	Distributed Ledger Technology
DSR	Design Science Research
DSS	Decision Support System
HF	Hyperledger Fabric
HPT	Hajutatud pearaamatu tehnoloogia
IDE	Integrated Development Environment
IOT	Internet of Things
P2P	Peer to Peer
POC	Proof of Concept
QR	Quick Response
RFID	Radio-frequency identification
SCM	Supply Chain Management
SDK	Software Development Kit
SME	Small to Medium Enterprise

Table of contents

List of figures

List of tables

1 Introduction

A distributed ledger is a decentralized database with an immutable data structure, that is shared between nodes in a peer-to-peer (P2P) network. Distributed Ledger Technology (DLT) enables decentralized processing of transactions and data storage, that takes place simultaneously on multiple nodes in a distributed ledger network. Supply chain management (SCM) refers to the handling of processes related to the flow of goods and services from raw materials to final products. This journey requires different companies to exchange information between each other, which can lead to two types of issues that DLT has the potential to solve. First of these is the issue of provenance that DLT can fix by providing an auditable trail of records from each step of the supply chain. The second is facilitating trust between participants in a supply chain by providing a shared, tamper-resistant data source. The use of programmable contracts called smart contracts, allows companies to move shared business logic on a distributed ledger, enabling to enforce business rules and contracts automatically as certain predefined events occur. Having both data and the application logic distributed amongst decentralized peers makes DLT networks highly resilient, since as long as there are operational peers, the network can continue to function and as nodes recover from faults, they can synchronise with changes in the ledger. DLT can also facilitate the use of Internet of Things (IOT) in SCM by replacing centralized gateways with nodes in the DLT network that are able to process vast amounts of data produced by IOT devices while eliminating the need for trusted intermediaries, creating more fault-tolerant supply chain networks with higher degrees of business processes automation, reducing cost and increasing efficiency. This makes DLT a good fit for SCM and has attracted the interest of logistics companies [1], [2], manufacturers [3] and retail companies [4] that are either using or exploring the use of DLT to enhance their supply-chain networks.

This thesis sets out to ease the process of designing enterprise DLT systems for SCM by identifying which DLT stacks support building decentralised applications (DApps) for SCM. This is done through the creation of an assessment method that can be used together with Decision Support Systems (DSS) such as Blockchain Platform Selection Decision

Support System (BPS DSS) [5] in order to identify DLT stacks that fulfil use case requirements of different SCM systems. Both DLT and SCM systems are complex topics and in order to understand the intersection points between the two, a taxonomy is created to chart the relationships between various interconnected technologies that influence the choice of DLT for SCM. By identifying the goals and constraints of using DLT in SCM, goal mapping can be used to derive generic requirements for DLT stacks that provide a foundation for system design that incorporates the best practices of using DLT in SCM. The taxonomy together with generic requirements will be used to develop criteria for assessing the utility of using different DLT stacks in SCM. To evaluate the utility of the assessment method a Proof of Concept (POC) application is created to demonstrate its use in DLT system design and development. Usability of the assessment method is evaluated by gathering feedback from domain experts.

1.1 Existing body of knowledge

The existing literature on using DLT for SCM mainly focuses on different supply chain areas such as pharmaceuticals [6], food and agriculture [7], [8], [9], [10], automobile industry [11], logistics [12] , application of smart contracts [12], [13], [14] and IOT [12], [13], [15], [9], [14] in the context of SCM. The choice of DLT can be at times influenced by various factors such as performance [16], [9], [17], [6], privacy [9], [11] and the ability to represent tracked goods as tradeable digital tokens [14], [18]. Although current literature contains examples of different use cases, the choice of a platform is at times made due to perceived lack of suitable alternatives [19], [20] or because the chosen DLT supports some desired features such as smart-contracts, but doesn't meet the performance requirements of scalable SCM specific decententralized applications [21], [22].

Literature on the subject of assessing DLT platforms tends to focus on general purpose DLT selection based on platforms features, with the creation of DLT taxonomies [23], [24], [25] being the most prevalent method. A DSS with customizable inputs is proposed by J.R.Q Verkelji in his master thesis *A Decision Support System for Blockchain Platform Selection* [26], that organizes the requirements for an application by DLT platform features, giving them weights based on the MoSCoW [27] prioritization method. BPS DSS is a support tool that is created based on this research and can be used to calculate a list of platform alternatives that are ordered by a score that indicates a platform’s fit for specified requirements.

1.2 Research gap

The existing research gap lies in the lack of methods and tools that can aid in SCM business domain centric DLT assessment for DApps. Although current literature contains methods that can aid in the process of determining suitable DLTs by platform features, the added complexity of SCM systems and the specific requirements posed by them, require a more in depth assessment to ensure that technology candidates meet all the necessary criteria. This thesis aims to fill this gap by developing an assessment method that can be used to identify DLT stacks that will provide features and qualities that are required by SCM.

1.3 Research methodology and research questions

This thesis follows design science research (DSR) methodology due to its focus on artifact creation in IS to solve relevant and important business problems. *Design science addresses research through the building and evaluation of artefacts designed to meet the identified business need* [28]. DSR applies business needs and a knowledge base around a subject to iteratively create theories and artefacts that are re-evaluated through every iteration to reach solutions for relevant problems.

1.3.1 Research questions

The main research question of **How to identify which DLT stacks support building decentralised applications for SCM** is too complex to answer alone, therefore it is divided into sub research questions which together provide the answer.

1.3.2 RQ1: What technologies are relevant for building SCM specific decentralised applications?

The establishment of a knowledge base around the use of DLT in SCM is necessary to understand the relationships between various technologies and how they can affect the choice of DLT. This will be done by gathering evidence in current literature, in order to map out key technologies and their relationships in the context of SCM with the purpose of creating a taxonomy of technologies central to using DLT for SCM.

1.3.3 RQ2: What are the generic requirements of SCM specific decentralized applications?

This question deals with finding generic requirements for DLT in SCM that can be used to improve system design by creating a foundation that matches the needs of SCM with DApp design. For this purpose, goal mapping is used to derive generic requirements from identified functional goals and qualities, seen from the perspective of different actors. The deliverables of this part are the goal models and the generic requirements of DLT in SCM.

1.3.4 RQ3: Which DLT stacks are suitable for use in SCM?

This question deals with finding DLT stacks that support developing DApps for SCM. Using the established knowledge base together with the goals and generic requirements of DLT in SCM, an assessment method is developed that can be used together with BPS DSS to find out which DLT stacks satisfy the criteria for use in SCM systems. The deliverable of this part is the SCM domain specific assessment method.

1.3.5 Design science research

The environment pertaining to this research is composed of businesses and technologies. Relevant businesses include SCM companies and DLT developers that use a combination of DLT stacks, SCM systems and IOT networks to create DApps for SCM. The centre part of the figure depicts how the application of a knowledge base around the subject is used for iterative artifact development and evaluation in order to solve relevant business needs. The knowledge base part of the figure is composed of foundations and methodologies. Foundations for this thesis include relevant literature on the subject of applying DLT in SCM and the BPS DSS. Figure 1 shows how DSR is applied to this research.

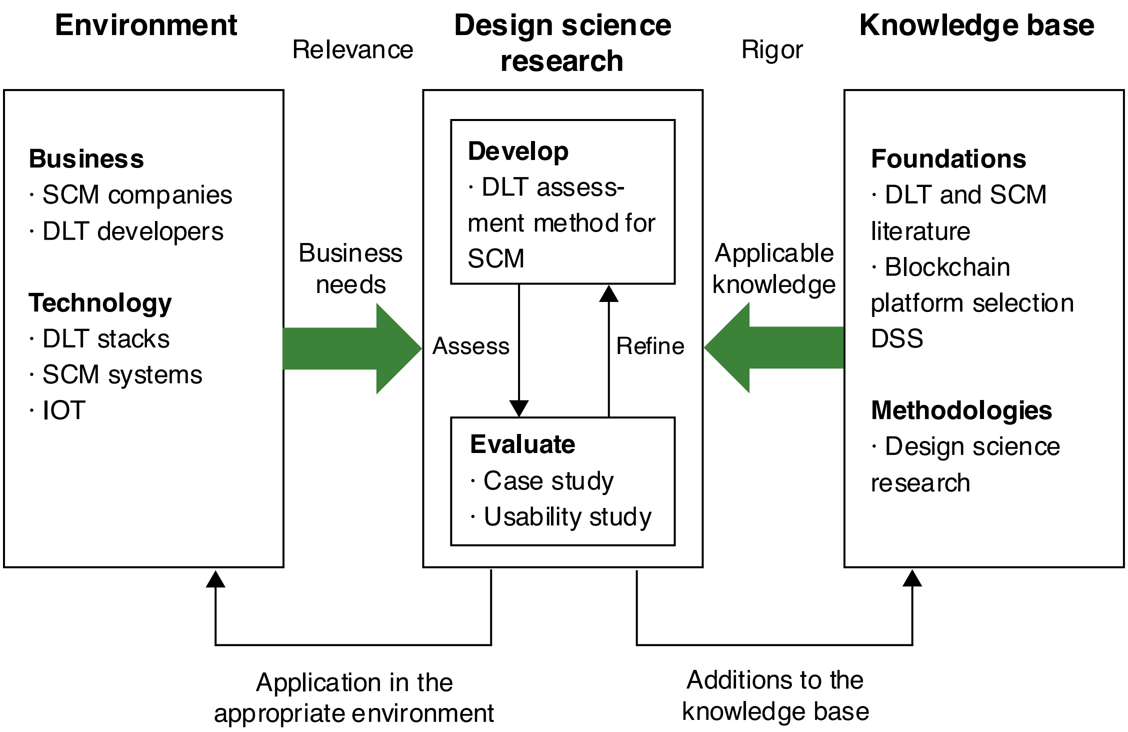

Figure 1. Design science research applied to this research.

2 Background information

The following sections outline background information necessary to understand the rest of this thesis. Section 2.1 gives an overview of the challenges of applying DLT in SCM. Section 2.2 presents the running case that this thesis tries to solve, and section 2.3 describes the preliminaries necessary to understand the following chapters.

2.1 The challenges of applying DLT in SCM

According to the 2nd Global Enterprise Blockchain Benchmarking Study which surveyed 67 operational enterprise projects, supply chain tracking made up 19% of live enterprise networks by use case [29]. While DLT has great potential to improve new and existing SCM solutions, it can also pose challenges for companies wishing to use it. A survey of 173 companies from the Association of Supply Chain Management found that the biggest obstacle for applying DLT in SCM is a lack of expertise about the technology [30]. One of the main contributors to this issue is the fast-paced evolution of new and existing DLT platforms along with complimentary third-party technologies. This can make the process of identifying which technology stacks support building complex SCM solutions a challenging endeavour. The lack of expertise about DLT can slow down innovation as companies can be reluctant to invest in this novel technology. This gap in expertise can be compensated with the inclusion of rigorous methods that help to identify relevant DLTs for building SCM DApps and thus ease the design and development of such systems.

2.2 Running case

Figure 2 depicts how SCM companies and start-ups along with consumers and societies at large can benefit from the application of DLT in SCM. SCM companies on the left side of Figure 2 are driven to apply DLT in their businesses in order to reduce operational costs and to increase information traceability along with security [30]. The right side of Figure 2 shows how these changes can have positive impacts for both consumers and societies. The operational costs of running supply chains are factored into consumer prices, which can be reduced by an increase in process efficiencies. Traceability provides benefits for both consumers and SCM companies as the provenance of products can be recorded on the distributed ledger and used to validate the origins and authenticity of different products. Improved product transparency can help to reduce counterfeiting of consumer goods and medicines, help trace the sources of food borne illnesses and validate environmental sustainability claims of various companies. Increased visibility and tamper resistance provided by distributed ledgers can help to mitigate corruption and reduce fraud. Although both SCM companies and consumers stand to gain from the application of DLT in SCM, there are currently many barriers such as a lack of expertise about the technology and a lack of tools for DLT implementation [30] shown on Figure 2. Easing the process of DLT selection for SCM can save development resources and time required for creating DApps that are aligned with the goals of SCM.

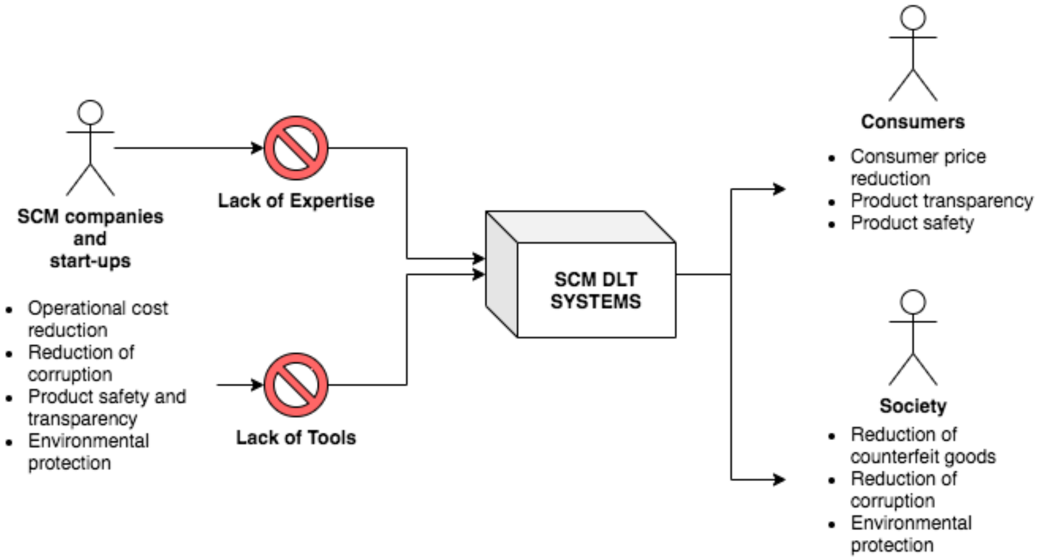

Figure 2. Current barriers and benefits of applying DLT in SCM.

2.3 Preliminaries

This thesis uses concept maps to create a taxonomy of technologies that affect the choice of DLT for SCM in Chapter 3. *Concept maps are graphical tools for organizing and representing knowledge* [31]. *A concept map consists of a graphical representation of a set of concepts, usually enclosed in ovals or rectangles of some type, and relationships between concepts indicated by a connecting line linking two concepts* [32]. Concept maps are chosen since they provide an intuitive way to incorporate and expand knowledge about complex subjects. Concept maps can be used for both learning about a subject and to evaluate the comprehension of a subject.

Decentralized Agent Oriented Modelling (DAOM) [33] framework is used in Chapter 4 to identify generic requirements of SCM DApps through goal modelling. The modelling notation is depicted on Figure 3 as following. Functional goals of a system are depicted as parallelograms. Quality goals representing non-functional requirements are depicted as clouds. Emotional goals that describe feelings towards a function are depicted as hearts. On-chain functions that alter the state of a distributed ledger are depicted as grayed rounded rectangles. Agents that can be either human or autonomous systems are depicted as figures and are assigned roles. The root goal of the DAOM goal modal is the overall system goal. Roles, quality and emotional goals are attached to functional goals and inherited to lower-level functional goals. Functional goals that alter the state of the ledger are placed inside grayed rounded rectangles.

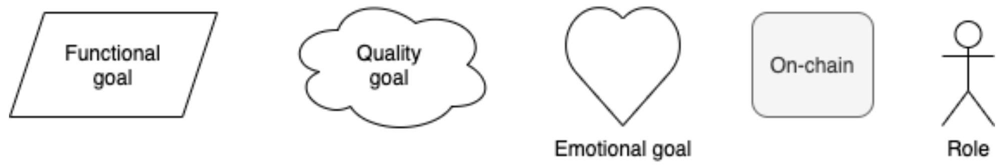

Figure 3. DAOM goal modelling notation.

3 Distributed ledger technology in the context of supply chain management

The following sections present and discuss key technologies that can affect the choice of DLT in SCM in order to provide an answer to RQ1: What technologies are relevant for building SCM specific decentralised applications? In order to explain the nature and relationships between these technologies, they are arranged into categories and presented through concept maps that each answer a sub question that helps to answer the research question. The categories and concept maps are divided into sections with 3.1 dealing with decentralised applications, 3.2 with scalability, 3.3 with privacy and 3.4 with integration and interoperability. Section 3.5 presents relevant technologies for building SCM DApps.

3.1 Decentralised applications

This section presents a concept map shown on Figure 4, that aims to answer the question of what are the technological components of SCM DApps? A decentralised application commonly referred to as a DApp, is a distributed computer system that is able to execute its functions independent of a centralised control system. DApps make use of distributed ledgers, decentralized computing and cryptography to create applications that can perform functions that would require the use of trusted intermediaries in traditional centralised systems. Having application logic distributed amongst decentralised nodes in a P2P network makes DApps resilient to faults and downtimes. DApps can be connected with various systems to provide traceability, automate business processes and reduce operational costs and overhead in SCM.

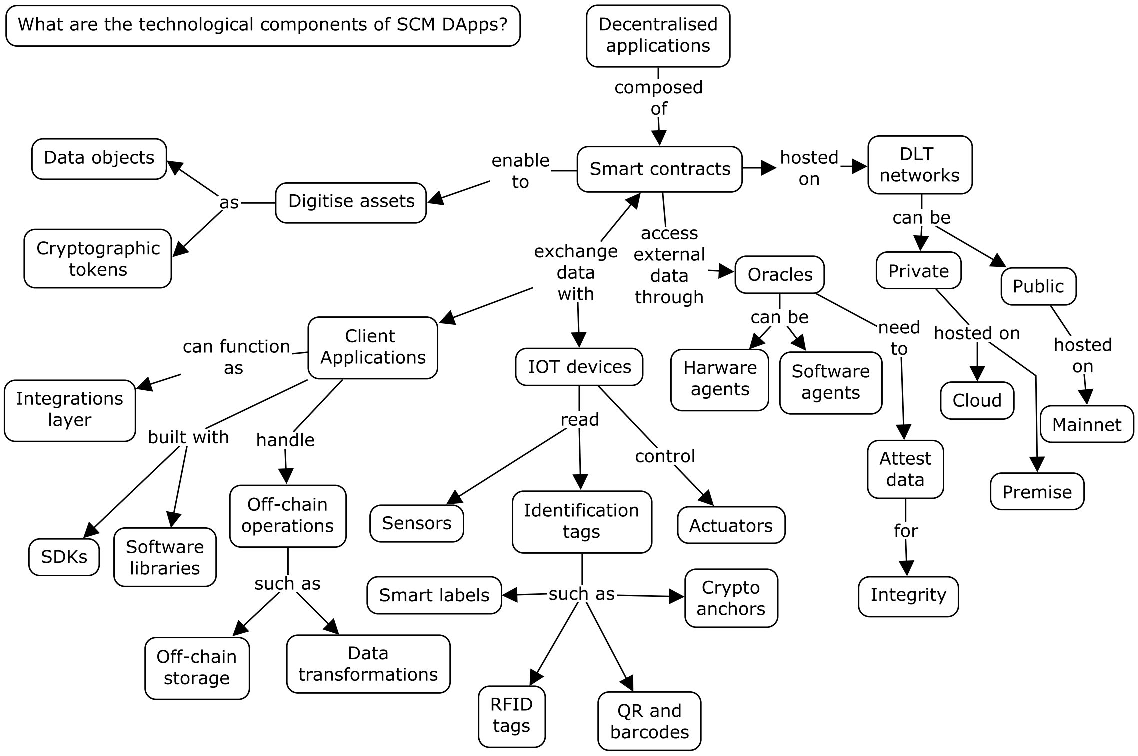

Figure 4. Concept map of SCM DApp components.

3.1.1 DLT networks

DLT networks are composed of peer-to-peer (P2P) nodes running specialised software that allows them to store and replicate the state of a distributed ledger. The most general distinction between different DLT networks structures is that of public and private ones. Public networks allow anyone to view and instantiate transactions as well as host nodes that form the network. Public networks achieve network security and resilience through decentralisation since compromising large networks can become infeasible due to the extensive resources required to do so. Private networks restrict access to a network based on established entities and are governed by a consortium of stakeholders or a single organisation. Private networks are much smaller in size in comparison to public networks, which makes them less decentralised, but as an advantage they can achieve higher transaction throughputs. Private networks can be hosted on premise or in the cloud and they rely on access restrictions for network security.

3.1.2 Smart contracts

Smart contracts are decentralised computer programs that are distributed amongst a group of nodes in a DLT network. Smart contracts allow to encode terms of contracts that can be used to exchange and manage arbitrary data or digital assets such as cryptocurrencies and tokens. Because smart contracts can enforce agreements automatically, they can replace the need for trusted intermediaries in many industries. For instance, a smart contract can be the custodian of an asset until all the necessary conditions for its transfer are met. When a smart contract is invoked, the computation is performed simultaneously on different nodes in a network. The result of the computation is decided by a consensus mechanism and appended to the distributed ledger.

3.1.3 Oracles

Oracles are software and hardware agents that interface with smart contracts in order to provide them with data from external systems. Oracles can be categorised by their data source, trust model, employed design patterns and interactions with smart contracts [34]. To ensure data integrity, oracles can make use of cryptographic proofs, aggregated data and reputation systems to attest accuracy, validity and the origin of data [35]. An effect by which a centralised data source becomes an oracle is called the oracle problem [36], since such a system could become a single point of failure when compromised. This issue is not unique to DLT, but in case of DLT it can diminish many of its decentralisation qualities.

3.1.4 Internet of things

Internet of Things (IOT) refers to a network of physical devices that are capable of connecting to the internet. IOT devices can perform various functions such as gathering and communicating sensor readings and controlling processes through actuators. Smart contracts that are integrated with IOT devices enable to execute business logic in near real-time based on input data without relying on centralized gateways. This can make a DLT powered IOT ecosystems resilient to single points of failure and reduce network loads by distributing data processing and storage to smart contracts. Limited computational power and large volumes of data produced by IOT networks can require specialized solutions to orchestrate devices that act as nodes in a DLT network [37], [22].

3.1.5 Identification technologies

Complimenting traditional technologies such as Radio-frequency identification (RFID), Quick Response (QR) and barcodes are newer identification technologies that can be used in SCM. The concept of smart labels is centered around improving the capabilities of identification labels with the inclusion of sensors, actuators and communication technologies that enable to modify and communicate data about the state and properties of an item [38]. Crypto anchors are another emerging technology that aims to tie a unique identifier to properties of an object that are hard to clone, forge or transfer and that would invalidate the authenticity of an item upon tampering [39]. Both of these technologies can widen the use cases for DLT in SCM by allowing to automate manual processes and protect against fraud and illegal modification.

3.1.6 Client applications

Client applications provide interfaces for interacting with smart contracts and are built with Software Development Kits (SDK) or software libraries that provide a layer of abstraction allowing for easier communication with smart contracts. Client applications can also be used to provide functionalities that due to the limitations of current DLT platforms would otherwise be harder to implement and to provide integrations with other systems.

3.1.7 Summary

Table 1 describes technologies discussed in this section along with inclusion and exclusion criteria that help to identify relevant use cases. In general, SCM DApps need smart contracts, a DLT network to host them and client applications for interacting with smart contracts. The critical decision point here lies in the choice between using a public or a private DLT network, as these may have very different and often contrasting characteristics. The use of other mentioned technologies can vary between use cases. For instance, attesting data coming from oracles helps to facilitate trust in environments where the validity of input data can't be relied on, but it might not be required in scenarios where all stakeholders have already established trust between each other. Similarly, the use of IOT devices and identification technologies is relevant for use cases where a DApp needs to act in response to the physical environment of SCM operations. While some of these technologies might not hold relevance in the initial scope of some SCM DApps, they can become more important as DApps and the ecosystems they support grow to involve different use cases.

Table 1. Criteria for DApps.

Technology category	**Inclusion criteria**	**Exclusion criteria**
Smart contracts	Prerequisite for SCM DApps	
Oracle attestation technologies	Unreliable input data Untrusted data sources Risk of fraud	Data sources are trusted
IOT	Collecting and reacting to data from the environment	
Identification technologies	Identity management of physical assets	
Client applications	Prerequisite for SCM DApps	
Private network	Data privacy Restricted access High throughput Control over governance	Decentralization Transparency Open governance
Public network	Strong network security Transparency Decentralization Open governance	Restricted access Data privacy Low throughput Control over governance

3.2 Scalability

This section presents a concept map shown on Figure 5, that aims to answer the question of what technologies affect the scalability of SCM DApps? The issue of scalability is often referred to as the Scalability Trilemma [40], according to which increasing scalability of a DLT network tends to lower decentralisation and security. The issue of scalability is highly relevant for SCM due to the large volumes of assets that can be tracked by DLT systems. Achieving sufficient transaction throughput is necessary to build SCM solutions that are able to compete with centralised solutions in their value propositions.

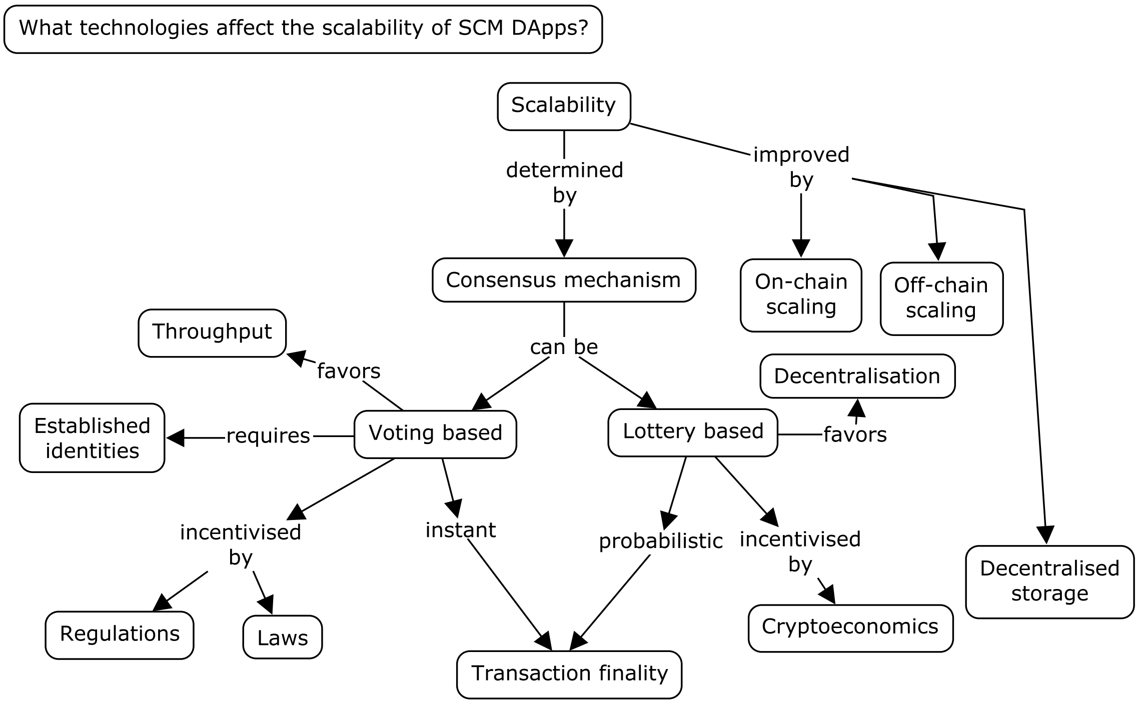

Figure 5. DLT scalability.

3.2.1 Consensus mechanisms

Nodes in a DLT network use a consensus mechanism to come to an agreement about the shared state of a ledger. Depending on the network type, different consensus algorithms can be used, with lottery and voting based consensus algorithms being the two main categories. Lottery based consensus algorithms also known as Nakamoto consensus, provide probabilistic consensus that can be scaled to a high number of nodes. Lottery based consensus algorithms such as Proof of Work (PoW) and Proof of Stake (PoS) are designed for trustless environments of public networks and reward participation in the consensus process through cryptoeconomic incentives. Voting based consensus mechanisms have high transaction throughputs with instant transaction finality but a precursor to using them is that all the nodes participating in the consensus have established entities. This makes them suitable for private networks as they also do not require the use of cryptoeconomic incentives in their consensus process.

3.2.2 On-chain scaling

On-chain scaling also known as layer 1 scaling [41], provides ways to increase transaction throughput by making changes to the underlying DLT protocol. These changes can include changing the size and content of transactions [42], [43], network sharding [44], parallel processing of transactions [45] and using Directed Acyclic Graphs (DAG) [46].

Another approach to on-chain scaling is offered by enterprise DLT platforms Hyperledger Fabric [47] and Hyperledger Sawtooth [45] which offer pluggable consensus that allows to implement different consensus algorithms without changing the core protocol.

3.2.3 Off-chain scaling

Off-chain scaling also known as layer 2 scaling [41] aims to increase transaction throughput by moving some of the transactions away from the main ledger, while maintaining to use it to verify and store the outcomes of off-chain transactions. Examples of off-chain scaling solutions are state channels [48], [49], side chains [50], plasma [51], ZK-rollups [52] and cross-chains [53], [54].

3.2.4 Decentralized storage

Decentralized storage solutions aim to overcome the limitations on the size of data that can be processed by distributed ledgers. Solutions such as IPFS [55], FileCoin [56], Sia [57], Storj [58] and Swarm [59] distribute files among peers in a P2P network and can provide cryptoeconomic incentives to nodes hosting files. Decentralised storage model fits DLT by avoiding single points of failure and centralised control mechanisms.

3.2.5 Summary

Table 2 describes technologies discussed in this section along with inclusion and exclusion criteria that help to identify relevant use cases. Scalability of SCM DApps is tied to consensus mechanisms employed by DLT networks. The two main options are either to use voting-based consensus mechanisms that provide high throughput but can only be used if the all the nodes participating in consensus have established identities or to use lottery-based consensus mechanisms which are suited for highly decentralised networks at the expense of lower transaction throughput. Scalability of a DLT network can also be increased with the inclusion of on-chain and off-chain scaling technologies. While the former can be applied only in circumstances where the DLT protocol itself can be modified, the latter can be used without modifying the protocol. In both cases the addition of scalability technologies will increase the complexity of a solution and therefor require more resources for development.

Table 2. Criteria for scalability.

Technology category	Inclusion criteria	Exclusion criteria
Voting based consensus	Identity based access High throughput	Decentralization
Lottery based consensus	Decentralization	Identity based access Low throughput
On-chain scaling	DLT protocol can be modified High throughput	Added complexity is not proportional to added value
Off-chain scaling	DLT protocol can't be modified High throughput	Added complexity is not proportional to added value
Decentralized storage	Processing of large files	

3.3 Privacy

This section presents a concept map shown on Figure 6, that aims to answer the question of what influences data privacy of SCM DApps? In many SCM scenarios there are limitations on the data that can be disclosed between different parties due to laws and regulations. Data privacy can also be required in situations where certain parties want to protect confidential data from competitors or adversaries. Privacy is mainly determined by the permission models of DLT networks and can be increased through the use of privacy-oriented technologies and data policies.

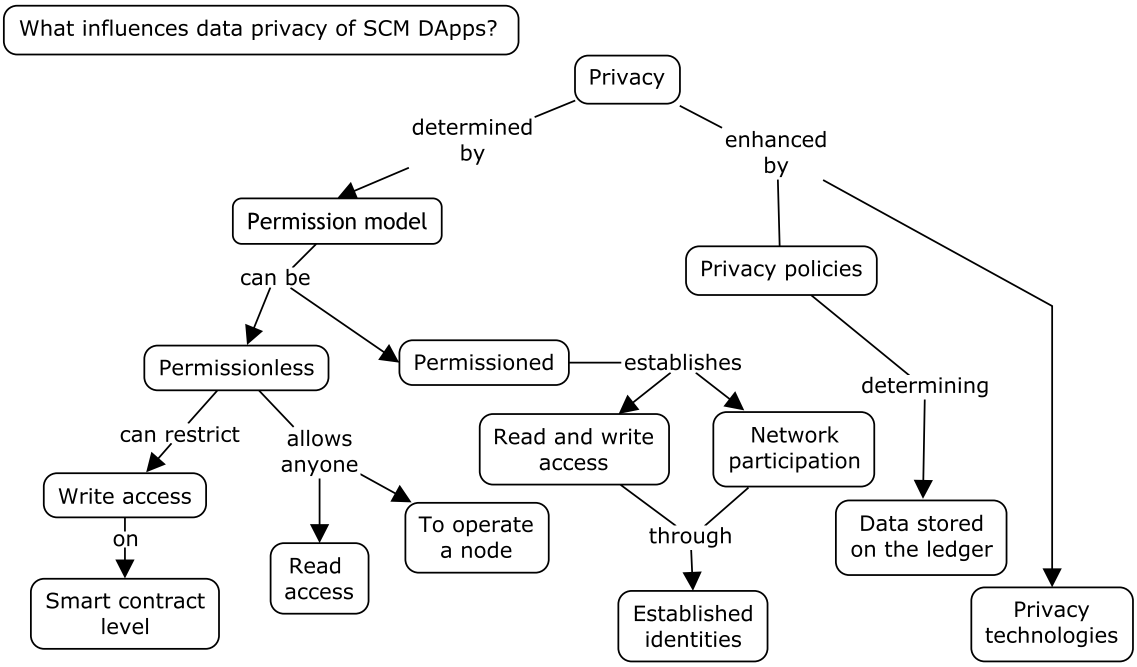

Figure 6. DLT privacy from the perspective of SCM.

3.3.1 Permission model

A permission model determines access rights on a DLT network. The two main permission models used in DLT are permissioned and permissionless. The permissionless model employed by public networks allow anyone to view the state of a ledger, operate a node and access smart contracts. Permissioned networks determine access rights based on established identities and roles. The need for permissioned networks originates from enterprise use cases where different confidentiality and compliance requirements place restrictions on data access and processing.

3.3.2 Data privacy

Implementing privacy policies requires collaboration between different stakeholders and regulators to establish what data can be shared on a distributed ledger. This can be due to laws and regulations governing different SCM processes or to limit the data exposed to competitors and adversaries. Data privacy and security can be further enhanced with the inclusion of different privacy-oriented technologies that leverage cryptographic techniques to obfuscate, encrypt or prove the existence of information without revealing its content. Examples of privacy technologies used or researched for use in DLT are zero knowledge proofs [60], state channels [48], [49], indistinguishable obfuscation [61], [62] and homomorphic encryption [63], [64], [62].

3.3.3 Summary

Table 3 describes technologies discussed in this section along with inclusion and exclusion criteria that help to identify relevant use cases. Vast majority of SCM DLT use cases need to ensure measures for data privacy and protection that originate from existing business models and compliance requirements. DLT networks support permissioned and permissionless access models which both come with trade-offs. Privacy requirements can make SCM DApps more inclined towards permissioned networks, but the downside to this approach lies in the need for some form of a centralized authority that grants access rights and assigns roles. Permissionless networks can offer an alternative due to their focus on decentralization but since all data is stored publicly, they need to employ privacy technologies to ensure data privacy and protection. These technologies are not limited to permissionless networks and their inclusion adds to the complexity of DApp design, requiring more resources for development.

Table 3. Criteria for privacy.

Technology category	**Inclusion criteria**	**Exclusion criteria**
Permissioned DLT	Identity based access Data privacy	Transparency Decentralization
Permissionless DLT	Privacy technologies Decentralization Transparency	Identity based access Data privacy
Privacy technologies	Data privacy	Added complexity is not proportional to added value

3.4 Integration and interoperability

SCM systems often consist of various subsystems that handle different aspects of SCM operations. The inclusion of DLT into such ecosystems requires the ability to connect and exchange data between a wide array of different systems that can belong to different organizations. In order to enable such broad options for connectivity, DLT systems offer tools and technologies that allow to integrate vastly different systems. To enable cross-industry connectivity, DLT solutions needs data architecture standards that can ease the processes of data migration, exchange and analysis. Figure 7 show the concepts of integration and interoperability applied to SCM.

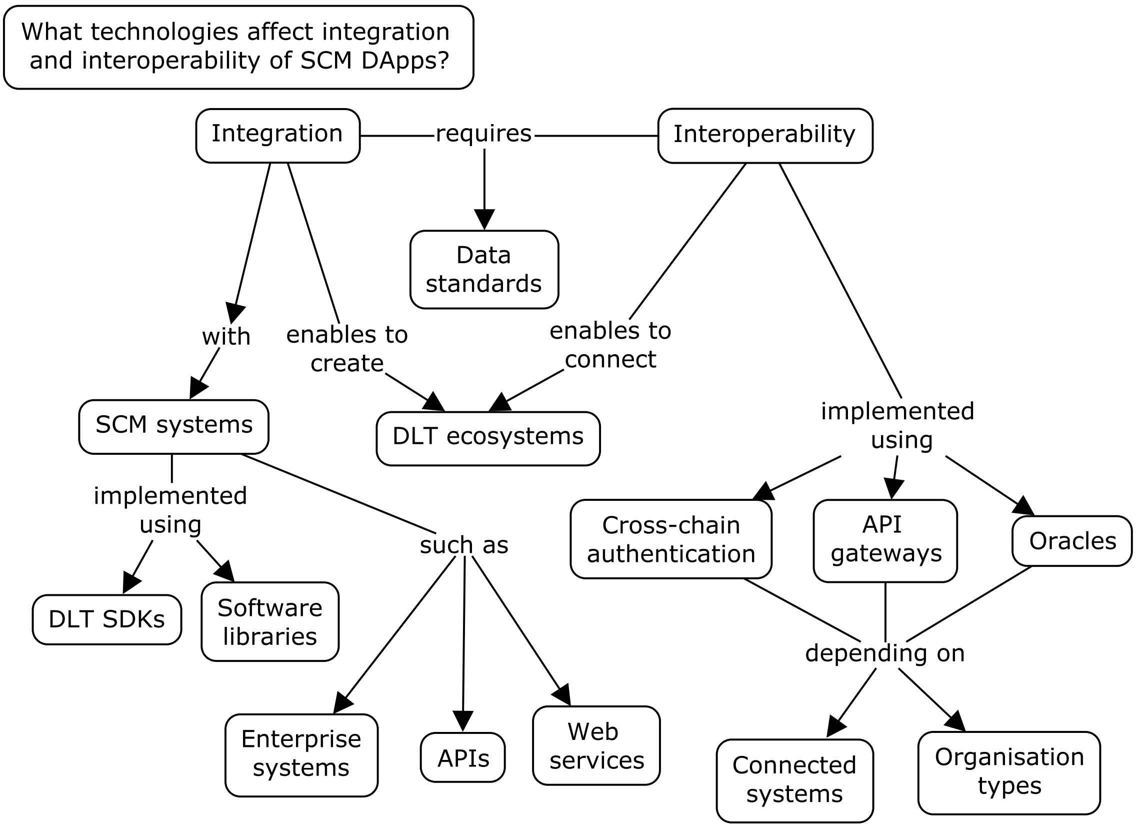

Figure 7. DLT integration and interoperability from the perspective of SCM.

3.4.1 Integration

In order to provide integrations with centralised systems, DLT platforms usually implement some form of SDKs and software libraries written in general purpose programming languages that enable to interact with the distributed ledger using prevalent programming tools. This approach enables developers with no prior experience with DLT to implement various software architectures that integrate DLT with existing technologies. Integrations are important to many SCM companies that have long running legacy systems that need connectivity with DLT.

3.4.2 Interoperability

DLT interoperability allows DLT networks with different core protocols to interact and exchange data with each other, enabling to connect different ecosystems and industry specific networks into greater value chains. Without interoperability DLT networks, especially more purpose-built networks, can run into the risk of turning into siloed ecosystems. Different approaches available for SCM DApps include cross-authentication, API gateways and oracles and are dependent on the systems that are to be connected and the types of organisations that operates them [65].

3.4.3 Summary

Table 4 describes technologies discussed in this section along with inclusion and exclusion criteria that help to identify relevant use cases. Integrations enable to create DLT ecosystems and to exchange data with existing SCM systems. While integrations are a present prerequisite, it's likely that as the use of DLT becomes more prevalent, interoperability between DLTs will be required to enable cross-industry use cases that connect different ecosystems.

Table 4. Criteria for integrations and interoperability.

Technology category	Inclusion criteria
SCM systems integrations	Prerequisite for SCM DApps
DLT interoperability	Intersection points with other DLT networks Multi-chain solutions

3.5 Relevant technologies for SCM DApps

Common prerequisites for SCM DApps include smart contract support, data privacy and protection, high transaction throughput and the ability to integrate DLT with existing SCM systems. This makes private permissioned DLTs a potential candidate for SCM DApps since they provide privacy through identity-based access, which also allows them to use consensus mechanisms that support high transaction throughput. The downside to this approach is centralization as such networks need to be governed by some entity that manages access rights and determines who gets to participate in the network. Public permissionless DLTs offer an alternative due to their focus on decentralisation and open participation which grants them high data transparency but poses challenges for achieving data privacy since all transactions are publicly accessible. Public DLTs also need highly decentralized consensus mechanisms which affect their transaction throughput. Both privacy and scalability can be improved with the inclusion of specialised technologies which widen the use cases for different DLTs but also increase the complexity of DApp design and development. The need for different technologies and the available options are greatly influenced by the type of DLT, making it one the key design decision in SCM DApp development.

Alongside technologies that pertain directly to DLT platforms are those that interface with DApps in order to extend their capabilities. These can range from IOT devices, oracles and interoperability solutions. While being able to integrate DApps with existing SCM systems is one of the prerequisites for DLT selection, the use of other technologies is more dependent on the use case. One of the key considerations for SCM DApps is how to provide data integrity. This can be achieved by attesting oracle data, using identification technologies, IOT or simply by trusting that network participants behave honestly. The combination and necessity of forementioned technologies can be highly specific to a use case but should be considered early on as inclusion of these technologies can alter the design of a system and pose compatibility requirements for a chosen DLT stack. The same holds true for business process automation through IOT, integrations and DLT interoperability as each such component might alter a system's requirements.

4 Generic requirements of supply chain management DApps

The following sections use DAOM goal modelling framework to provide an answer to RQ2: What are the generic requirements of SCM specific decentralized applications? Section 4.1 shows the main value proposition offered by DLT in SCM. Section 4.2 presents a generic goal model that applies to various provenance and data sharing solutions in SCM. Section 4.3 presents the generic requirements of SCM DApps.

4.1 Value propositions

SCM is an established field that can benefit from the inclusion of DLT since some of the value propositions offered by DLT coincide with relevant challenges of current centralised technologies. Among these are tracking and sharing data along the full life cycle of supply chains as well as opportunities to connect and automate various SCM systems. In order to fit into various ecosystems, SCM DApps need to offer capabilities that are compatible with the goals of using DLT in SCM. The root value proposition of *Supply chain provenance and data sharing* presented in the model on Figure 8, is chosen for its fit for common SCM DLT use cases. Supply chain provenance can be used to track and analyse the flow of assets along full life cycles of SCM processes and to enable collaboration by securely sharing data between relevant stakeholders. The quality goals for this level are scalable, secure, trusted and integrable which apply to all functional goals below. These quality goals are selected to ensure compatibility with existing business models, SCM systems and compliance requirements. Scalable means that a system is capable of handling a large number of simultaneously occurring processes. Secure refers to the confidentiality, integrity and availability of data and authorized access. Trusted means that the stakeholders can place trust in the stored data and the technology used to manage and govern a DApp. Integrable refers that a DApp can be integrated with external centralized systems.

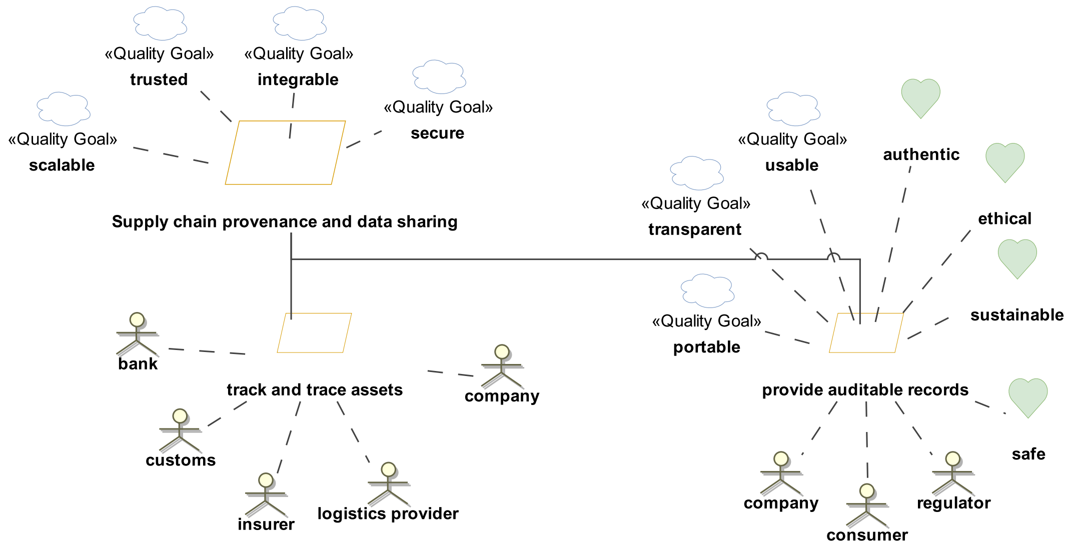

Figure 8. SCM DApp goal model.

While DLT can be used in SCM for various use cases such as providing provenance of goods [66], [67], tracking shipments [1], [68], supply chain digitalization [69] and trade finance [70], [71], [72], the majority of these use cases at their core deal with functions pertaining to tracking and tracing assets such as physical goods, shipments and documents. Functional goal *track and trace assets* is mainly aimed at enterprise collaboration involving different roles depicted in the left side of Figure 8 as following. A company refers to a generic stakeholder responsible for producing, manufacturing, modifying or changing ownership of an asset that is managed by a SCM DApp. While this broad definition covers majority of different stakeholders, following notable roles are brought forth to illustrate the variety of stakeholders involved in many SCM processes, especially in regard to global trade. These include logistics providers, banks, customs agencies and insurance providers amongst others.

Distributed ledgers can be used to determine the provenance of different assets. The functional goal of *provide auditable records* shown on the right side of Figure 8, allows companies to securely share data in a manner that allows for the verification and analysis of stored data. The role of consumer in this context refers to a stakeholder that consumes the final goods or services provided by companies involved in SCM processes. The role of regulator refers to a stakeholder that is mandated to request records in order to meet compliance requirements. Company refers to a stakeholder that is involved in SCM operations. Transparent refers that the transactions recorded on a distributed ledger have high visibility to different stakeholders. Usable refers that a system provides an intuitive way for interacting with a DApp. Portable refers that a system can be used on different computing platforms. Emotional goals of ethical, sustainable, safe and authentic originate from market pressures created by increased consumer awareness and demand for goods and services that appeal to these values. Ethical refers to that goods or their composite materials are sourced from or produced in conflict free areas and in accordance with international laws. Sustainable refers to that products or processes meet environmental sustainability goals. Safe refers to the ability to validate the safety of goods by examining their provenance. Authentic refers to the ability to determine authenticity of goods by examining their provenance.

4.2 Generic functions of SCM DApps

Figure 9 shows the refinement goal model with generic functions that can be used to realize the enterprise focused functional goal of *track and trace assets*. Generic functions *define transaction rules*, *digitize asset, invoke transaction*, *emit event*, *listen to event* and *view transaction*, *view transactional history* shown on Figure 9 provide a basis that can be used to implement more use case specific functions. The top-level quality goals of scalable, secure, integrable and trusted are inherited from the main value proposition and applied to functions below. The new quality goals introduced in this model are highly-automated and modifiable. Highly-automated refers to a function been carried out with minimal or no involvement from stakeholders. Modifiable refers to a function being responsive to changes in context. The role of stakeholder is a generic role that refers to any stakeholder that participates in SCM operations, while acknowledging that different use cases and implementations assign and limit functionalities to more specific roles.

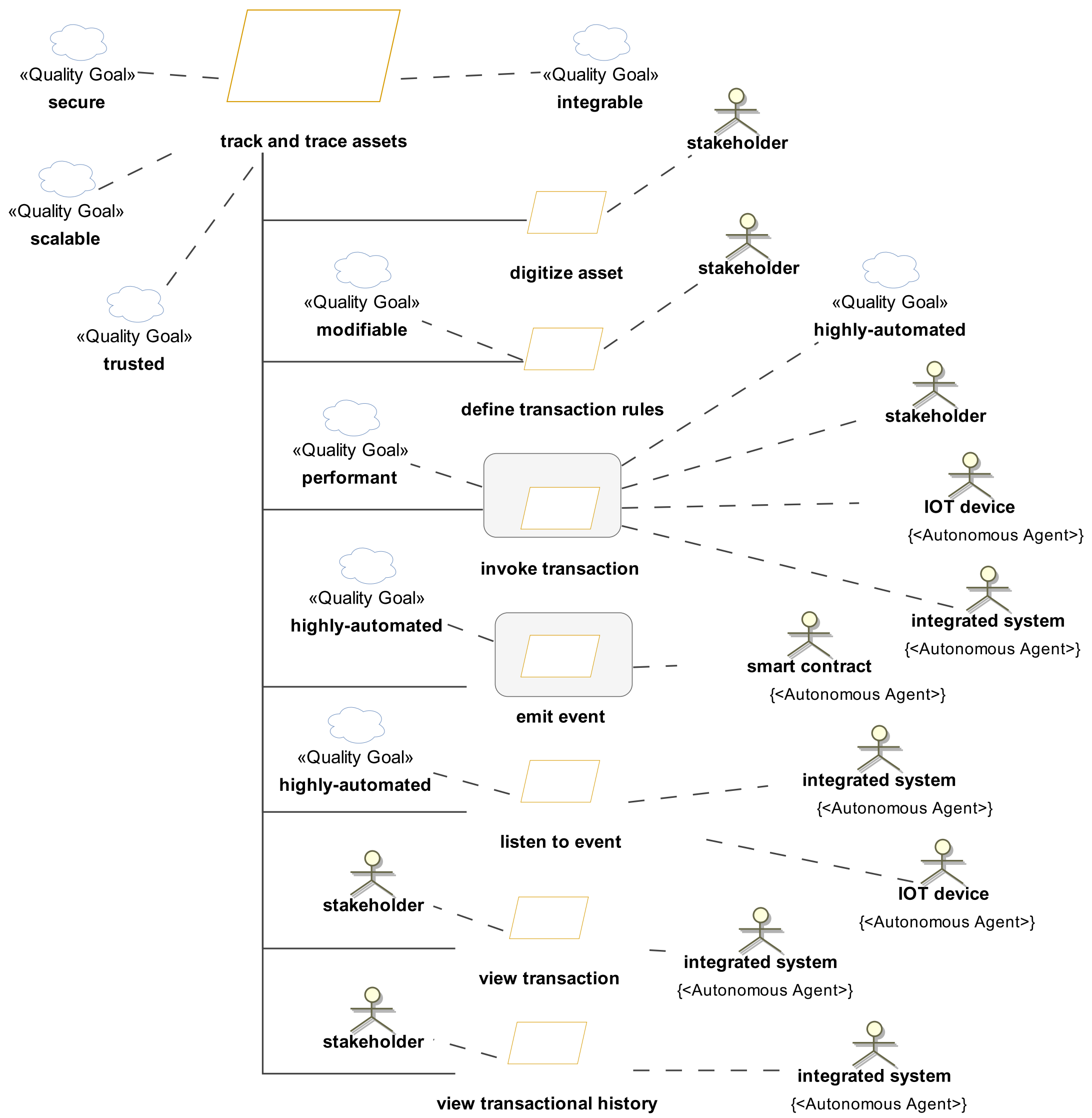

Figure 9. Asset management goal model.

By creating digital representations of assets such as goods, shipments and documents, DApps can be used to track the provenance of different assets along supply chain processes and to share that data with relevant stakeholders. In order to create digital representations of assets, relevant stakeholders need to decide upon data formats that are compatible between existing SCM systems and the distributed ledger. To control the flow of assets according to predefined business rules, stakeholders also need to define how they can be encoded onto smart contracts. Due to the collaborative and long running nature of both DLT and SCM systems, such rules can be suspectable to change and thus SCM DApps need to ensure mechanisms that allow for their modification. SCM DApps also need to ensure that smart contracts are invokable by systems belonging to different stakeholders. The latter ensures that business processes can be automated in order to replace manual steps and create new business flows. In some cases, this can help to make DApps more autonomous for instance direct IOT integrations with smart contracts allow to enforce business rules based on changes in environmental conditions. Integrations can also raise requirements for smart contract performance in case they are used to process large volumes of data or to process data in near real-time. Since DLT networks are closed systems, they often employ event-driven patterns to notify other systems of changes. A common way to achieve this is to have smart contracts relay events in the scope of different transactions that can be picked up by systems listening for them. Results of transactions are stored on a distributed ledger where they need to be accessible to all relevant stakeholders and integrated systems. In order to track the provenance of different assets, SCM DApps need to provide ways by which historical records of transactions can be retrieved for specific assets. Using a shared ledger to store data enables stakeholders to collaborate and gain oversight of data and processes that are not available due to the segmented nature of centralised SCM.

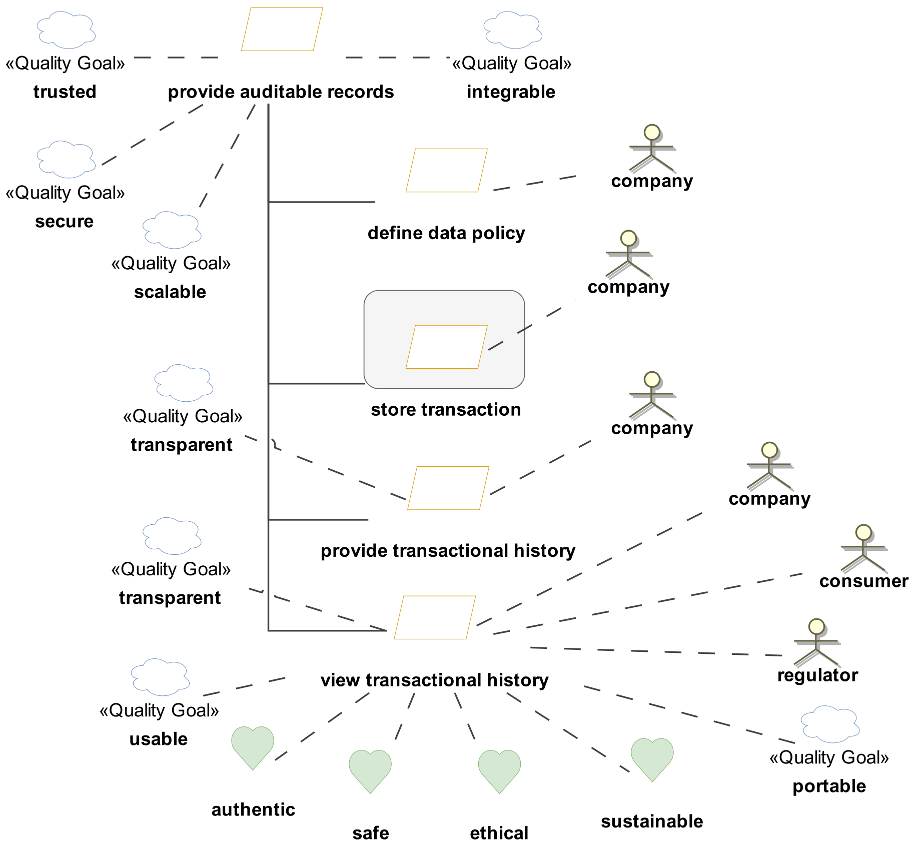

Figure 10. Auditable records goal model.

Figure 10 shows a goal model with generic functions *define data policy*, *store transaction*, *provide transaction history* and *view transaction history* that enable SCM companies to provide an auditable trail of records. Auditable records provide visibility into SCM processes which may be required in order to comply with regulations or to provide information to consumers that helps to verify different qualities of products while also reducing harm caused by unsafe or fraudulent products. Another application for auditable records is to improve and develop computational models by analysing vast amounts of SCM data which can lead to advancements in related fields as well as bring positive societal outcomes such as reducing shortages of goods or reenforcing vital supply lines. SCM operations often involve handling of confidential data, therefor it's necessary to implement policies that define the data and the extent to which it can be made available to stakeholders that are not involved in SCM operations. Data provenance is established by recording all relevant SCM events as transactions on a distributed ledger. In order to inspect the lifecycles and provenance of specific assets and processes, companies involved in SCM operations need to organize related transactions in a manner that provides transparency into the data itself and the ways in which it was recorded. The usefulness of such data is among other factors dependent on the way by which it is accessible to interested parties. This can include being available on different computing platforms as well as the overall useability of such solutions especially in regard to consumer-oriented applications.

4.3 Generic requirements

Through applying the DAOM framework on common SCM use cases, a generalized goal model was deduced in order to examine generic requirements of SCM DApps. The aim of this model is to identify generic stakeholders, functional and quality goals that can be used in system design process to improve the compatibility of DLT stacks with SCM use cases. Generic requirements for SCM are strongly influenced by current modes of operations and the challenges of existing centralized solutions. As such the generic functional requirements are centered around providing shared data provenance with possibilities for achieving higher business process automation. Quality requirements of *trusted*, *secure*, *scalable* and *integrable* aim to ensure that DLT can be fitted alongside existing business models and centralized systems. While these qualities are desirable for majority of SCM DApps, individual use cases may pose requirements that aim to maximize other aspects of DLT. This can limit the extent to which this model can be applied outside initial stages of DApp design. A possible solution would be to create generic templates that are specific to different SCM areas. Such templates could be used to prototype DApp designs that can be extended to meet use case specific requirements.

5 Assessment method

The following sections present an assessment method that can be used to identify components of a DLT stack in order to provide an answer to RQ3: Which DLT stacks are suitable for use in SCM? Section 5.1 gives an overview of the assessment method. Sections 5.2 to 5.7 discuss technology categories used in the assessment process. Section 5.8 presents mappings between the assessment method and BPS DSS. Section 5.9 presents DLT stacks that are suitable for building SCM DApps.

5.1 Overview

The aim of the assessment method is to provide a tool for identifying DLT stacks that can be used to design and develop SCM DApps based on use case requirements. The assessment method consists of linear steps shown on Figure 11, that are organized based on technologies identified in Chapter 3. Each category contains a decision tree that is organized as following, at the root of a tree is a decision point presented as a question with a binary outcome of yes or no, that either yields a component of the stack or branches further following a similar structure. Decision points are based on technologies identified in Chapter 3 and generic requirements identified in Chapter 4. The steps are ordered so that decisions that affect more than one category can be made sequentially and, in some cases, to provide input for further decision points. The assessment method is constrained to determining categories of technologies as the complexity of identifying individual technologies puts it outside the scope of this paper. This limitation can be in part compenstated by using the outcome of the assessment method as input for BPS DSS. By combining the two methods it's possible to determine a set of suitable DLT platforms as well as the necessity for complimentary technologies such as IOT and oracle attestation methods.

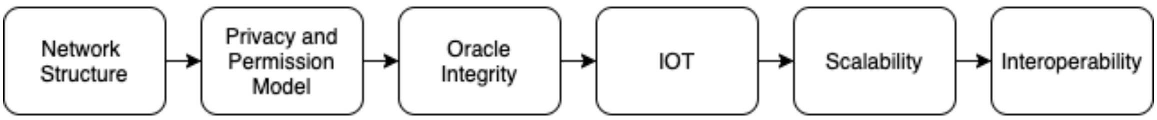

Figure 11. Technology categories for DLT stack assessment.

The conceptual model that combines both methods is shown on Figure 12. Decision outcomes that correlate with feature requirements from BPS DSS are given weights based on the MoSCoW prioritization technique as required by BPS DSS. Mappings between the assessment method and BPS DSS are further explained in Section 5.7.

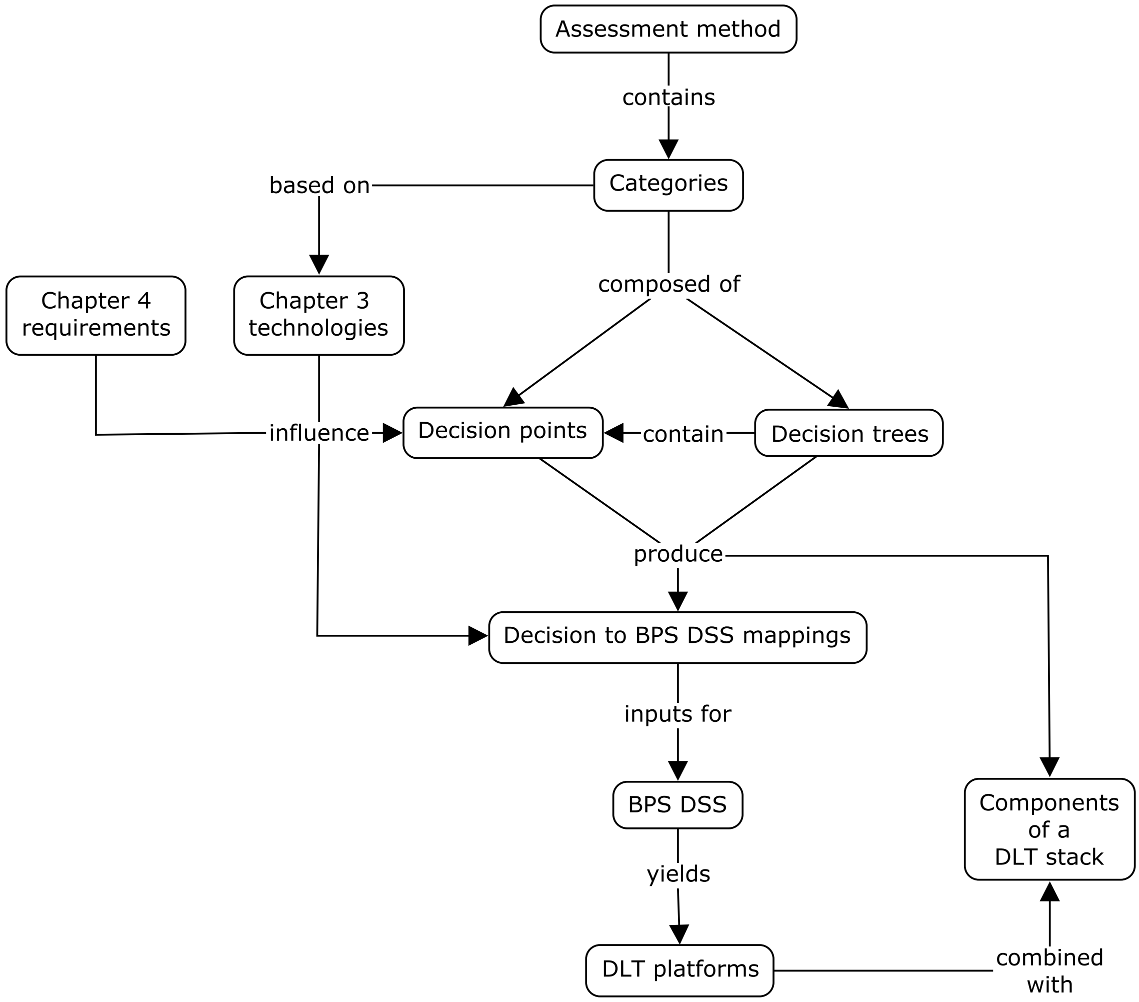

Figure 12. Conceptual model of the assessment method.

5.2 Network structure

Decision tree depicted on Figure 13 determines which DLT network structure fits a given use case. DLT networks are further discussed in Section 3.1.1.

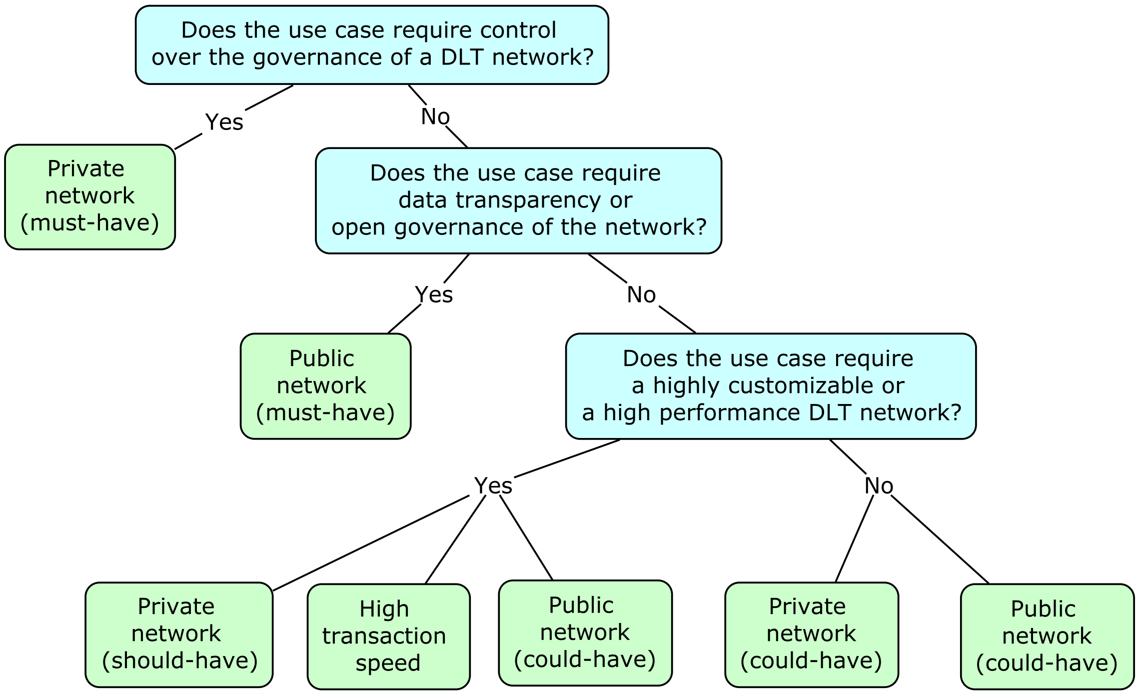

Figure 13. Decision tree for DLT network type.

Table 5 presents decision points along with descriptions and relevant criteria from Section 3.1.7 Table 1 and criteria introduced for this category. The outcomes from this category correlate with the following BPS DSS feature requirements *Public, Private, Transaction speed – High* and are given weights according to their effect on decision points.

Table 5. Decision points network structure.

Question	**Criteria**	**Description**
Does the use case require control over governance of a DLT network?	+ Data privacy + Restricted access + Control over governance + High throughput - Control over network governance is not required	Governance determines who can host nodes, access or make changes to the network and manage network operations.
Does the use case require data transparency or open governance of the network?	+ Transparency + Open governance + Decentralization - Data transparency is not required - Open governance is not required	Transparency provides SCM process visibility that can be used to verify data and to provide data provenance. Open governance can protect against concentration of influence over the operations or management of a DLT network.

Does the use case require a highly customizable or a high performance DLT network?	+ Modifiable core protocol + High throughput + DLT implemented in a technically complex environment - Protocol modifications are not required - Average throughput	Customization can be required to alter the behaviour of the core protocol in order to change ledger architecture or the consensus mechanism.

5.3 Permission model

Decision tree depicted on Figure 14 determines the permission model of a DLT network and whether privacy technologies are required for a given use case. Permission models are further discussed in Section 3.3.1 and privacy technologies in Section 3.3.2.

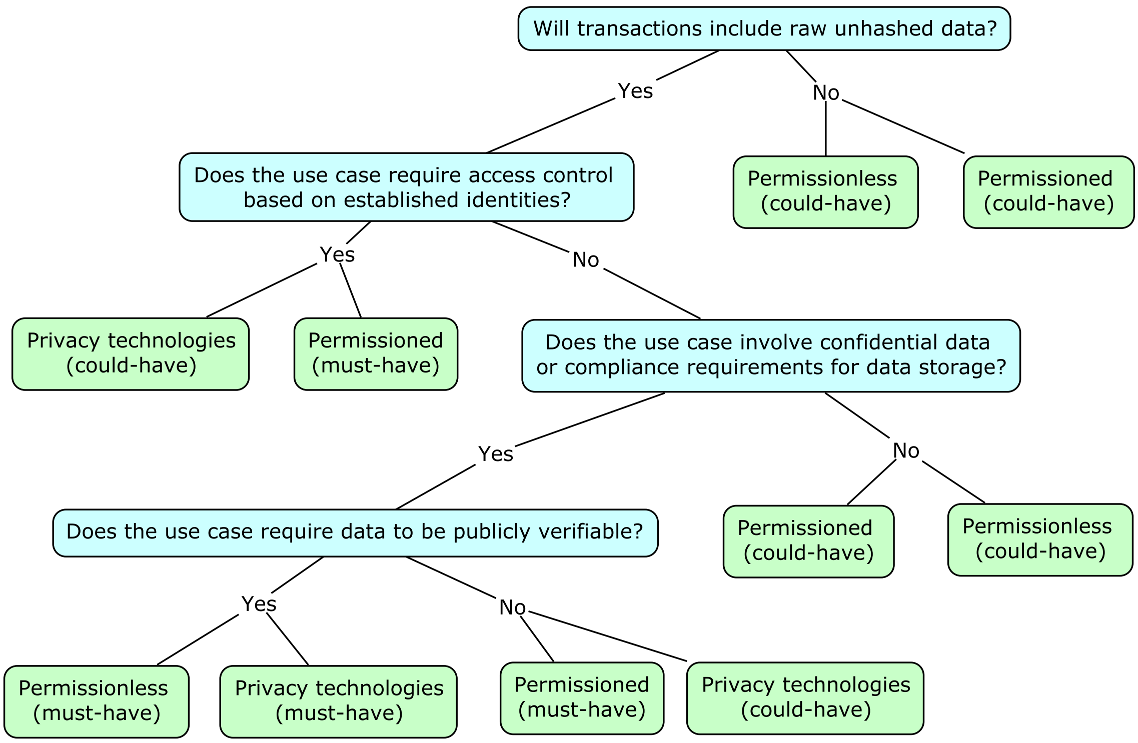

Figure 14. Decision tree for permission model and privacy technologies.

Table 6 presents decision points along with descriptions and relevant criteria from Section 3.1.7 Table 3 and criteria introduced for this category. The outcomes from this category correlate with the following BPS DSS feature requirements *Permissionless, Permissioned, Privacy technologies* which are given weights according to their effect on decision points.

Table 6. Decision points for permission model and privacy technologies.

Question	Criteria	Description
Does the use case require storing unhashed data on a distributed ledger?	+ Ledger used as a database - DApp used only for off-chain data verification	Storing hashes instead of raw data enables to verify the integrity off-chain data, while also limiting utility for other use cases.
Does the use case require role or identity-based access to DApp functions?	+ Identity based access + Data privacy - Identity based access is not required - Open access	Identities can be used to grant different levels of access and to comply with regulations such as Know Your Client (KYC) requirements.
Does the use case involve confidential data or compliance requirements for data handling?	+ Compliance requirements + Confidential data + Data privacy - Confidential data is not stored on the ledger	Regulations can pose requirements for the way certain data is handled. Data confidentiality can also be required to protect sensitive data from competitors or adversaries.
Does the use case require data to be verifiable by anyone on the network?	+ Existence of data or its integrity needs to be verifiable across the network - Data contents are available only to certain parties	Use cases that require keeping data contents confidential while making verification available across the network, can utilize various privacy technologies to do so.

5.3.1 Oracle integrity

Decision tree depicted on Figure 15 determines if attestation methods are required to improve the integrity of data originating from oracles. Oracles are further discussed in Section 3.1.3.

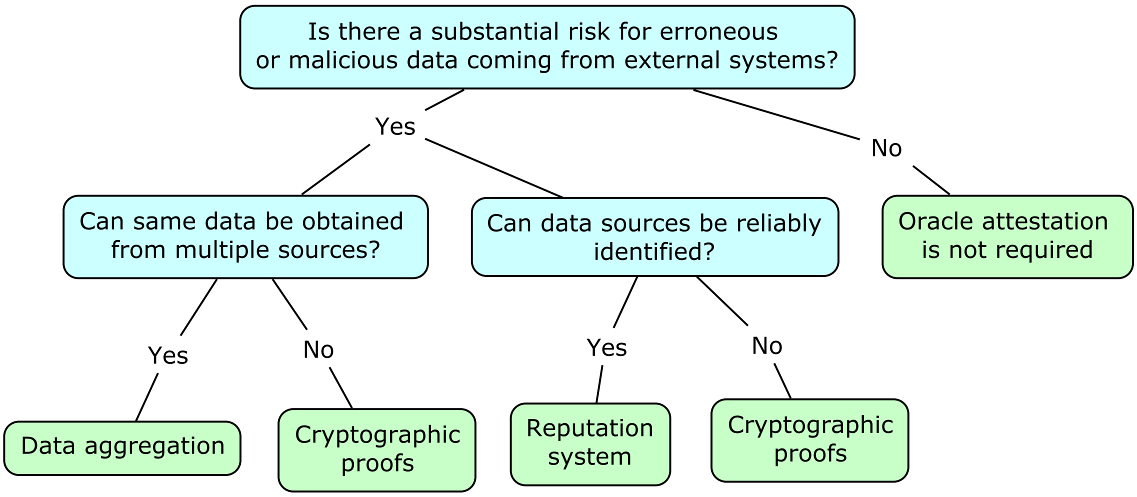

Figure 15. Decision tree for oracle integrity.

Table 7 presents decision points along with descriptions and relevant criteria from Section 3.1.7 Table 1 and criteria introduced for this category.

Table 7. Decision points for oracle integrity.

Question	**Criteria**	**Description**
Is there a risk of erroneous or fraudulent data coming from external systems?	+ Unreliable input data or untrusted data sources - Trusted data sources	Oracle attestation methods can protect against data faults originating from external systems that can’t be recognized by consensus mechanisms.
Can same data be obtained from multiple sources?	+ Multiple data sources - Single sources of data	By aggregating data from multiple sources, the impact of individual faults can be reduced. Oracles can use cryptographic proofs to verify the integrity of data coming from a single source.
Can data sources be reliably identified?	+ Identities of external data sources are verifiable - Identities of external data sources can't be reliably verified	Identities can be used to build reputation systems, while data sources that can’t be reliably verified can be attest by oracles using cryptographic proofs.

5.4 IOT

Decision tree depicted on Figure 16 determines whether IOT is applicable for a given use case. IOT in the context of SCM DApps is further discussed in Section 3.1.4.

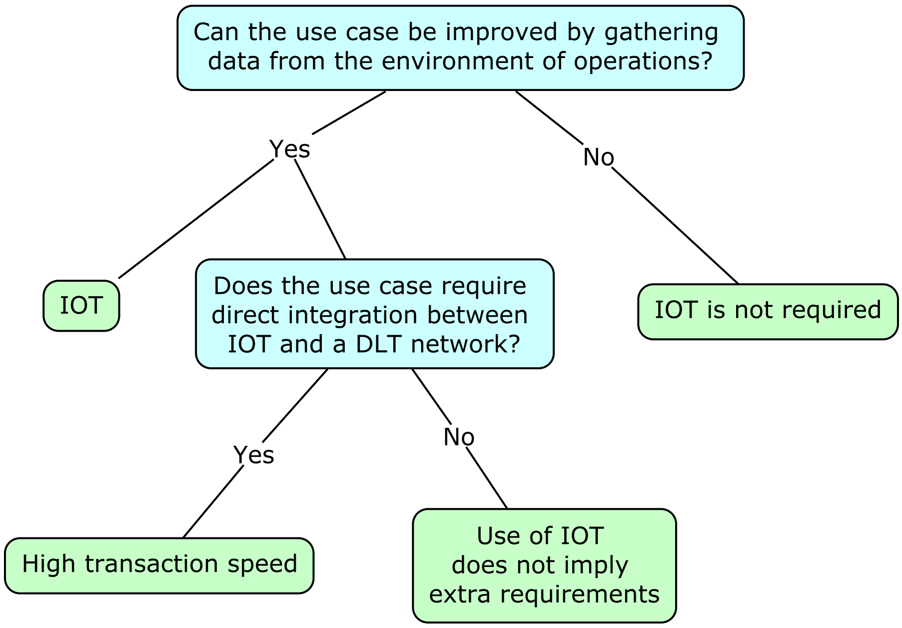

Figure 16. Decision tree for IOT.

Table 8 presents decision points along with descriptions and criteria introduced for this category. The outcomes from this category correlate with the following BPS DSS feature requirement *Transaction speed – High*.

Table 8. Decision points for IOT.

Question	**Criteria**	**Description**
Can the use case be improved by gathering data from the environment of operations?	+ Automated process tracking + Use case involves tangible assets + Conditions of assets affect business processes - Use case doesn't involve tangible assets	IOT can be used to monitor and relay data about different conditions and processes.
Does the use case require direct integration between IOT and a DLT network?	+ DLT processes IOT data + Highly automated - DLT used only to store IOT data	Direct integration allows to autonomously execute smart contracts in near real-time.

5.5 Scalability

Decision tree depicted on Figure 17 determines the scalability requirements of a given use case. Scalability is further discussed in Section 3.2.

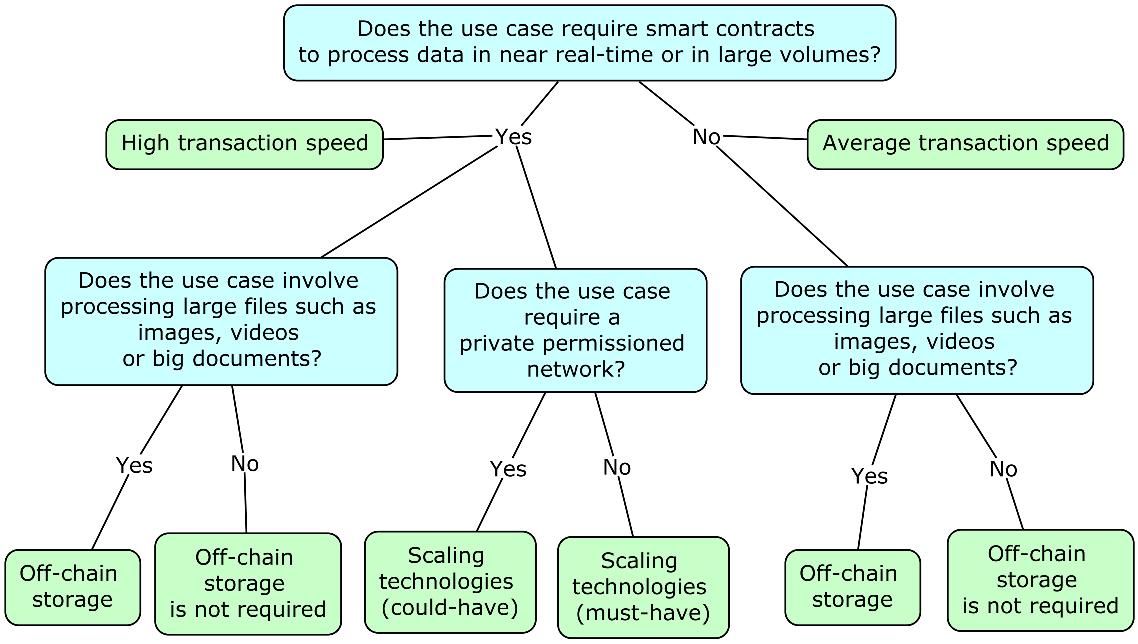

Figure 17. Decision tree for scalability.

Table 9 presents decision points along with descriptions and relevant criteria from Section 3.2.5 Table 2 and criteria introduced for this category. The outcomes from this category correlate with the following BPS DSS feature requirements *Transaction speed – Average, Transaction speed – High, Scaling technologies* which are given weights according to their effect on decision points.

Table 9. Decision points for scalability.

Question	**Criteria**	**Description**
Does the use case require smart contracts to process data in near real-time or in large volumes?	+ Large data volumes + Near real-time data processing + Enterprise system integrations - Moderate data loads - Few integrations with external systems	Near real-time processing of data allows to use DLT to autonomously execute business rules based on incoming data. Yes, if IOT will be integrated directly to DLT

Does the use case require a private permissioned network?	+ High throughput + Control over governance + Identity based access - Open governance - Decentralization	Identity based network structures enable private permissioned networks to use consensus mechanisms that achieve high throughputs at the cost of centralization. Yes, if private permissioned network has been determined. No, if public or permissionless network has been determined.
Does the use case involve storing or processing large files such as images, videos or big documents?	+ Processing or storing large files - Processing or storing large files on-chain	Current DLT network designs aren't well suited for processing large files, requiring off-chain data storage.

5.6 Interoperability

Decision tree depicted on Figure 18 determines whether DLT interoperability is applicable to a given use case. Interoperability is further discussed in Section 3.4.2.

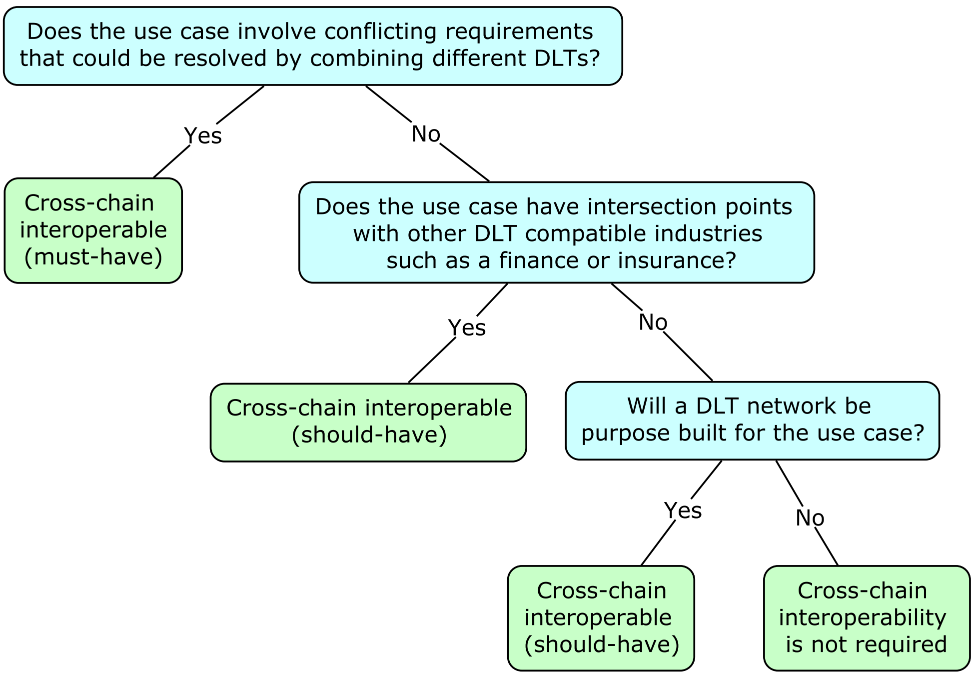

Figure 18. Decision tree for DLT interoperability.

Table 10 presents decision points along with descriptions and relevant criteria from 3.4.3 Table 4 and criteria introduced for this category. The outcomes from this category correlate with the following BPS DSS feature requirements *Cross-chain interoperable* and are given weights according to their effect on decision points.

Table 10. Decision points for DLT interoperability.

Question	**Criteria**	**Description**
Does the use case involve conflicting requirements that could be resolved by combining different DLTs?	+ Needs both transparency and privacy + Needs both decentralization and scalability - Use case doesn't involve conflicting requirements	Complex use cases can leverage the combination of different DLT networks to combine functionalities that cater to different stakeholders or business processes.
Does the use case include intersection points with other DLT compatible industries such as a finance or insurance?	+ Intersection points with financial, insurance, manufacturing or retail industries - Use case doesn't expand to other industries	Interoperability can be used for connecting industry specific networks into greater value chains.
Will a DLT network be purpose built for the use case?	+ Restricted access + Control over governance	Interoperability can be used to bridge isolated DLT ecosystems to enable broader collaboration. Yes, if private network structure has been determined. No, if private network structure hasn't been determined.

5.7 Decision outcome mappings for BPS DSS

BPS DSS allows to determine a set of suitable DLT platforms from a predefined set based on feature requirements and platform qualities. Table 11 presents relevant mappings between BPS DSS and correlating assessment method categories. In order to use the BPS DSS, feature requirements need to be given weights based on the MoSCoW prioritization method that gives each feature one of the following values of *must-have*, *should-have*, *could-have*, *won't have*. Qualities of DLT platforms are rated as *low*, *average* or *high*. These weights will be used by the BPS DSS to calculate suitable platform alternatives. Following features and qualities are given static values based on their high relevance for SCM use cases as identified in Chapter 3 and Chapter 4. *Smart contracts* and *Turing complete* are prerequisites for developing SCM oriented DApps. *Enterprise system integration* is a prerequisite for connecting DLT with existing SCM systems. *Technology maturity* is assigned the value *high* since it is seen as a barrier for DLT application in SCM [30].

Table 11. Decision outcome mappings for BPS DSS.

BPS DSS feature requirement	**Value**	**Description**
Smart contracts	Must-have	Smart contracts are a prerequisite for SCM DApps. Described in Section 3.1.2
Turing complete	Must-have	Required for implementing custom business logic.
Public	Determined by Network structure	Described in Section 3.1.1
Private	Determined by Network structure	Described in Section 3.1.1
Permissionless	Determined by Permission model	Described in Section 3.3.1
Permissioned	Determined by Permission model	Described in Section 3.3.1
Privacy technologies	Determined by Permission model	Described in Section 3.3.2
Scalability technologies	Determined by Scalability	Described in Section 3.2.2 and Section 3.2.3
Enterprise system integration	Must-have	Determined by top level quality goal of integrable. Described in Section 3.4.1
Cross-chain interoperable	Determined by Interoperability	Described in Section 3.4.2
Transaction speed	Determined by Scalability	Described in Section 3.2
Technology maturity	High	Generic requirement for SCM DApps

5.8 Suitable DLT stacks for SCM DApps

The assessment method allows to identify DLT stack components in an easy-to-use manner by focusing on use case goals to determine a high-level architecture for SCM DApps. The process follows a linear pattern in which decisions are grouped into categories based on technologies identified in Chapter 3. Each category uses decision trees with questions posed in natural language to determine applicable technologies. Based on the possible outcomes of the assessment process, the following generalized DLT stacks were deduced to answer the research question. Private permissioned stacks that cater to use cases in which a consortium of stakeholders requires control over governance, high transaction throughput or data privacy, but can pose challenges for cases where control over governance is not a sought-after feature or where DLT interoperability can be hard to achieve. Public stacks with extended capabilities that strive to achieve levels of performance and privacy similar to private permissioned stacks by combining a highly decentralized public network with scaling and privacy technologies. This approach relies on technologies that increase the complexity of development and on open governance structures that manage over public networks. Public or private stacks for simple storage and verification that use DApps to store hashes of data or unique data points that allow to verify the integrity of off-chain records. This approach tends to have lower requirements for privacy and transaction throughput but can pose challenges if the chosen stack can't be scaled to support more complex use cases. The current solution for determining DLT stack components is limited to technology categories, which makes identifying specific technologies reliant on composability with other methods such as BPS DSS. The assessment method can be improved by further research exploring possibilities for compatibility with other tools and methods.

6 Evaluation

In order to evaluate utility provided by the assessment method, a case study is conducted where it is applied to developing a POC SCM DApp. Additionally, to evaluate usability of the assessment method, a usability study is conducted to gather feedback from domain experts. Section 6.1 presents the case study for a POC DApp. Section 6.2 presents evaluation criteria and results.

6.1 Case study - POC logistics DApp

The scope of the POC is to develop a prototype for a logistics DApp in order to explore the applicability of DLT for small to medium enterprise (SME) supply chain provenance. The use case for the POC is focused on creating a simplified logistics flow in which DLT is used to trace shipments of goods. The long-term goal is to create a logistics platform for food traceability that would allow to form a consortium of logistics operators, food producers and regulators in order to trace the provenance of food products across flows that involve multiple stakeholders. The value propositions provided by the platform are secure data sharing, supply chain provenance and improved process automation. Traceability improves the safety of food products and enables stakeholders to reduce costs that incur due to limited oversight and the overhead of managing segmented supply chain data and processes. Automation of processes enables for a more streamlined data flow across supply chains that rely on collaboration between multiple stakeholders. In order provide a high degree of automation, the DApp needs to be able to support integrations with IOT devices as this can greatly enhance supply chain visibility by providing relevant insights during transportation and storage.

6.1.1 Requirements

The POC DApp is in its initial design limited to the following stakeholders. Company A that is responsible for the production and packaging of food products. Company B that is responsible for the transportation and storage of shipments containing said food products. Both Company A and B need to able to see the history of all the transactions between them, while being able to hide certain transaction details from other stakeholders. This would allow to comply with regulations as well as protect circumstantial agreements between companies from their competitors. Functions that modify the state of the ledger will be role based, meaning that certain operations are only available to stakeholders who have been approved to carry them out. For this reason, participation in the network would require a vetting process in order to establish the identities and roles of different stakeholders. Functions are divided by stakeholders as following, Company A needs to be able register shipments for pickup and Company B to register pickup, transport, intermediate storage, outbound transport and delivery. Transaction data needs to be modelled according to Blockchain in Transport Alliance Standards Council (BiTAS) Tracking Data Framework [73] in order enhance integrability and interoperability between different SCM systems. Since IOT is applicable for this use case, the DLT stack needs to be able to processes sensor data, while implementing IOT integration falls out of the scope for the POC.

6.1.2 Application of the assessment method

In order to identify relevant DLT stack components, the POC DApp requirements are used together with the assessment method and BPS DSS. To facilitate easier use of the assessment method, a support tool has been developed in the form of a web application [74]. The support tool implements the decision algorithm as described in Chapter 5 in a front-end application developed using NuxtJS (v2.0) framework. The code for the application is available in GitHub (https://github.com/ijogi/scm-dlt-stack-assessment-method). By using the POC DApp requirements together with the support tool, the following criteria shown in Table 12 were identified. Based on these criteria, the assessment method identified feature requirements shown in Table 13, qualities shown in Table 14 and peripheral technologies shown in Table 15.

Table 12. Criteria identified by the assessment method.

Decision category	Criteria
Network structure	Control over governance. Restricted access. High throughput, Data privacy.
Permission model	Ledger used as a database. On-chain business logic. Identity based access. Data privacy.
Oracle integrity	Unreliable input data or untrusted data sources. Single sources of data. Identities of external data sources are verifiable.
IOT	Use case involves tangible assets. Conditions of assets affect business processes. Automated process tracking. DLT used to process IOT data. Highly automated.
Scalability	Near real-time data processing or large volumes of data. Use case doesn't involve processing or storing large files.
Interoperability	Use case doesn't involve conflicting requirements. Intersection points with financial, insurance, manufacturing or retail industries.

Table 13. Feature requirements identified by the assessment method.

Must-have	Should-have	Could-have
Private network	Cross-chain interoperable	Privacy technologies
Permissioned	Must-have	Scaling technologies
Smart contracts		
Turing complete		
Enterprise system integration		

Table 14. DLT qualities identified by the assessment method.

Quality	Value
Transaction speed	High
Technology maturity	High

Table 15. Peripheral technologies identified by the assessment method.

Peripheral technologies
Oracle attestation - Cryptographic proofs
Oracle attestation - Reputation system
IOT

6.1.3 POC implementation

According to the combined output from the assessment method and BPS DSS shown on Figure 19, Hyperledger Fabric (HF) is chosen as the base of the DLT stack. The code for the application is available on GitHub (https://github.com/ijogi/scm-dapp). HF is a private permissioned DLT platform developed by The Linux Foundation [47]. The POC DApp is developed using IBM Blockchain Platform Developer Tools (v2.0.2) extension in Visual Studio Code Integrated Development Environment (IDE) (v1.55.2) which allows to develop smart contracts and host them on a local network. The DApp consists of a preconfigured HF network consisting of two organisations, smart contracts developed in TypeScript and client applications developed using NodeJS based NestJS (v.7.6.13) framework. The DApp functionalities are developed based on the use case description and generic functions shown on Figure 9. Data models used for transacting between smart contracts and client applications follow BiTAS Tracking Data Framework [73]. HF enables to develop integrations with centralized systems using NodeJS and Java based SDKs [75] that enable to construct different software architectures capable of connecting to smart contracts. Data privacy is achieved by permissioned access that can be implemented both on the network and smart contract level, with additional capabilities provided for selectively encrypting data stored on peer nodes, making it accessible only to certain parties [76]. HF is a performance-oriented platform that provides pluggable consensus mechanisms [77], [78] that can be changed according to their fit with underlying HF architecture and use case needs. While HF's modular architecture supports different oracle architectures [79], due to simplified nature of the POC DApp, it is not possible to conclude whether oracle attestation method suggested by the assessment method can be successfully implemented. HF achieves DLT interoperability by combining HF with Hyperledger Cactus [80] interoperability tool.

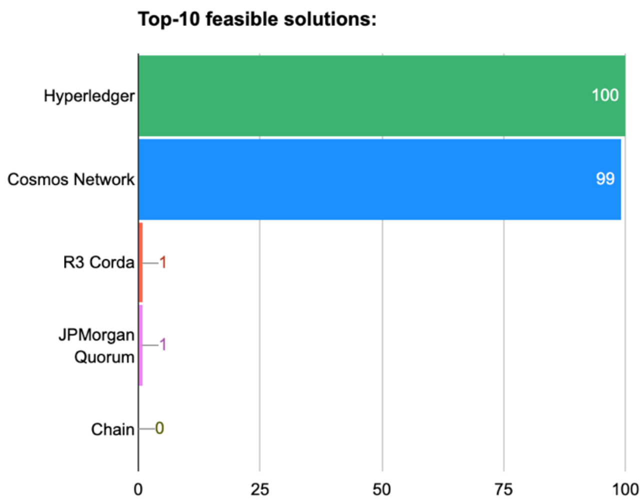

Figure 19. Feasible DLT platforms determined by BPS DSS.

6.2 Artifact evaluation

Based on DSR methodology, artifacts need to be rigorously evaluated in order to determine if they provide qualities that are relevant for their business environments. The assessment method's usefulness is evaluated based on the qualities of utility, usability and composability for use in software development lifecycles pertaining to the design and development of SCM DApps.

6.2.1 Utility

The utility of the assessment method is evaluated based on its ability to successfully identify DLT stacks that support building SCM DApps. The evaluation is constructed in the form of a case study in which the assessment method is used to identify a DLT stack components for implementing a POC SCM DApp. Compared to BPS DSS and DLT platform taxonomies [23], [24], [25] the assessment method focuses on identifying stack components by SCM specific use case requirements rather than identifying DLT platform features that can be matched to said requirements. This allows to use SCM domain expertise in the decision process in order to partially compensate for technical knowledge about DLTs and complimentary technologies. The decision points used in the assessment method are designed through rigorous research into prevalent SCM use cases and technologies as demonstrated in Chapter 3 and Chapter 4. Based on the case study implementation and its analysis, the assessment method was successful in identifying a suitable DLT stack for building the POC DApp in regard to the base DLT platform, while unable to verify the validity of suggested peripheral technologies. The case study also demonstrates that the assessment method allows to approximate DApp requirements to criteria that can be used to navigate key decision points concerning DApp components and to highlight how different decisions can shape the components of a DLT stack. This provides verification for the utility of the assessment method based on the given use case, while further case studies are required to determine whether satisfying outcomes can be achieved with different starting requirements and with more complex use cases.

6.2.2 Usability

Assessment method's usability is evaluated by gathering expert opinions through a feedback form following an exercise in which participants use the web-based application to identify DLT stack components for a SCM use case scenario of their choice. The feedback form asks to rate qualities such as ease-of-use, learnability, usefulness and satisfaction on a scale from 1 to 7, where 1 is the lowest possible score and 7 is the highest possible value. Usability study includes 3 participants shown in Table 16, with expertise in a SCM related field and an understanding of the role of DLT in SCM. Feedback forms for each participant are presented in the appendices as following Appendix 2 and Appendix 3 present the results for participant 1, Appendix 4 and Appendix 5 for participant 2 and Appendix 6 and Appendix 7 for participant 3. Based on the gathered feedback shown in Table 17, ease-of-use, satisfaction and usefulness were rated fairly positively with the average across those qualities being 5.3 out of 7. This indicates that the assessment method is capable of providing value for its intended use with moderately good usability. Learnability was rated on average 2.7 of 7, indicating that effective use of the assessment method requires more supportive and easier to understand materials that explain the concepts and technologies covered in the decision process.

Table 16. Usability evaluation participants.

Participant	**Professional background**
Participant 1	Guardtime, KSI Blockchain company.
Participant 2	DPD Estonia IT Manger, Telia Company distributions logistics software developer.
Participant 3	Experience with first and last mile eCommerce delivery startups in product manager capacity with a strong technical affinity. Some exposure to general supply chain processes of sourcing foreign manufactured electronics for MNCs.

Table 17. Result of the usability evaluation rated from 1 to 7.

	Ease-of-use	Learnability	Satisfaction	Usefulness
Participant 1	5	2	5	5
Participant 2	6	2	5	5
Participant 3	6	4	5	6
Average	5.7	2.7	5	5.3

6.2.3 Composability

Composability measures the ease by which the assessment method can be combined with different tools and methods to facilitate easier design and development of SCM DApps and is evaluated by analysing opportunities for doing so. While the assessment method can be used as a standalone tool, it is designed to be compatible with BPS DSS for the purpose of determining suitable DLT platforms at the core of every DLT stack. Because the assessment method identifies generic features of SCM DApps that determine DLT stack components, it allows BPS DSS to be swapped for any other method that determines DLT stacks or platforms based on prevalent features and qualities. Combining the outcome of the assessment method with BPS DSS allows to identify DLT platforms, but it can't be applied to identifying specific IOT or oracle attestation solutions. This limitation could potentially be overcome by developing tools and methods that are specific to such technology categories. The proposed assessment method provides a base for further research into tools and methods that can be combined in order to bridge the expertise gap in designing domain specific DApps. Composability could be also furthered by improving compatibility between the assessment method and DAOM framework to streamline DApp development. One possibility for doing so would be to use generic DAOM DApp templates that correlate with DLT stacks determined by the assessment method.

7 Conclusion, Limitations and Future Work

The following sections present conclusions drawn from this research, answers to research questions along with limitations and future work. Section 7.1 presents the conclusion. Section 7.2 Provides answers to research questions. Section 7.3 presents limitations and Section 7.4 future work.

7.1 Conclusion

This thesis presents research focused on developing an assessment method for identifying DLT stacks that can be used to design and develop DApps for SCM. The aim of this method is to address a research gap pertaining to the lack of SCM specific methods and tools for doing so. The development of said method helps to overcome a lack of expertise that stems from the novelty of DLT, which is a seen as an obstacle in its wider adoption in the SCM industry [30].

The assessment method sets out to match use case specific requirements with technological components and qualities of a DLT stack. Relevant technologies are identified by establishing a taxonomy of technologies that are organized into categories in the form of concept maps based on research into current literature on the subject of developing SCM specific DApps. Requirements are established by constructing goal models using the DAOM framework, that help to identify generic requirements and qualities of prevalent in SCM use cases.

The established knowledge base is used to design a decision process consisting of technology categories that each contain a decision tree consisting of decision points that help to identify which DLT stack components are relevant for a given SCM use case. Each decision point is posed as a question with additional criteria that help to guide the decision process. Decision outcomes from the assessment method present mappings that enable to use them as input for BPS DSS, that allows to determine DLT platforms by their features and qualities.

In order to determine utility provided by the assessment method, it is evaluated by conducting a case study in which it is used to identify a suitable DLT stack for implementing a POC SCM DApp. The implementation of the DApp is analysed to verify whether the technological components suggested by the assessment method satisfy given requirements. Based on the case study, the assessment method was successful in identifying relevant DLT stack components, while establishing utility for different use cases would require further studies.

Usability of the assessment method is evaluated by conducting a study in which domain experts use the method to determine DLT stacks based on a SCM use case scenario of their choice. The experience is evaluated in a feedback form that rates usability qualities such as ease-of-use, learnability, satisfaction and usefulness. Based on the feedback, the assessment method is capable of providing value in its intended business environment with moderately good usability. Learnability of the method was rated fairly low, indicative that effective use of the assessment method requires more supportive material that explain different concepts and technologies covered in the decision process.

7.2 Research questions

The main research question of **How to identify which DLT stacks support building decentralised applications for SCM** is addressed by providing answers to sub-research questions that together help to answer it.

7.2.1 RQ1: What technologies are relevant for building SCM specific decentralized applications?

Based on the research presented in this thesis, SCM DApps can be built with a variety of technologies such as private and public DLT networks, smart contracts, permission models and consensus mechanisms as well as technologies that can enhance various qualities of existing DLTs such as privacy and scaling technologies. Additionally, since SCM DApps interface with the tangible world of supply chains, they can require integrations and interoperability with various systems such as enterprise systems, IOT and other DLT networks. To secure integrity of data coming from external systems, SCM DApps can make use of oracles and oracle attestation methods as well as identification technologies.

7.2.2 RQ2: What are the generic requirements of SCM specific decentralized applications?

The application of DLT in SCM is strongly influenced by existing business models which require that DApps are able to provide confidentiality, integrity and availability of data with possibilities for authorized access, are capable of handling a large number of simultaneously occurring processes, enable stakeholders to place trust in the stored data and the technology used to manage and govern a DApp, and that DApps can be integrated with existing SCM systems.

7.2.3 RQ3: Which DLT stacks are suitable for use in SCM?

Suitable stacks include private permissioned stacks for use by consortiums that require control over governance, high transaction throughput and data privacy. Public stacks with extended capabilities that provide performance and privacy by combining a public network with scaling and privacy technologies. Public or private stacks for simple storage and verification that use DApps to store hashes of data or unique data points that allow to verify the integrity of off-chain records.

7.2.4 Main research question: How to identify which DLT stacks support building decentralised applications for SCM?

This research found that DLT stacks for SCM DApps can be identified by establishing relevant connections between SCM use cases, technological components of DLT stacks and systematically applying that knowledge to determine which combinations of technologies and qualities fit a given use case. The assessment method built on these principles has proven itself to be an effective tool in reducing some of the complexities involved in the decision process and easing the design and development of SCM DApps.

7.3 Limitations

Limitations of the assessment method stem from a lack of case studies with varied starting requirements that could evaluate the accuracy of results in different conditions. Such case studies should ideally include complex systems with strict requirements that might point out the need for more fine-grained decision options or to validate the present scale of abstraction used to determine a base DLT stack. Usability study showed that effective use of the assessment method requires strong knowledge about the concepts and technologies used in the decision process. This indicates that the method would need to include more explanatory material to provide points of reference that could ease the decision process.

7.4 Future work

The assessment method provides many possibilities for future work. Firstly, by conducting more in-depth studies of if its application in SCM scenarios, relevant data could be captured that can improve both the assessment method and to provide input for developing similar tools and methods. Domain centric methods can potentially simplify the process of designing and developing industry specific POCs and prototypes. Therefor expanding the approach used by the assessment method for other domains could yield positive results, while alternatively the assessment method could be developed into a more generalized enterprise use oriented framework. Future use of the assessment method can be greatly improved by interoperability with other methods and tools. One potential direction discovered through the course of this paper would be to have generalized DAOM DApp templates that correlate with a decision outcome. This approach could improve the design of SCM DApps by highlighting common functions, qualities and interactions between different components and processes of the designed system.

References

[1] https://www.tradelens.com/, “TradeLens,” 2020. [Online]. Available: https://www.tradelens.com/. (Accessed 6 May 2020).

[2] R. Miller, “IBM-Maersk blockchain shipping consortium expands to include other major shipping companies,” Tech Crunch, 28 May 2019. [Online]. Available: https://techcrunch.com/2019/05/28/ibm-maersk-blockchain-shipping-consortium-expands-to-include-other-major-shipping-companies/. (Accessed 6 May 2020).

[3] Nestle, “Nestlé breaks new ground with open blockchain pilot,” 2 July 2019. [Online]. Available: https://www.nestle.com/media/pressreleases/allpressreleases/nestle-open-blockchain-pilot. (Accessed 16 May 2021).

[4] The Linux Foundation, “Case Study: How Walmart brought unprecedented transparency to the food supply chain with Hyperledger Fabric,” [Online]. Available: https://www.hyperledger.org/resources/publications/walmart-case-study. (Accessed 15 May 2021).

[5] University Utrecht, “Decision Model Studio,” [Online]. Available: https://dss-mcdm.com/. (Accessed 16 May 2021).

[6] M. Hulea, O. Rosu, R. Miron and A. Aştilean, “Pharmaceutical cold chain management: Platform based on a distributed ledger,” in *2018 IEEE International Conference on Automation, Quality and Testing, Robotics (AQTR)*, Cluj-Napoca, Romania, 2018.

[7] Q. Lin, H. Wang, X. Pei and J. Wang, “Food Safety Traceability System Based on Blockchain and EPCIS,” *IEEE Access,* pp. 20698 - 20707, 2019.

[8] Y. P. Tsang, K. L. Choy, C. H. Wu, G. T. S. Ho and H. Y. Lam, “Blockchain-Driven IoT for Food Traceability With an Integrated Consensus Mechanism,” *IEEE Access,* pp. 129000 - 129017, 2019.

[9] A. Arena, A. Bianchini, P. Perazzo, C. Vallati and G. Dini, “BRUSCHETTA: An IoT Blockchain-Based Framework for Certifying Extra Virgin Olive Oil Supply Chain,” in *2019 IEEE International Conference on Smart Computing (SMARTCOMP)*, Washington, DC, USA, 2019.

[10] M. P. Caro, M. S. Ali, M. Vecchio and R. Giaffreda, “Blockchain-based traceability in Agri-Food supply chain management: A practical implementation,” in *2018 IoT Vertical and Topical Summit on Agriculture - Tuscany (IOT Tuscany)*, 2018, Tuscany, Italy.

[11] D. Miehle, D. Henze, A. Seitz, A. Luckow and B. Bruegge, “PartChain: A Decentralized Traceability Application for Multi-Tier Supply Chain Networks in the Automotive Industry,” in *2019 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON)*, Newark, CA, USA, 2019.

[12] A. S. S. Arumugam, V. Umashankar, N. C. Narendra, R. Badrinath, A. P. Mujumdar, J. Holler and A. Hernandez, “IOT Enabled Smart Logistics Using Smart Contracts,” in *2018 8th International Conference on Logistics, Informatics and Service Sciences (LISS)*, Toronto, Canada, 2018.

[13] H. Moudoud, S. Cherkaoui and L. Khoukhi, “An IoT Blockchain Architecture Using Oracles and Smart Contracts: the Use-Case of a Food Supply Chain,” in *2019 IEEE 30th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, Istanbul, Turkey, 2019.

[14] M. Kim, B. Hilton, Z. Burks and J. Reyes, “Integrating Blockchain, Smart Contract-Tokens, and IoT to Design a Food Traceability Solution,” in *2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, 2018, Vancouver, Canada.

[15] R. C. Celiz, Y. E. D. L. Cruz and D. M. Sanchez, “Cloud Model for Purchase Management in Health Sector of Peru based on IoT and Blockchain,” in *2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, Vancouver, Canada, 2018.

[16] G. Perboli, S. Musso and M. Rosano, “Blockchain in Logistics and Supply Chain: A Lean Approach for Designing Real-World Use Cases,” *IEEE Access,* vol. 6, pp. 62018 - 62028, 2018.

[17] H. Wu, J. Cao, Y. Yang, C. L. Tung, S. Jiang, B. Tang, Y. Liu, X. Wang and Y. Deng, “Data Management in Supply Chain Using Blockchain: Challenges and a Case Study,” in *2019 28th International Conference on Computer Communication and Networks (ICCCN)*, Valencia, Spain, 2019.

[18] M. Westerkamp, F. Victor and A. Küpper, “Blockchain-Based Supply Chain Traceability: Token Recipes Model Manufacturing Processes,” in *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, Halifax, Canada, 2018.

[19] F. M. Benčić, P. Skočir and I. P. Žarko, “DL-Tags: DLT and Smart Tags for Decentralized, Privacy-Preserving, and Verifiable Supply Chain Management,” *IEEE Access,* vol. 7, pp. 46198 - 46209, 2019.

[20] F. Longo, L. Nicoletti, A. Padovano, G. d'Atri and M. Forte, “Blockchain-enabled supply chain: An experimental study,” *Computers & Industrial Engineering,* vol. 136, pp. 57-69, 2019.

[21] X. Xu, Q. Lu, Y. Liu, L. Zhu, H. Yao and A. V.Vasilakos, “Designing blockchain-based applications a case study for imported product traceability,” *Future Generation Computer Systems,* vol. 92, pp. 399-406, 2019.

[22] J. Hinckeldeyn and K. Jochen, “Developing a Smart Storage Container for a Blockchain-Based Supply Chain Application,” in *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*, Zug, Switzerland , 2018.

[23] P. Tasca and C. J. Tessone, “A Taxonomy of Blockchain Technologies: Principles of Identification and Classification,” *Ledger,* vol. 4, 2019.

[24] S. M.Sarkintudu, H. H. Ibrahim and A. B. Abdwahab, “Taxonomy development of Blockchain platforms: Information systems perspectives,” in *AIP Conference Proceedings 2016:1*, Sintok, Kedah, Malaysia , 2018.

[25] O. Labazova, T. Dehling and A. Sunyaev, “From Hype to Reality: A Taxonomy of Blockchain Applications,” in *Proceedings of the 52nd Hawaii International Conference on System Sciences (HICSS 2019)*, Wailea, Maui, HI, USA, 2018.

[26] J. R. Q. Verkleij, "A Decision Support System for Blockchain Platform Selection," July 2018. [Online]. Available: https://dspace.library.uu.nl/handle/1874/368090. (Accessed 4 May 2021).

[27] Agile Business Consortium Limited, "Chapter 10: MoSCoW Prioritisation," [Online]. Available: https://www.agilebusiness.org/page/ProjectFramework_10_MoSCoWPrioritisation. (Accessed 16 May 2021).

[28] A. R. Hevner, S. T. March, J. Park and S. Ram, "Design Science in Information Systems Research," *MIS Quarterly,* pp. 75-105, 2004.

[29] M. Rauchs, A. Blandin, K. Bear and Stepheen McKeon, "2nd Global Enterprise Blockchain Benchmarking Study," 2019. [Online]. Available: https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/2nd-global-enterprise-blockchain-benchmarking-study/. (Accessed 16 May 2021).

[30] S. Saberi, M. Kouhizadeh and J. Sarkis, "Blockchains and the Supply Chain: Findings from a Broad Study of Practitioners," *IEEE Engineering Management Review,* vol. 47, no. 3, pp. 95-103, 2019.

[31] J. D. Novak and A. J. Cañas, "The Theory Underlying Concept Maps and How to Construct and Use Them," 2008. [Online]. Available: https://cmap.ihmc.us/docs/pdf/TheoryUnderlyingConceptMaps.pdf. (Accessed 11 February 2021).

[32] A. J. Cañas, J. D. Novak and P. Reiska, "How good is my concept map? Am I a good Cmapper?," *Knowledge Management & E-Learning,* vol. 7, no. 1, pp. 6-19, 2015.

[33] C. Udokwu, P. Brandtner, A. Norta, A. Kormiltsyn and R. Matulevičius, "Evaluation of the DAOM Framework and Tool Support for Designing Blockchain Decentralized Applications," December 2020. [Online]. Available: https://www.researchgate.net/publication/346678605_Evaluation_of_the_DAOM_Framework_and_Tool_Support_for_Designing_Blockchain_Decentralized_Applications. (Accessed 1 March 2021).

[34] H. Al-Breiki, M. H. U. Rehman, K. Salah and D. Svetinovic, "Trustworthy Blockchain Oracles: Review, Comparison, and Open Research Challenges," *IEEE Access,* vol. 8, pp. 85675-85685, 2020.

[35] World Economic Forum, "Data Integrity," 2020. [Online]. Available: https://widgets.weforum.org/blockchain-toolkit/data-integrity. (Accessed 8 March 2021).

[36] G. Caldarelli, "Understanding the Blockchain Oracle Problem: A Call for Action," *Information,* vol. 11, no. 11, 202.

[37] S. Zoican, M. Vochin, R. Zoican and D. Galatchi, "Blockchain and Consensus Algorithms in Internet of Things," in *2018 International Symposium on Electronics and Telecommunications (ISETC)*, Timisoara, Romania, 2018.

[38] T. M. Fernández-Caramés and P. Fraga-Lamas, "A Review on Human-Centered IoT-Connected Smart Labels for the Industry 4.0," *IEEE Access,* vol. 6, pp. 25939 - 25957, 2018.

[39] G. Dittmann and J. Jelitto, "Crypto Anchors," IBM Research, [Online]. Available:

https://researcher.watson.ibm.com/researcher/view_group.php?id=9954. (Accessed 10 Janauary 2021).

[40] Ethereum Foundation, "Ethereum Wiki Sharding-FAQ," Ethereum Foundation, [Online]. Available: https://eth.wiki/sharding/Sharding-FAQs. (Accessed 16 May 2021).

[41] Q. Zhou, H. Huang, Z. Zheng and J. Bian, "Solutions to Scalability of Blockchain: A Survey," *IEEE Access,* vol. 8, pp. 16440-16455, 2020.

[42] bitcoincash.org, "bitcoincash.org," bitcoincash.org, 02 01 2021. [Online]. Available: https://www.bitcoincash.org/. (Accessed 16 May 2021).

[43] E. Lombrozo, J. Lau and P. Wuille, "Bitcoin Improvement Proposal 141," 21 12 2015. [Online]. Available: https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki. (Accessed 2 January 2021).

[44] EthHub, "Sharding on Ethereum," HTML5 Up, [Online]. Available: https://docs.ethhub.io/ethereum-roadmap/ethereum-2.0/sharding/. (Accessed 4 February 2021).

[45] The Linux Foundation, "Hyperledger Sawtooth," [Online]. Available: https://www.hyperledger.org/use/sawtooth. (Accessed 17 January 2021).

[46] IOTA Foundation, "IOTA," [Online]. Available: https://www.iota.org/. (Accessed 17 January 2021).

[47] The Linux Foundation, "Hyperledger Fabric," [Online]. Available: https://www.hyperledger.org/use/fabric. (Accessed 17 January 2021).

[48] J. Poon and T. Dryja, "The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments," 14 January 2016. [Online]. Available: https://www.bitcoinlightning.com/wp-content/uploads/2018/03/lightning-network-paper.pdf. (Accessed 17 January 2021).

[49] "Raiden Network," [Online]. Available: https://raiden.network/. (Accessed 17 January 2021).

[50] A. Back, M. Corallo, L. Dashjr, M. Friedenbach, G. Maxwell, A. Miller, A. Poelstra, J. Timón and a. P. Wuille, "Enabling Blockchain Innovations with Pegged Sidechains," 22 October 2014. [Online]. Available: http://kevinriggen.com/files/sidechains.pdf. (Accessed 17 January 2021).

[51] J. Poon and V. Buterin, "Plasma: Scalable Autonomous Smart Contracts," 11 August 2017. [Online]. Available: https://www.plasma.io/plasma-deprecated.pdf. (Accessed 17 January 2021).

[52] "ZK-Rollups," [Online]. Available: https://docs.ethhub.io/ethereum-roadmap/layer-2-scaling/zk-rollups/. (Accessed 17 January 2021).

[53] Tendermint Inc, "Cosmos Network," [Online]. Available: https://cosmos.network/. (Accessed 17 January 2021).

[54] Web3 Foundation, "Polkadot Network," [Online]. Available: https://polkadot.network/. (Accessed 17 January 2021).

[55] Protocol Labs, "IPFS," [Online]. Available: https://ipfs.io/. (Accessed 17 January 2021).

[56] Filecoin, "Filecoin," [Online]. Available: https://filecoin.io/. (Accessed 17 January 2021).

[57] D. Vorick and L. Champine, "Sia: Simple Decentralized Storage," 29 November 2014. [Online]. Available: https://sia.tech/sia.pdf. (Accessed 17 January 2021).

[58] Storj Labs, Inc, “Storj: A Decentralized Cloud Storage Network Framework,” 30 Octorber 2018. [Online]. Available: https://storj.io/storjv3.pdf. (Accessed 17 January 2021).

[59] Ethereum Foundation, “Swarm,” [Online]. Available: https://swarm.ethereum.org/. (Accessed 17 January 2021).

[60] O. Goldreich and Y. Oren, “Definitions and Properties of Zero-Knowledge Proof Systems,” *Journal of Cryptology,* vol. 7, pp. 1-32, 1994.

[61] S. Garg, C. Gentry, S. Halevi, M. Raykova, A. Sahai and B. Waters, “Candidate Indistinguishability Obfuscation and Functional Encryption for all circuits,” 21 July 2013. [Online]. Available: https://eprint.iacr.org/2013/451.pdf. (Accessed 26 January 2021).

[62] I. Bashir, “Scalability and Other Challenges,” in *Mastering Blockchain*, Birmingham , Packt Publishing, 2020, pp. 707-743.

[63] Massachusetts Institute of Technology, “Project Enigma,” [Online]. Available: https://www.media.mit.edu/projects/enigma/overview/. (Accessed 26 January 2021).

[64] C. Gentry, “A Fully Homomorphic Encryption Scheme,” September 2009. [Online]. Available: https://crypto.stanford.edu/craig/craig-thesis.pdf. (Accessed 26 January 2021).

[65] World Economic Forum, “Inclusive Deployment of Blockchain for Supply Chains: Part 6 – A Framework for Blockchain Interoperability,” 2020 April 2020. [Online]. Available: http://www3.weforum.org/docs/WEF_A_Framework_for_Blockchain_Interoperability_2020.pdf. (Accessed 16 May 2021).

[66] Foreverhold Ltd., “Everledger,” [Online]. Available: https://www.everledger.io/. (Accessed 24 February 2021).

[67] Project Provenance Ltd., “Provenance,” [Online]. Available: https://www.provenance.org/. (Accessed 24 February 2021).

[68] CALISTA Supply Chain Orchestration Platform, “CALISTA Supply Chain Orchestration Platform,” [Online]. Available: https://globaletrade.services/blogs/calista-supply-chain-orchestration-platform. (Accessed 24 February 2021).

[69] Wave, “Wave BL,” [Online]. Available: https://wavebl.com/. (Accessed 24 February 2021).

[70] “Skuchain,” [Online]. Available: https://www.skuchain.com/. (Accessed 24 February 2021).

[71] we.trade Innovation DAC | , “we.trade,” [Online]. Available: https://we-trade.com/. (Accessed 24 February 2021).

[72] “Komgo,” [Online]. Available: https://komgo.io/. (Accessed 24 February 2021).

[73] Blockchain in Transport Alliance Standards Council (BiTAS), “BiTAS Tracking Data Framework Profile,” 27 February 2019. [Online]. Available: https://static1.squarespace.com/static/5aa97ac8372b96325bb9ad66/t/5c7e88397817f73e6c60a967/1551796284047/BiTAS+Tracking+Data+Frameowork+Profile+v9_ISTO.pdf. (Accessed 19 April 2021).

[74] I. Jõgi, “SCM DApp Assessment,” 17 April 2021. [Online]. Available: https://scm-dapp-assessment.herokuapp.com/. (Accessed 17 April 2021).

[75] Hyperledger 2020, “Hyperledger Fabric SDKs,” [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/release-2.2/fabric-sdks.html. (Accessed 15 May 2021).

[76] Hyperledger 2020, “Private data,” [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/release-2.2/private-data/private-data.html. (Accessed 20 April 2021).

[77] Hyperledger 2020, “Pluggable Consensus,” [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/release-2.2/whatis.html#pluggable-consensus. (Accessed 20 April 2021).

[78] Hedera, “Getting Started with the Hedera Consensus Service Fabric Plugin,” [Online]. Available: https://docs.hedera.com/guides/resources/tutorials/getting-started-with-the-hedera-consensus-service-fabric-plugin. (Accessed 20 April 2021).

[79] L. Desrosiers and R. Olivieri, “Oracles: Common architectural patterns for Hyperledger Fabric,” 11 March 2019. [Online]. Available: https://developer.ibm.com/technologies/blockchain/articles/oracles-common-architectural-patterns-for-fabric/. (Accessed 20 April 2021).

[80] H. Montgomery, H. Borne-Pons, J. Hamilton, M. Bowman, M. Bowman, S. Fujimoto, T. Takeuchi, T. Kuhrt and R. Belchior, “Hyperledger Cactus Whitepaper,” [Online]. Available: https://github.com/hyperledger/cactus/blob/main/whitepaper/whitepaper.md. (Accessed 20 April 2021).

Appendix 1 – Non-exclusive licence for reproduction and publication of a graduation thesis[1]

I Indrek Jõgi

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis Method for choosing distributed ledger technology in supply chain management, supervised by Alexander Horst Norta
    1.1. to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;
    1.2. to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.
2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.
3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

17.05.2021

1 The non-exclusive licence is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive license shall not be valid for the period.

Appendix 2 – Usability evaluation: participant 1 page 1

Usability evaluation: DLT assessment method for SCM

https://scm-dapp-assessment.herokuapp.com/

Professional background in a supply chain management related field *

Guardtime, KSI Blockchain company. https://guardtime.com/scm/

How would you describe method's ease-of-use? *

	1	2	3	4	5	6	7	
Very difficult	○	○	○	○	◉	○	○	Very easy

How would you describe the learning effort required to effectively use the method? *

	1	2	3	4	5	6	7	
Very difficult	○	◉	○	○	○	○	○	Very easy

How satisfying did you find using the method? *

	1	2	3	4	5	6	7	
Very unsatisfying	○	○	○	○	◉	○	○	Very satisfying

Appendix 3 - Usability evaluation: participant 1 page 2

How would you describe the method's usefulness for designing SCM Dapps? *

	1	2	3	4	5	6	7	
Doesn't provide any value	○	○	○	○	◉	○	○	Very useful

Comments and recommendations

Business users would require customisation depending on their own stack/tech. Customers would need more visualisation or business perspective. Good tool for ealry customer qualification and technical basics mapping.

Appendix 4 - Usability evaluation: participant 2 page 1

Usability evaluation: DLT assessment method for SCM

https://scm-dapp-assessment.herokuapp.com/

Professional background in a supply chain management related field *

DPD Estonia IT Manger, Telia Company distributions logistics software developer

How would you describe method's ease-of-use? *

	1	2	3	4	5	6	7	
Very difficult	○	○	○	○	○	◉	○	Very easy

How would you describe the learning effort required to effectively use the method? *

	1	2	3	4	5	6	7	
Very difficult	○	◉	○	○	○	○	○	Very easy

How satisfying did you find using the method? *

	1	2	3	4	5	6	7	
Very unsatisfying	○	○	○	○	◉	○	○	Very satisfying

Appendix 5 - Usability evaluation: participant 2 page 2

How would you describe the method's usefulness for designing SCM Dapps? *

	1	2	3	4	5	6	7	
Doesn't provide any value	○	○	○	○	◉	○	○	Very useful

Comments and recommendations

For somebody who is new to Distributed Ledger Systems, this decision helper can identify core concept and technologies that would be most beneficial for SCM System developer to learn.

Appendix 6 - Usability evaluation: participant 3 page 1

Usability evaluation: DLT assessment method for SCM

https://scm-dapp-assessment.herokuapp.com/

Professional background in a supply chain management related field *

Experience with first and last mile eCommerce delivery startups in product manager capacity with a strong technical affinity.
Some exposure to general supply chain processes of sourcing foreign manufactured electronics for MNCs.

How would you describe method's ease-of-use? *

	1	2	3	4	5	6	7	
Very difficult	○	○	○	○	○	◉	○	Very easy

How would you describe the learning effort required to effectively use the method? *

	1	2	3	4	5	6	7	
Very difficult	○	○	○	◉	○	○	○	Very easy

How satisfying did you find using the method? *

	1	2	3	4	5	6	7	
Very unsatisfying	○	○	○	○	◉	○	○	Very satisfying

Appendix 7 - Usability evaluation: participant 3 page 2

How would you describe the method's usefulness for designing SCM Dapps? *

	1	2	3	4	5	6	7	
Doesn't provide any value	○	○	○	○	○	◉	○	Very useful

Comments and recommendations

Formatting:
- Suggesting a section at the start explaining who the audience is.
- Adding "read more links" would embellish the content quite nicely for a very low effort (e.g. on first page https://es.wikipedia.org/wiki/Distributed_Ledger_Technology_(DLT))
- Some diagram, especially on the Network Structure page would boost the content a lot, so that the reader develops a mental visual model first. See mockup image.

Content:
- "Does the use case involve conflicting requirements that could be resolved by combining different DLTs?" < This is difficult to answer without having a solution already in mind. At least for me.