Odin Rørvik

Blockchain Technology applied in Aquaculture Supply Chains

Hovedoppgave i Marin Teknikk / Marine Technology
Januar 2022

Hovedoppgave

NTNU
Norges teknisk-naturvitenskapelige universitet

NTNU
Norwegian University of
Science and Technology

Odin Rørvik

Blockchain Technology applied in Aquaculture Supply Chains

Hovedoppgave i Marin Teknikk / Marine Technology
Januar 2022

Norges teknisk-naturvitenskapelige universitet

NTNU
Kunnskap for en bedre verden

Blockchain Technology applied in Aquaculture Supply Chains

Department of Marine Technology

Odin Søreide Rørvik

March 31, 2022

Preface

This master's thesis is written as part of a specialization in Maritime Systems Design and Logistics at the Department of Marine Technology. The work was carried out at the Norwegian University of Science and Technology (NTNU) in Trondheim during the winter of 2021/22. This thesis is a follow-up to a project paper written during the spring semester of 2021. It focuses on the concept of blockchain technology and its potential impact on aquaculture supply chains and how it breaks down functional silos to increase performance. The workload is equivalent to 30,0 ECTS.

I want to thank several people for their guidance and help during the writing of this thesis. Firstly, my supervisor, Professor Bjørn Egil Asbjørnslett, for guidance and productive discussions. I also offer sincere thanks to my contacts at FiiZK, Eivind Brendryen, Håkon Skjelten, Henrik Schultz, and other FiiZK staff in Trondheim. I especially want to thank my roommate for valuable conversations and fun discussions around blockchain technology while writing the thesis.

Lastly, I would like to thank my girlfriend for her tremendous support and my friends and family for the exciting discussions during the report's writing.

Acknowledgment

My supervisor, Professor Bjørn Egil Asbjørnslett, is acknowledged for his continuous input and advice during the preparation and development of the report. Eivind Brendryen, Håkon Skjelten, Henrik Schultz, Alexander Snarli, Marte Myran, Gajaen Chandrasegaram, Erik Osland, and Basile Bonnemarie have provided valuable information during the writing of the master's thesis. Lerøy Seafood, FiiZK Digital, Atea, and Norwegian Seafood Trust, among others, are recognized for their openness as interviewees and for sharing valuable industry insight and discussing the role of blockchain technology. The results of this report would not be possible without their participation.

Abstract

Blockchain technology has gained traction across various industries during the last several years, including supply chains. Blockchain technology can increase efficiency in supply chains by linking previously siloed supply chain systems and supply chain entities, possibly end-to-end. It may also enable supply chains to increase trust, manage transparency, and establish cross-participant process automation and governance. Many pilots and proposals in the supply chain sector draw toward the potential benefits of digital transformation through blockchain.

Since there are no common trust mechanisms, the various supply chain participants' ability to gain analytical insight is severely limited. Hence, cross-boundary data sharing becomes undesirable and results in multiple sources of truths that are subject to manipulation. This creates limitations to the aquaculture industry's common ground in developing technology and techniques that enable sustainable growth. Functional silos must therefore be broken down to enable organizations to connect to their complete supply network to enable end-to-end visibility, collaboration, and improved data-driven decision-making.

This thesis examines the benefits and drawbacks of blockchain in aquaculture supply chains and the criteria for implementing blockchain technology to create a compelling value proposition. Finally, application scenarios for a blockchain-based supply chain management model and a collaborative machine learning paradigm are introduced. The value proposition of this solution for the aquaculture supply chain is supported by arguments in performance, process automation, connection, provenance, authentication, collaboration, and innovation.

The thesis shows that the significant opportunities for value creation is integrating a decentralized blockchain solution in the supply chain. By integrating a decentralized blockchain solution, companies can improve end-to-end visibility and data-driven decision-making.

Sammendrag

Blockchain-teknologi har fått gjennomslag i ulike bransjer i løpet av de siste årene, inkludert forsyningskjeder. Blockchain teknologi kan øke effektiviteten i forsyningskjeder ved å koble sammen forsyningskjedesystemer og forsyningskjedeenheter, muligens ende-til-ende. Det kan også gjøre det mulig for forsyningskjeder å øke tilliten, administrere åpenhet og etablere prosessautomatisering og styring på tvers av deltakere. Mange piloter og forslag i forsyningskjedesektoren trekker mot de potensielle fordelene ved digital transformasjon gjennom blockchain.

Siden det ikke finnes felles tillitsmekanismer, er de ulike leverandørkjededeltakernes mulighet til å oppnå analytisk innsikt sterkt begrenset. Derfor blir grenseoverskridende datadeling uønsket og resulterer i flere kilder til sannheter som er gjenstand for manipulasjon. Dette skaper begrensninger for havbruksnæringens felles grunnlag for utvikling av teknologi og teknikker som muliggjør bærekraftig vekst. Funksjonelle siloer må derfor brytes ned for å gjøre det mulig for organisasjoner å koble seg til sitt komplette forsyningsnettverk for å muliggjøre ende-til-ende-synlighet, samarbeid og forbedret datadrevet beslutningstaking.

Denne oppgaven undersøker fordelene og ulempene med blockchain i akvakulturforsyningskjeder og kriteriene for å implementere blokkjedeteknologi for å skape et overbevisende verdiforslag. Til slutt introduseres applikasjonsscenarier for en blockchain basert forsyningskjedestyringsmodell og et samarbeidende maskinlæringsparadigme. Verdiforslaget til denne løsningen for akvakulturforsyningskjeden støttes av argumenter innen ytelse, prosessautomatisering, tilkobling, herkomst, autentisering, samarbeid og innovasjon.

Oppgaven viser at de betydelige mulighetene for verdiskaping er å integrere en desentralisert blockchain Løsning i forsyningskjeden. Ved å integrere en desentralisert blockchain løsning kan bedrifter forbedre ende-til-ende-synlighet og datadrevet beslutningstaking.

Terminology

Application Programming Interface (API) / A set of clearly defined methods, protocols, and tools for communicating among other various components.

Bill of lading (BOL) / A document issued by a carrier (or their agent) to acknowledge receipt of cargo for shipment.

Blockchain / A structure for storing data in which groups of valid transactions, called blocks, form a chronological chain, where each block is cryptographically linked to the previous one.

Consensus protocol/mechanism / A process, encoded in software, by which computers in a network, called nodes, reach an agreement about a set of data.

Cryptocurrency / A digital asset defined by a blockchain protocol and exchanged via that blockchain system.

Decentralization / A hard-to-quantify measure of a network's resistance to attack, a function of how broadly control is distributed among different actors.

Distributed ledger technology (DLT) / A system, most commonly a blockchain, for creating a shared cryptographically secure database.

Disruptive / A technology or innovation creating a new value network and market replacing an already existing value network and market within the ecosystem.

Double spending problem / Ensuring that a digital asset cannot be copied or used more than once.

Hash function / A cryptography tool that turns any input into a string of characters that serves as a virtually unforgeable digital fingerprint of the data, called a hash.

Internet of Things (IoT) / The network of devices containing software, electronics, connectivity, and actuators allowing these to interconnect and exchange data.

Ledger / An account book in which business transactions are recorded.

Mining / The process by which nodes in Bitcoin, Ethereum, and other blockchain systems add new blocks to their respective chains.

Permissioned blockchain / A shared database with a blockchain structure that requires participants to obtain permission before reading or writing to the chain.

Permissionless blockchain / The same as a permissioned blockchain but where anyone can join the network.

Public blockchain / A blockchain without any access restrictions. Anyone with a computer and internet connection can read and write transactions within the network.

Private blockchain / A blockchain where joining is granted by the administrators within the network. The permission to read and write within the network is restricted.

Proof-of-Work (PoW) / A consensus protocol used in Bitcoin and many other cryptocurrencies. To add a new block, miners must calculate a hash that meets certain narrow criteria. Doing so requires an enormous amount of random guesses, making it a costly process that deters attempts to commit fraud.

Proof-of-Stake (PoS) / A novel consensus protocol in which, instead of mining, nodes can validate and make changes to the blockchain on the basis of their existing economic state.

Scalability / The amount of transactions the network is able to process.

Smart contract / A computer program stored in a blockchain that automatically moves digital assets between accounts if conditions encoded in the program are met. It serves as a way to create a mathematically guaranteed promise between parties.

51% attack / Referring to an attack on a blockchain where a group of miners control more than 50% of the network's computing power.

Nonce / A value used for hash calculation in PoW

Stable-coin / Cryptocurrency where price is pegged to another cryptocurrency, fiat money, or exchange-traded commodity.

Contents

List of Figures

List of Tables

1 Introduction

Imagine this scenario. Two friends decide to create a joint savings account to set off a specific amount to save for an apartment. They decide on a monthly deposit and agree to never withdraw until achieving the desired amount. Despite agreeing to the terms, the two are constantly worried that the other will access it. So, they finally decide to lift the burden of trust and ask the bank to remove the withdrawal option until they return together.

Similar to this scenario, trust is the foundation of the partners' relationship in the aquaculture supply chains. The lack of trust in supply chains limits analytical insight, data-driven decisions, and collaboration between partners. In addition, the present solutions entails weakness such as functional self-interested silos, multiple sources of truths, data reconciliation, conflict resolution costs, and dispute. The recurring cause of these problems stems from companies' challenges with developing competitiveness, innovation, and resilience in the supply chain. However, the key contributor identified is the inability to integrate proper trust mechanisms throughout the supply chain.

1.1 Background

Curiosity and a newfound interest were first discovered upon the first encounter with blockchain technology in 2018. A need to gain a deeper understanding of the magnitude of this technology quickly arose. This led to a decision to partner with a startup company utilizing blockchain in finance. However, the potential of applying blockchain to various industries sparked the idea of further examination within the aquaculture industry. As a marine technology student, theoretical and practical studies have created a deep understanding of the strength and weaknesses of this industry. Thus, due to a strong passion for innovation and a high intrinsic motivation, this topic was selected to uncover how this technology can reduce barriers and foster innovation in aquaculture companies.

1.2 Limitations

Blockchain being a relatively recent innovation, this thesis is subject to certain limitations. Although the technology remains recognized in the finance technology industry and generates significant impact. Blockchain technology has only recently moved into the supply chain industry. Thus, there is a lack of necessary data. In addition, the economic impact of blockchain implementation from a monetary and quantitative perspective is usually kept silent.

1.3 Objectives

The main objective of this thesis is **to provide insight into how blockchain can deliver added value to the Norwegian aquaculture industry.** To achieve this, the following secondary objectives are identified:

1. Get a thorough understanding of Blockchain Technology by conducting a state-of-the-art literature review on the underlying fundamental aspects of the technology, its potential role in business aspects, and its potential alignment with Industry 4.0 applications.

2. Get an understanding of how the Norwegian aquaculture industry and supply chains have evolved.

3. Identify a fundamental problem in the Norwegian aquaculture industry that propagates to multiple problems.

4. Compare two technologies that can potentially solve the problem and decide on one.
    (a) Relate the literature review and industry actors to identify critical features required in the technology.
5. Identify how the technology (blockchain) can be utilized to solve the problem,
    (a) Relate the literature review and industry actors to identify two use cases that can potentially add value to the industry.
6. Investigate and identify specific areas that can add value, save resource efforts, and ensure accountability.

1.4 Thesis Structure

The remainder of this thesis is organized with regard to the objectives above as follows:

Section 2	Objective 1	A thorough literature review of blockchain technology.
Section 3	Objective 2	Examination of the evolution of supply chains and aquaculture supply chains.
Section 4	Objective 3	Problem analysis and statement.
Section 5	Objective 4	Blockchain as a method.
Section 6	Objective 5	Presents two interconnected blockchain-based models that can work simultaneously and independently.
Section 7	All Objectives	Discussion and conclusion.

2 Blockchain Technology

2.1 The emergence of Blockchain

Blockchain was first introduced when Satoshi Nakamoto published the whitepaper *Bitcoin: A Peer-to-Peer Electronic Cash System* in 2008 (Nakamoto, 2008). Since then, blockchain has gained much attention, meaning the technology has been further developed and evolved. Its evolution can typically be divided into three stages, shown in Figure 2.1.

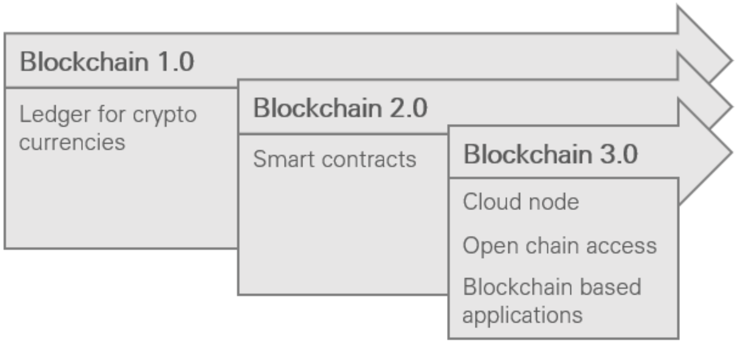


Figure 2.1: Stages of blockchain development

Blockchain 1.0 is the first stage in the development of this technology and consists of the public ledger for holding cryptocurrencies over the distributed network. The blockchain framework handling Bitcoin at this stage aroused great popularity as it solved many issues concerning data, authenticity, security, and integrity using concepts such as hashing and cryptography (Section 2.6). However, the script issued with Bitcoin was considered limited and purpose-built, and innovators subsequently started looking at different applications to blockchain technology. *Blockchain 2.0* was then introduced with *Ethereum* in 2015 and is considered the next stage of the blockchain evolution. This stage includes the trust management feature using smart contracts (Section 2.7), operating itself by disintermediating third parties.

As smart contracts are growing every day, the volume of *micro-transactions* also increases. However, due to scalability issues (Section 2.10.1) in Blockchain 1.0 and 2.0, these technologies are still not sufficient to efficiently assist today's economy in this matter. Hence, *Blockchain 3.0* was introduced. Blockchain 3.0 is the present stage of blockchain technology (as of June 2021) and is still under development. This stage can be considered as the convergence towards decentralized applications (DApp). DApps typically has its backend running on a blockchain network, while the frontend code and user interface (UI) is held in any programming language. The frontend is then able to call the backend for functionality support. This also enables permissioned applications to be built on top of a permissionless network, which will have an important role in Section 6. The Blockchain 3.0 stage includes various application areas such as DeFi (decentralized finance), IoT (internet of things), education, identity management, big data, AI (artificial intelligence), healthcare etc. (Srivastava et al., 2018; Idrees et al., 2021).

A final stage can also be introduced as *Blockchain 4.0*. This stage is not included in the figure as the industry and literature have not yet reached a consensus for what exactly Blockchain 4.0 should be defined as. Blockchain 4.0 is the next-generation blockchain. It aims to operate as an umbrella platform to allow e.g., cross-chain interoperability and communication (Pillai et al., 2020), allowing users from different platforms to work together as one unit. This is necessary in case the technology is to be seamlessly integrated with Industry 4.0 (Bodkhe et al., 2020), businesses, real-world use cases, and applications, such as e.g., supply chain management (SCM).

2.2 Blockchain fundamentals

The development of blockchain technology is still in its initial stages, definitions are still emerging, and no consistent definition has yet been adopted. However, several authors agree that a blockchain should be considered as a *distributed append-only timestamped data structure* (Christidis and Devetsikiotis, 2016; Weking et al., 2020; Du et al., 2019; Yadav and Singh, 2020).

Blockchain is a distributed ledger consisting of interconnected blocks of data protected by cryptographic concepts against tampering (Sanka et al., 2021). Each node participating in the network has its own copy of the blockchain, which is synchronized with other nodes using a peer-to-peer protocol (Group, 2016). Blockchain is immutable, meaning that once the data blocks are added to the blockchain, they cannot be altered or deleted unless most network participants agree upon this.

Figure 2.2 illustrates a simplified structure of the blockchain, the hash chain uses cryptographic encryption to calculate the data blocks linked before and after (Luo et al., 2020). Any data modifications cause the hash of the respective block to change and can then be detected since the new hash is different from the previously stored hash in the next block.

Each block is composed of two parts: a block header and a block body. The block header includes items such as the hash of the previous block, timestamp (block creation time), Merkle root, difficulty, and the nonce. The block data contains all the transaction data within the block. All blocks can be traced back to the *genesis block* (the first block) for verification (Sanka et al., 2021).

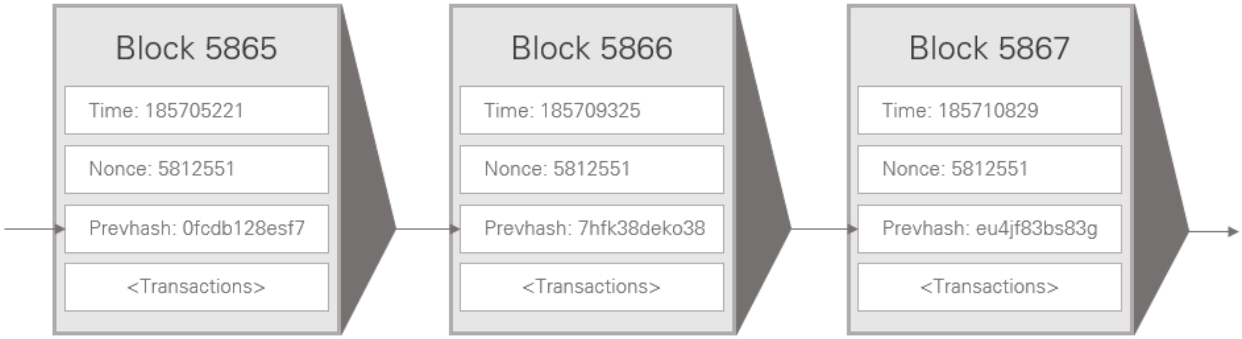


Figure 2.2: Blockchain structure

2.3 The importance of Blockchain

The blockchain has the potential to transform multiple industries and to significantly alter the fields of its application (Reyna et al., 2018). Table 2.1 shows some of the features and benefits which blockchain possesses.

Features	Description	Reference
Distributed	Data stored on the blockchain are replicated across multiple storage devices (nodes), meaning every node holds a copy of the data. This feature prevents data loss, record tampering and double-spending.	Sunyaev (2020)
Data integrity and security	Once data are validated and verified by consensus, block data are immutable, i.e. data is practically infeasible to be erased or altered.	Khan and Salah (2018)
Transparency and traceability	Blockchain records are time-stamped and shared among all participants on the network, meaning all the transactions can be traced.	Gupta (2017)
Decentralized	Blockchain enables disintermediation and may be fully or partly decentralized; Transactions are facilitated by peer-to-peer networks.	Group and Garzik (2016)
Cost saving	Blockchain implementations can reduce transaction costs, currency exchange fees, intermediaries costs, IT-infrastructure costs, cash reserves, payment lead time and cross-border transactions time.	Morkunas et al. (2019); Gregorio (2017)
Efficiency	Based on which consensus algorithm used in the blockchain, it may prove efficient due to disintermediation and allow for autonomous systems.	Mingxiao et al. (2017); Sanka et al. (2021)
Verifiability	Blockchain uses digital signature algorithms in its cryptography. This allows for verification and authentication of a record.	Sanka et al. (2021)

Table 2.1: Blockchain benefits

2.4 Types of blockchain networks

According to Hyperledger (2020) a blockchain network is a technical infrastructure that provides ledger and smart contract (chaincode) services to applications. Due to different utilization and interests in these applications, blockchain is divided into public, private, or consortium networks (Bulterin, 2015). Figure 2.3 represents the three main blockchain networks and their level of decentralization. Note that decentralization in the blockchain is not a binary attribute and should instead be considered as a spectrum.

Public blockchains (the likes of Bitcoin and Ethereum) are permissionless, meaning everyone can join as a new user or node miner and participate in the *consensus process* (explained in Section 2.5) without prior permission. As a substitute for centralized or quasi-centralized trust, public blockchains are secured by *cryptoeconomics* - the use of incentives and cryptographic verification such as proof of work/stake to maintain the network (Stark, 2017). These blockchains are considered fully decentralized, but may be a target to 51% attacks due to the high concentration of mining-power in the hands of few who act in unison to increase profits and network influence (Kotha, 2017; Sanka et al., 2021).

Consortium blockchains (e.g., Hyperledger, EEA), also known as feredated blockchains, are blockchains where the consensus process is controlled by a pre-selected set of nodes (validators). Consortium blockchains are designed for independent organizations, typically of several companies, sharing information with little or no trust. The right to read, do transactions and verify new blocks may be public or restricted to the participants of the network. These blockchains may be considered partially decentralized. Being part of a blockchain consortium network enables participants to securely validate, trust and

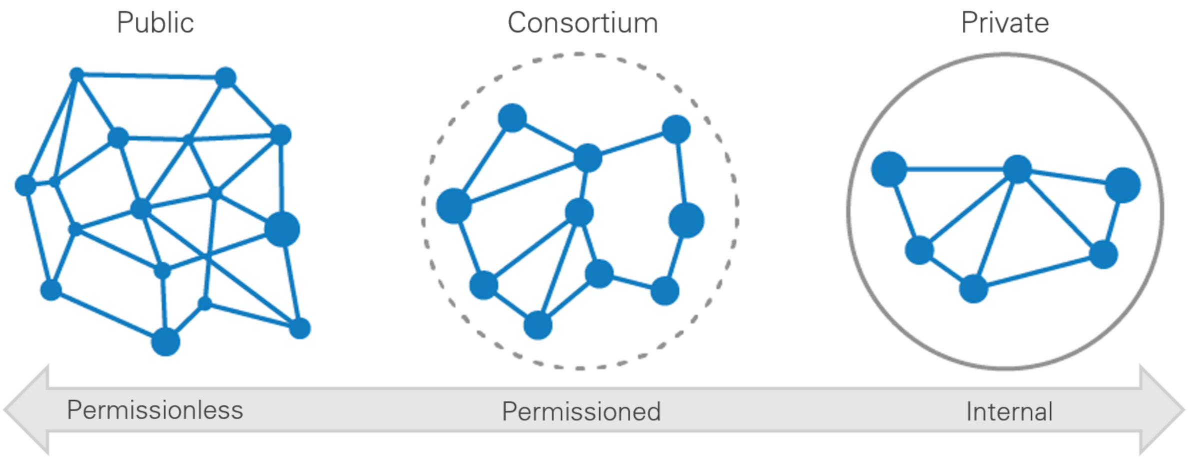


Figure 2.3: Public vs consortium vs private decentralization

share information with each other (Bulterin, 2015).

Private blockchains are blockchains where all *write permissions* are kept centralized within an organization and have strict authority management on data access. All participants are known and may read, write and validate transactions. In other words, a private blockchain resembles a traditional centralized system (database) with some degree of cryptographic auditability attached. However, the nodes of a private chain are not necessarily dependent on a central computer running it, eliminating the single point of error (Demush, n.d.; Bulterin, 2015).

2.5 Consensus in blockchain technology

Consensus mechanisms are central to the functioning of any blockchain or distributed ledger. Essentially, the consensus protocol makes sure that every new update in the blockchain ledger is the only version of the truth that is agreed upon by all the nodes in the blockchain. It allows for authentication and validation of a value or transaction on a blockchain without the need for intermediaries or a central authority (Group, 2016; Seibold and Samman, 2015). Several consensus methods and algorithms are explored, where three of those considered relevant to this literature study will be presented.

Proof-of-Work (PoW) is the backbone concept for the consensus in Bitcoin and other permissionless blockchain networks and cryptocurrencies. PoW is compute-intensive and hence energy demanding, but essential for dealing with the double-spending problem and security of the blockchain (Vranken, 2017). The PoW consensus uses computing power in the form of block *mining*. Each nodes participating in the mining process compete by solving complex mathematical problems to qualify for creating and validating new blocks. The first miner to detect the solution is rewarded with cryptocoins as an incentive. The fraction of the total computational power which is supplied by a node is proportional to the probability of being rewarded. In the Bitcoin network, one block is generated approximately every 10 min on average (due to increasing block *difficulty* and security reasons), which means that a miner with a small fraction of the total mining power is unlikely to be rewarded for a long time. Thus, miners resort to join open mining pools to increase the possibility of gaining a stable income. (Seang and Torre, 2018; Wang, Tang, Lin, Zheng and Chen, 2019). The security of the network also relies on PoW, meaning an attacker is required to solve the same tasks as the rest of the network, which poses an obstacle against

DoS-attacks and *double-spending* (a potential flaw in a digital cash scheme in which the same single digital token can be spent more than once) (Cohan, 2021). When a PoW based network *forks*, and the blockchain diverges into two potential paths forward, every active miner creating blocks on the network must choose which fork to continue to mine on.

Proof-of-Stake (PoS) is another possible consensus implemented in a distributed ledger. PoS require no mining power and selects the creator of a block in a deterministic fashion where the probability to add new blocks and receiving the associated rewards is usually proportional to the validator's ownership stake in the system. The rationale behind PoS is that owners of large stakes are less likely to sabotage the network, as they would suffer the consequences the most (Seang and Torre, 2018; Group, 2016). One of the major criticisms related to the PoS consensus mechanisms is the *nothing-at-stake* problem - meaning a validator can stake its assets on both chains when a network forks, see Figure 2.4, and thereby increasing the chance of double-spending attacks (Martinez, n.d.). However, some may counter-argue this statement due to the traceability of attackers and as they could face a sizeable *stock* cost (Tudón, 2018).

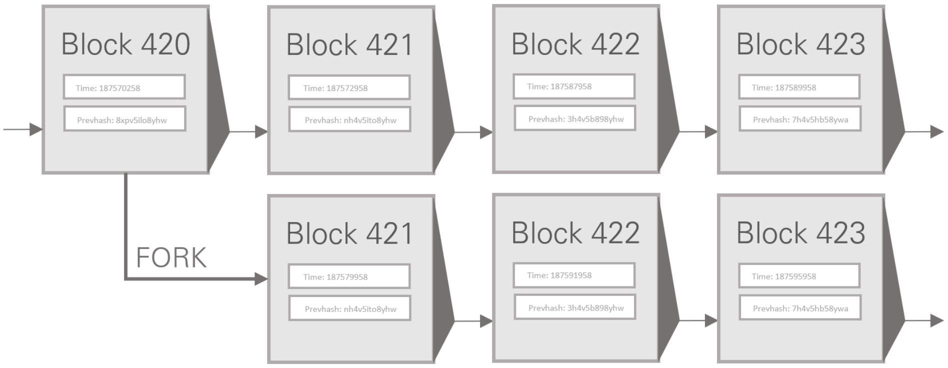


Figure 2.4: Nothing-at-stake problem during a fork: in PoS both paths (chains) can be built simultaneously, whereas in PoW only one path can be mined.

Practical Byzantine Fault Tolerance (PBFT) is a three-phase *voting* consensus protocol typically used in private and consortium networks to provide higher capacity and consistency with restricted access control by exploiting solutions to the *Byzantine Generals' Problems* (Lamport et al., 2019). This is an agreement problem describing the challenges of reaching a peer-to-peer consensus when malicious nodes (traitors) are working to prevent consensus. The PBFT algorithm is resilient, fast, and scalable, and it has been proved that the algorithm can ensure a secure and reliable network to reach consensus, as long as there is no more than $\frac{n-1}{3}$ malicious nodes or faulty replicas out of a total n nodes. Meaning new blocks can only be added if 2/3 of the participating nodes agree. No forks may occur using this consensus protocol; hence new blocks added to the network are absolute. One of the major drawbacks of PBFT is that it scales poorly against the network size due to the O(N^2) message complexity (overhead). The algorithm is therefore not efficient on networks with a high number of nodes. The algorithm also requires all nodes to be adequately identified, certified, and authorized, which makes it most suitable for small, private networks (Zha et al., 2019).

Proof of Autority (PoA) consensus algorithm, often used for enterprise purposes, demands that nodes are authorized and approved before participating in the blockchain. Nodes are given equal opportunities to publish new blocks and earn rewards after approval. As a result, nodes do not have to waste many resources competing with one another. PoA is a highly efficient consensus method in terms of network bandwidth use. Choosing block producers takes less time, leaving greater time for transaction data transmission. As a result, within the limits of the underlying network, the system can have a high throughput, or TPS (”Transactions Per Second”).

Several other consensus protocols exists as well, either combinations and hybrids of the ones above or independent ones, each of them suitable for different uses. Delegated Proof-of-Stake (DPoS), Proof-of-Importance (PoI), Proof of Reputation (PoR), Proof of elapsed time (PoET), Proof of capacity (PoC), Proof of Stake Velocity (PoSV), Ripple and Tendermint, are a few to mention.

2.6 Cryptography behind Blockchain

Blockchain, put simply, is just a combination of existing concepts within cryptography, consensus, and incentive mechanisms. The cryptographic concepts in blockchain include (but are not limited to) hashing operations, digital signatures, Merkle tree, Merkle Patricia trie, and zero-knowledge proofs (Sanka et al., 2021).

2.6.1 Hashing operations in blockchain

In simple terms, hashing is the process of transforming an input string of any length to an output of a fixed length and scrambled hex string. In cryptocurrencies like bitcoin, the transactions can be considered as the input, which is then run through a hashing algorithm, e.g., SHA-256 (Bitcoin) which gives an output of a fixed 256-bit length (see Table 2.2). This is critical when dealing with vast amounts of data and transactions because hashes are ways of encoding files that are much smaller than the actual file itself (Chumbley et al., 2021). For a cryptographic hash function to be considered secure, it must contain six properties described in Table 2.3; deterministic, quick computation, pre-image resistance, avalanche effect, collision-resistant, and puzzle friendly (Rosic, 2020).

Input	Hash
Hi	639EFCD08ABB273B1619E8E7BC29A7DF02C1051B1820E99FC395DCAA3326B8
Welcome	53A53FC9E2A03F9B6E66D84BA70154CDCF5F01FB498C41731881BCDC68A7C8

Table 2.2: Example of secure hashing algorithm (SHA-256)

2.6.2 Merkle tree and Merkle root

The hash of a block is essentially the hash of the block header, which contains the timestamp, nonce, previous block hash, and the root hash of a data structure called the *Merkle tree* storing all transactions in the block. A block in a blockchain may contain thousands of transactions. Merkle trees are devised to encode blockchain data more efficiently and securely and allow nodes of a blockchain network to authenticate, with a unique signature, a specific message or transaction without disclosing the other transactions. In practical terms, this means that these nodes, commonly referred to as *lightweight nodes*, can determine with a strong guarantee of security the status of a transaction while only downloading a small portion (relevant branches) of the entire blockchain (Frankenfield, 2020; Carminati, 2009). Note that lightweight nodes are effectively dependent on the *full nodes* to function.

A Merkle tree is composed of nodes with a large number of leaf nodes at the bottom of the tree

Properties	Description
Deterministic	Same input parsing through the hashing operation will consistently provide same output.
Quick computation	For the system to be efficient, the hash function is required to return the hash of the input quickly.
Pre-image resistance	For a given output hash $H(A)$ it is infeasible to determine the input A. Brute-force technique is the only way to determine the original input. The difficulty of finding a hash increases exponentially with the number of inputs.
Avalanche effect	Any small changes in input will reflect huge difference in the hash value. Connections between hash values should not be possible to detect to determine the input.
Collision resistant	Given two different inputs A and B, where $H(A)$ and $H(B)$ are their hashes, respectively. The chance of the hash values being equal should be infeasible. However, this may happen due to the *Birthday Paradox*.
Puzzle friendly	Represented by the equation $H = k\|x = Y$. It must be infeasible finding an x-value such that the concatenation between a randomly chosen k-value and x is equal to the output hash Y.

Table 2.3: Blockchain features

containing the underlying data, a set of intermediate nodes where each node is the hash of its two children, and finally, a single root node. The root node (Merkle root) is the last hash value of the Merkle tree constructed from the hashes of the transactions in a block, also formed from the hash of its two children. The hashes propagate upwards, meaning any malicious alterations will ultimately lead to a change in the Merkle root and thus the block's hash, causing the protocol to register it as a completely different block. Figure 2.5 shows a simple structure of a Merkle tree. The left-hand side of the figure explains that it is adequate to present only a small number of nodes in a Merkle tree to prove the validity of a branch. The right-hand side introduces how any changes or alterations in the structure will eventually lead to an inconsistency somewhere up the chain (Becker, 2008; Buterin, 2013).

2.6.3 Digital signature in blockchain

Digital signatures are used in blockchain technology to ensure that the transactions are validated (Huynh et al., 2019). A digital signature scheme can be divided into two phases, signing and verification, and is illustrated in the diagram in Figure 2.6; The sender/signer hashes the data and encrypts the hash with their secret key (sk); `sig := sign(pk, transaction)`. The recipient decrypts the encrypted hash with the sender's public key (pk) and verifies (using e.g. a verification algorithm) that the decrypted hash is the same value as hashing the data without any encryption; `isValid := verify(pk, transaction, sig)`.

A digital signature scheme is an adequate approach to authenticate transactions and achieve *non-repudiations* in the blockchain. Non-repudiation is the assurance that someone cannot deny the validity of something, referring to the ability to ensure that a party to a contract or communication must accept the authenticity of their signature on a document or send a message. Fang et al. (2020*b*) discusses the characteristics of blockchain and the digital signature to guarantee information non-repudiation. The paper also classifies, analyses, and investigates typical and state-of-the-art signature schemes in application fields, methods, security, and performance. It is also demonstrated that a combination of

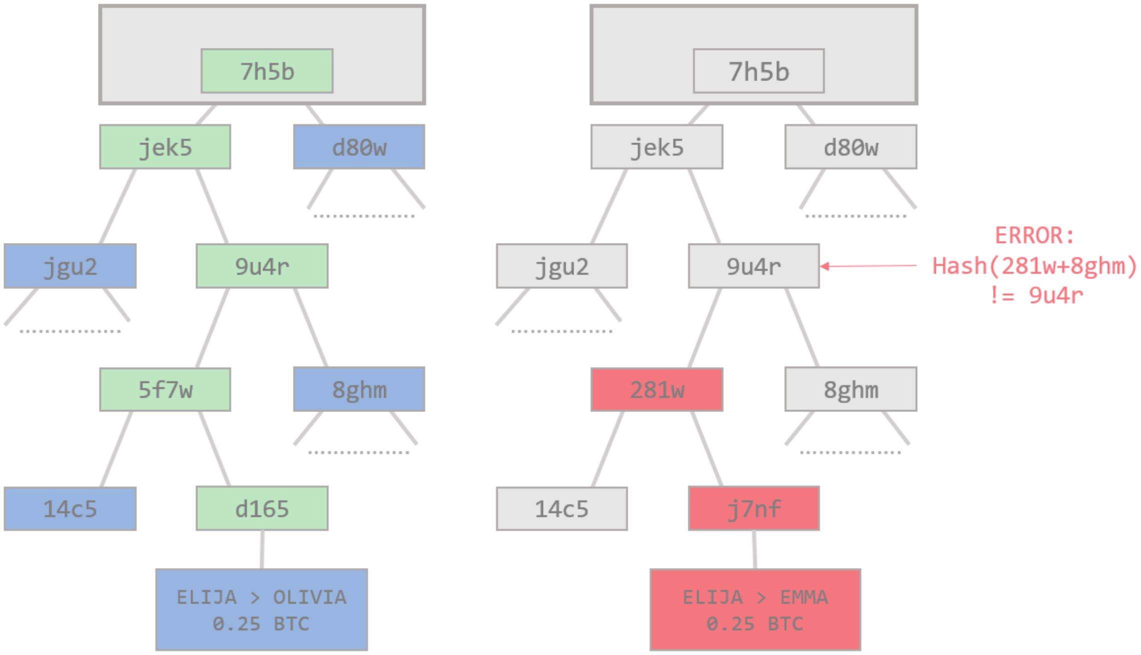


Figure 2.5: Merkle tree

different digital signature schemes can effectively satisfy numerous application properties of blockchains and meet the security requirements in different sectors.

2.7 Smart contracts

Interdisciplinary legal scholar Nick Szabo proposed the concept of *smart contracts* in 1995 (Szabo, 1997). Smart contracts can create collaboration and trust between multiple participants on the blockchain by defining a set of commitments (including contract partakers) in digital form, increasing the breadth of cooperation and depth.

Any shared database application may theoretically be built with a blockchain as its foundation. However, several technological difficulties do not exist in a centralized scenario, such as:

- **Transaction rules.** How can it be verified that participants obey the application's rules if they have direct access to the database? What prevents a single user from manipulating the database's contents for personal gain?
- **Determinism.** These rules will be enforced numerous times by various nodes when processing transactions for their own copy of the database once they have been established. How can we make sure that every node gets the same result?
- **Conflict prevention.** How can two transactions that both obey the application's requirements but disagree with one other without central coordination be dealt with? Conflicts can arise due to unlucky timing or intentional attempts to rig the system.

The main goal of smart contracts (and smart filters and chaincode) is to overcome these problems by collaborating with the blockchain's underlying infrastructure. Smart contracts are the decentralized

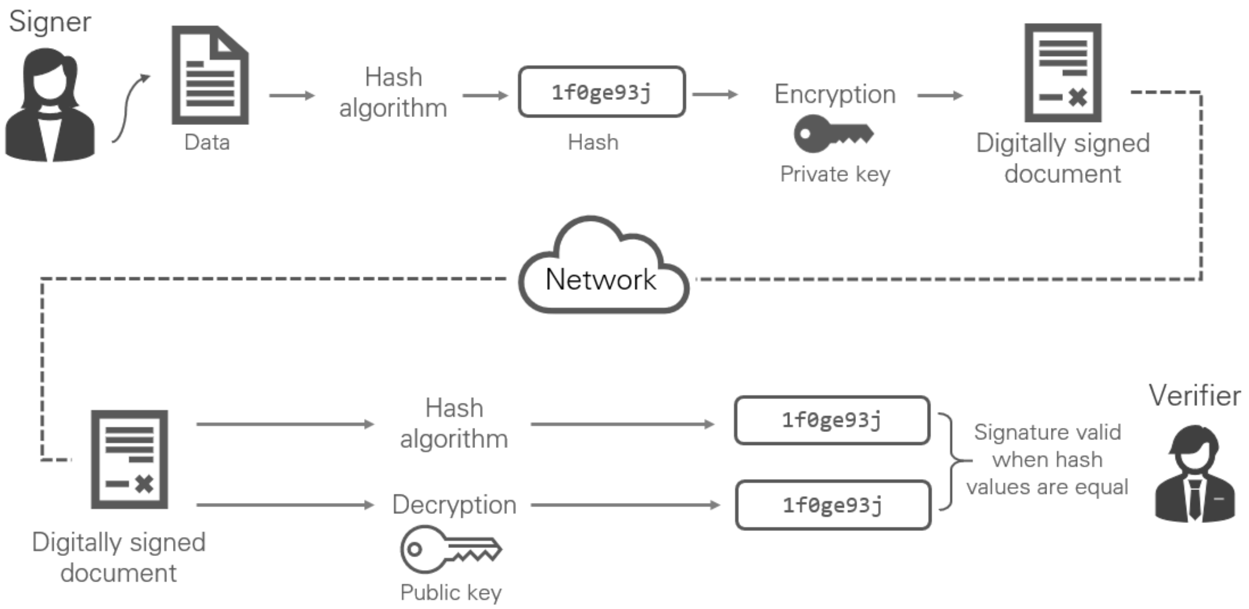


Figure 2.6: Digital signing and verifying scheme (based on Fang et al. (2020*a*))

counterpart of application code; rather than executing in a single location, they execute on several nodes in the blockchain, initiating or verifying transactions that change the database's contents.

Buterin (2013), co-founder of *Ethereum*, defines smart contracts as "systems which automatically move digital assets according to arbitrary pre-specified rules". Smart contracts built on a blockchain allows for mitigation of intermediaries among transacting counterparties, as well as facilitating transactions without malicious alterations and tampering, hence outperforming traditional contracts (Kim and Laskowski, 2016). By removing human judgment from the equation and thus enabling complete process automation, smart contracts allow solving common problems in a way that eliminates the need for trust.

The following three stages can be used to execute smart contracts (Wang et al., 2019).

1 **Develop smart contracts**: Contract participants write the terms of the agreement in programming languages and sign them with private keys.

2 **Integrate with the blockchain system**: Each blockchain node will receive the contract, verify it, and reach a consensus mechanism.

3 **Execution**: The contract agreement will be successfully executed, and contract participants will be notified when the majority of nodes have been verified. The smart contract's operating flow chart is shown in Figure 2.7.

Blockchain paired with smart contracts can realize the verifiability of data, files, and contract records. The user can use the wallet address (owner account) of the deployed contract to *call* the smart contract, or other wallet addresses can call the smart contract if the defined smart contract conditions allow it.

The main idea behind the concept of smart contracts is to allow complex contractual agreements, algorithms, and workflows to be expressed where users are allowed to digitize any physical asset and map real-world logic into the smart contracts, typically by using an expressive (universal) programming

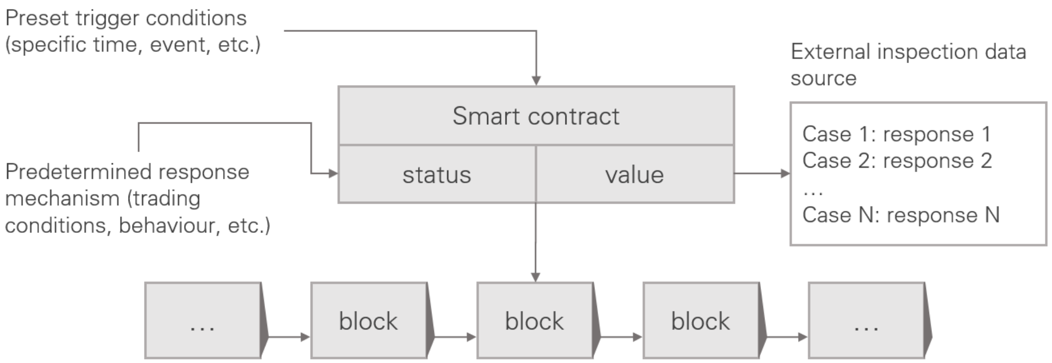

Preset trigger conditions
(specific time, event, etc.)
External inspection data source
Smart contract
status
value
Predetermined response mechanism (trading conditions, behaviour, etc.)
Case 1: response 1
Case 2: response 2
…
Case N: response N
…
block
block
block
…

Figure 2.7: Smart contract operating flow chart (based on Wang et al. (2019))

language (Srivastava et al., 2018).

Smart contracts are best suited to automatically execute two types of transactions: (1) ensuring the payment of funds upon certain triggering events and (2) imposing financial penalties if certain objective conditions are not satisfied (Lipton et al., 2018). Figure 2.8 shows the general way of how a smart contract function.

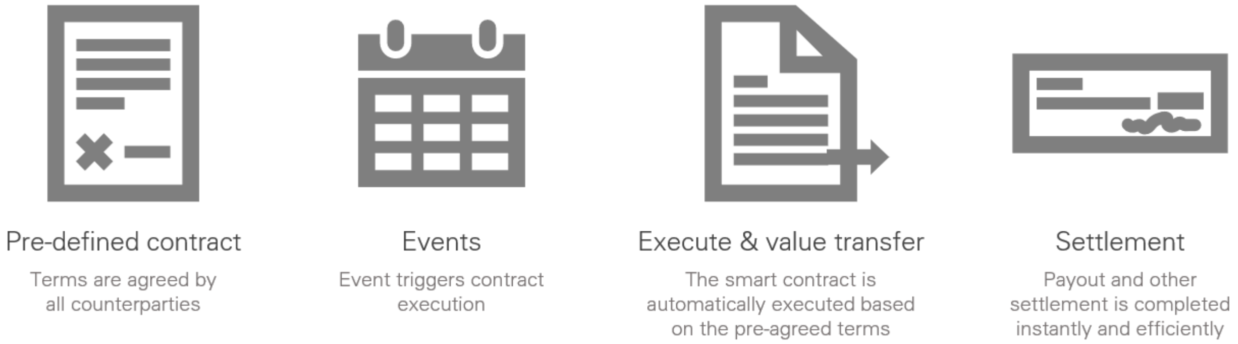

Pre-defined contract
Terms are agreed by all counterparties
Events
Event triggers contract execution
Execute & value transfer
The smart contract is automatically executed based on the pre-agreed terms
Settlement
Payout and other settlement is completed instantly and efficiently

Figure 2.8: Smart contracts

Smart contracts on blockchain-based platforms can have several applications in many different fields. Regulated conditions and agreements can be coded in smart contracts to decrease the likelihood of fraud, theft, and managerial risk. It can also facilitate event-driven mechanisms without interference from single entities and be used for conditioned payment transactions and asset transfers (Chang and Chen, 2020; Dolgui et al., 2020). Besides improving trade efficiency and process automation, this technology enables traditional paper-based procedures to be significantly mitigated while reducing transaction costs and intermediaries. Long-term smart contracts may even hold the assets and encode the bylaws of an entire organization, namely *decentralized autonomous organizations (DAO)* (Buterin, 2013).

Although smart contracts have made massive progress in recent years, they still face many challenges and vulnerabilities concerning transaction-ordering and timestamp dependence, mishandled exceptions, re-entrance, and performance issues (Khan et al., 2021). For example, when running smart contracts on Ethereum accounts or Hyperledger channels, throughput issues can be experienced due to constraints on the blockchain design. This means they are not easily scaled using traditional and proven approaches like *clustering* and *load balancing*. The development of smart contracts, therefore, requires a cross-disciplinary approach, combining technological, economic, and legitimation practices (Yuan et al., 2018).

2.8 Tokenization and Non-Fungible-Tokens (NFTs)

Blockchain is a priority investment for many companies. A recent global blockchain survey executed by Deloitte (Pawczuk et al., 2018) showed that 39% of the respondents reported that their organization intent to invest $5 million or more in blockchain technology. However, most use cases were limited to private and consortium networks with the intention of making record keeping of transactions more efficient. Due to considerations of enterprise requirements (e.g. privacy and scalability), companies limits its scope of blockchain exploration to private and consortium blockchains, meaning they would miss out on a key element with revolutionary potential, specifically *tokenization*.

Note that there is a difference between traditional tokenization and blockchain tokenization. Traditional tokenization revolves around the process of replacing sensitive data with a non-sensitive equivalent. Whereas blockchain tokenization is about creating a digital representation of a wide range of assets deemed valuable by society. Tokenization allows distribution of ownership in both *fungible* and *non-fungible* assets, hence not only unlocking incredible value creation opportunities for enterprises (Laurent et al., 2019), but it may also lead to new sustainable business models which up until this point have been infeasible (Chen, 2018).

Non-fungible-tokens (NFTs) are units of data stored on a blockchain that certifies digital assets or items to be unique and therefore not interchangeable (Dean, 2021). There are plenty of application areas regarding NFT applications ranging from the art-, luxury- and gaming industry to finance and real-estate.

An interesting concept regarding NFTs was issued by Nielsen et al. (2020); exploring the connection between digital twins and blockchain where NFTs act as a determining factor to ensure immutability and traceability for physical objects within a supply chain. By enriching NFTs with data from digital twins, physical events can be transferred to the blockchain network. It will also be possible to create smart contracts based on the conditions which the physical representations experience.

2.9 Micropayments

Micropayments is one of the elements that can be successfully enabled due to tokenization and blockchain technology. A successful micropayment scheme will have the power to create new business models and streamlining existing ones. Some would say it can open up entirely new economies and that it will become the future of online payments. As the name implies, micropayments are small electronic transactions usually less than a dollar, or in some cases only a fraction of a cent (Pass and shelat, 2015). Due to relatively high transaction costs, fees, and overheads in today's systems, payments this size become infeasible. Micali and Rivest (2002) reviews several micropayment schemes that have been suggested over the past few years. However, none have seen an extensive adoption, partly because a trusted party is required to facilitate payments and resolve disputes (Chiesa et al., 2017). Techniques used for bypassing payment processors, by attaching the micropayments to other bills, or using funded wallets outside of banks, are also common practices to avoid dealing with microtransactions. With the appearance of blockchain and cryptocurrencies, the intermediate processing of the transaction is unnecessary, and therefore transaction fees decrease drastically. However, fees are still not consistently competitive with bank fees on the most widely adopted cryptocurrencies (Schneider, 2019). Additionally, small transactions tend to get stuck due to consensus because each block is mined sequentially and due to the fact that miners have the option to prioritize blocks with the highest rewards. Figure 2.9 displays the number and size of the unconfirmed transactions in the Bitcoin network (November 2020 - May 2021), also known as the transactions in the *mempool*. The data is separated into different fee levels in satoshi per bytes, a unit for measuring transaction priority.

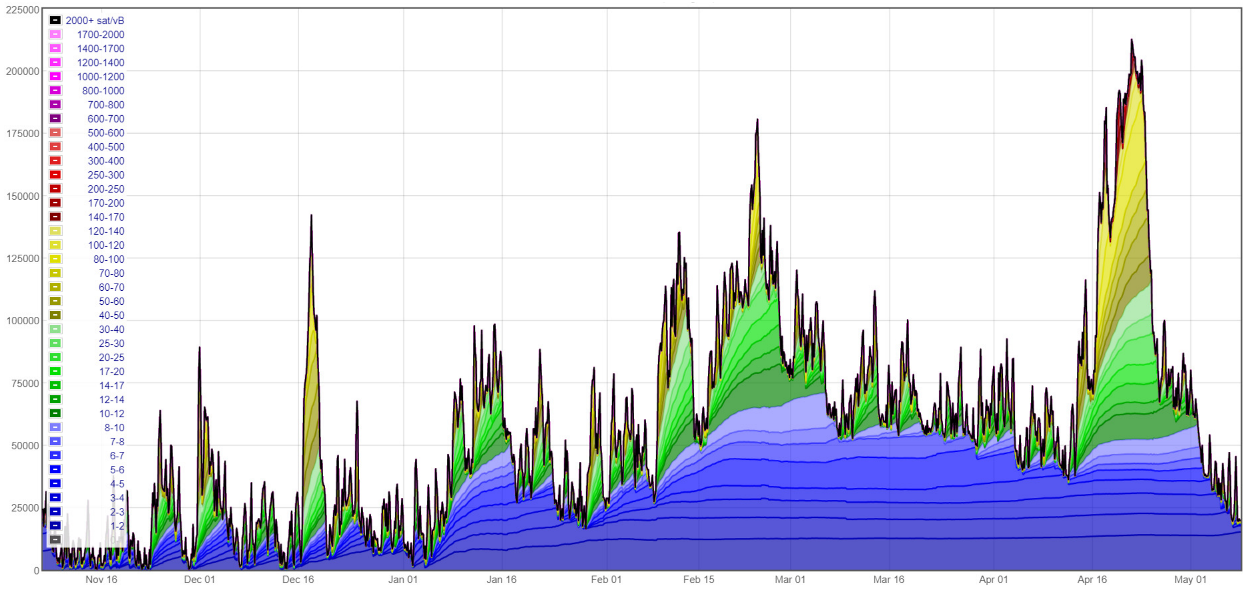


Figure 2.9: Adapted from Hoenicke (2021); The lowest colored stripe is for transactions that pay the lowest fee. Higher fee transactions are stacked on top of it. Since miners prefer high fee transactions, a new block usually only removes the top-most 1 MB worth of transactions from the queue.

Seeing that many permissionless blockchains have a poor ability to *scale*, which may lead to network congestion in cases where large amounts of transactions are pending - many of blockchain's current consensus protocols and system parameters can be ruled out in regards to large scale adoption of microtransactions.

Stable-coins, where the price is pegged to a cryptocurrency, fiat money, or exchange-traded commodity, also has huge potential regarding microtransactions. Assuming stable-coins are managed in good faith and have mechanisms for redeeming the asset(s) backing them, they are considered preferable by many companies implementing blockchain for microtransactions or e.g., settlement architectures (**??**), as the price fluctuation is much smaller compared to other decentralized cryptocurrencies. The prices in stable-coins and governmental coins are unlikely to drop below the underlying asset's value due to arbitrage (Bitstamp and CoinMetrics, 2020). Some stable-coins are; *Tether*, *USD Coin*, *Binance USD* and *Dai*.

2.10 Challenges to be addressed with regards to Blockchain adoption

Despite the strength of blockchain, it still has to overcome some challenges regarding scalability, security, privacy, data retention, compatibility, interoperability, and other psychological barriers.

2.10.1 Technical barriers

Scalability is one of the most discussed problems in blockchain among industry practitioners and academic researchers since the technology was first introduced with Bitcoin in 2008 (Croman et al., 2016; Sanka et al., 2021; Ren and Zhou, 2019). The *scalability trilemma* visualized in Figure 2.10 indicates the difficulty of combining decentralization, scalability and security. With today's technology, one cannot simultaneously exploit each of these properties' full potential. When developing or selecting a blockchain architecture, it must be seen with the value proposition of its application and which tradeoffs to make.

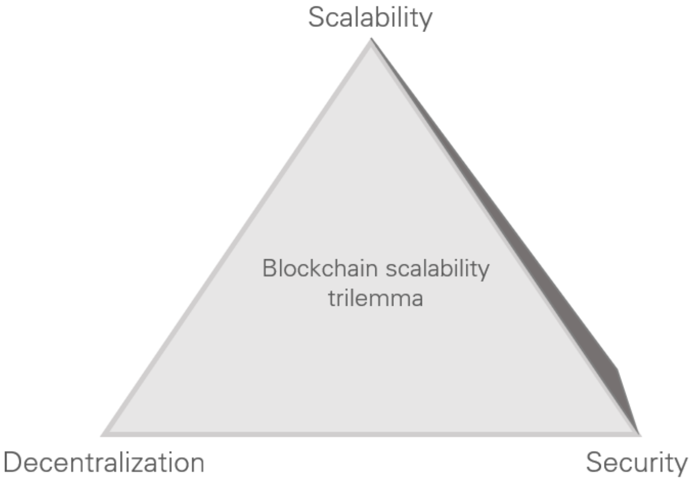


Figure 2.10: Blockchain scalability trilemma (based on Croman et al. (2016))

The scalability for computer systems (e.g., database) often refers to their ability to handle a growing amount of work (or to scale). Whereas in terms of blockchain, the word has a much broader meaning. Croman et al. (2016) analyzed the bottle-necks of Bitcoin and states that any improvements in the perspective of *throughput, transaction confirmation latency, bootstrap time, or cost per transaction (CPT)* can be expressed as "scaling" and the resulting blockchain system scalable. The throughput (tps) of a blockchain is directly influenced by the *block interval* and the *block size*, where a trade-off between the two must be made to get the optimal throughput (Göbel and Krzesinski, 2017). In order for blockchain (e.g., Bitcoin, Ethereum) to compete with non-blockchain counterparts (Visa, PayPal) in terms of throughput, several approaches have been proposed: *segregated witness*, *sharding*, *lightning network* (Poon and Dryja, 2016), *off-/side chains*, *directed acyclic graph* (Bai, 2019), *scale-out blockchains*, *plasma*, economic incentives and alterations to the consensus protocol (Zhou et al., 2020; Wang and Wang, 2019). Ethereum, for instance, is in the process of changing its entire PoW consensus to PoS and sharding (reducing network congestion and increasing transactions per second by creating new chains, known as "shards").

Changes in the consensus may lead to hard forks of the blockchain network, resulting in a new blockchain path (Frankenfield, 2021). Examples of a few noteworthy hard forks which has occurred in the Bitcoin network are; *Bitcoin Cash* forked at block `478558` (1 August 2017), *Bitcoin Gold* forked at block `491407` (24 October 2017), and *Bitcoin SV* which forked at block `556766` from Bitcoin Cash (15 November 2018). Bitcoin SV (Satoshi Vision) was originally designed with a default block size of 128MB but underwent its Quasar Protocol Upgrade in July 2019, known as the *Genesis update*, where the default setting for the maximum block size was removed. (Staff, 2021). As mentioned above, an increased block size will improve the network transaction speeds, drastically increase scalability, and increase the number of transactions per second. This way, distributed and decentralized blockchains can match centralized payment services such as VISA or PayPal in terms of throughput. Blockchains with larger block sizes could therefore be suitable for microtransactions.

Nevertheless, arguments in opposition to increasing the block size and trade-offs have been discussed, e.g., in Bitcoin Magazine (2020) and Sedlmeir et al. (2020). Disagreements in the literature and among industry practitioners due to the technology's immaturity are one of the critical difficulties regarding the implementation of blockchain, as there are many solutions "promising the earth". It is, therefore, logical for companies to wait out the storm until someone else manages the risk and accomplishes a successful implementation before taking action.

Layer-2 solutions (such as *zkRollups* and *optimistic rollups*) on the Ethereum network have also entered the field. Layer 2 refers to technologies that allow an application to scale by processing transactions outside the Ethereum Mainnet (layer 1) while preserving the same security and decentralization as the mainnet. Layer 2 solutions increase throughput (transaction speed) while lowering gas costs. They are at the very beginning stage of development, but they can be an excellent solution contributing to solving the scalability trilemma, especially when combined with Ethereum 2.0.

Another issue is the substantial *blockchain storage size* which is constantly accumulating in decentralized networks. This discourages running full nodes (nodes with a copy of the entire blockchain) and will need to buy more formidable disk space to participate in the network. The blockchain storage size may also affect the read performance, and data retention requests (Casino et al., 2019). This may prove an obstacle to, e.g., IoT devices, as they would need unnecessarily large storage capacity. However, techniques for distribution of lightweight nodes, sharding, or for instance, lightweight blockchain layers can contribute to overcoming this barrier (Na and Park, 2021).

2.10.2 System related barriers

Blockchain is still considered an immature technology; hence there are still concerns regarding the system-related barriers, which include security and privacy barriers, compatibility, and interoperability barriers. Generally, firms are highly resistant to adopting a system that they have no substantial understanding of. However, when users are confident of the technology and risk aspects, they tend to be more open for adoption (Wong et al., 2021).

To use and engage with blockchain effectively, it is necessary to consider the *security and privacy* aspects related to the technology. A blockchain network is only as secure as its infrastructure, and *security* itself can be considered as a measure of how immutable and resistant to attacks the system proves to be. Security and decentralization tend to be interrelated in the sense that one avoids a single point of failure. However, there are several other ways for a blockchain to be attacked, and which pose a risk to decentralized networks. Table 2.4 describes some common attacks that a blockchain may encounter.

In order to defend against such attacks, several solutions have been proposed in literature and industry: *51% attacks*; Two-phase PoW (Eyal and Sirer, 2014), random mining group selection technique (Bae and Lim, 2018), proof-of-activity (Bentov et al., 2014). *Double-spending*; PoW scheme and a distributed timestamping service (Nakamoto, 2008), listening period, inserting observers and forwarding double-spending attempts (Karame et al., 2012). *Selfish mining*; Freshness preferred mechanism (Heilman, 2014), decentralized backward-compatible defense mechanism (Zhang and Preneel, 2017). *Eclipse*

Security attacks	Description
51 %	Once a miner node holds 51 % or more of the mining power in the blockchain network, it can take control the chain. Hence, it can perform several other types of attacks such as double spending, DDoS, and selfish mining.
Double spending	Double spending happens when a dishonest node spend the same coins in in multiple transactions.
Selfish mining	When a dishonest miner node finds a new block and keeps it private, (usually this is broadcasted to the public) to continue mining on this block and thereby increasing its chances detecting new blocks. Honest miners are then forced to spend their computation cycles on blocks that are destined to not be on the public chain. (Nayak et al., 2016)
Eclipse	When a dishonest node controls all the victim's connections from the rest of its peers in the blockchain network, making it possible to filter the victim's transactions or execute other attacks such as selfish mining or/and double spending. (Zhang et al., 2019)
DDoS	A dishonest miner node uses large number of nodes in order to send many requests such as invalid transactions or/and blocks to victim nodes. The purpose of a DDoS attack is to disrupt victim's operations (Huynh et al., 2019).

Table 2.4: Blockchain features

attacks; several comprehensive solutions by Heilman et al. (2015). *DDoS attacks*; proof-of-activity (Bentov et al., 2014).

In a blockchain, as mentioned, all transactions of nodes can be tracked and viewed, meaning the technology itself cannot guarantee transactional privacy. However, some solutions have been proposed to overcome this, to ensure privacy in selected transactions. Kosba et al. (2016) for instance, presented a solution named *Hawk*, which is a blockchain model using cryptographic primitives such as *zero-knowledge proofs* for privacy-preserving smart contracts. Zero-knowledge proof, simply put, is a method where a party can prove to another party that they know a value x, without revealing any information apart from the fact that they know the value x (Zeilberger, 2019).

Other systems-related issues include challenges of interoperability and compatibility of integration. A supply chain, for instance, typically involves multiple stakeholders, and blockchain should therefore not be considered as a stand-alone system (Wong et al., 2021). Interoperability is defined as the ability for blockchains to exchange data between platforms, including off-chain data and transactions—without the aid of third parties.

Due to different characteristics of the various blockchain projects; consensus, hashing, algorithms, transactions, networks, regulatory controls, and governance rules, a series of unconnected blockchain ecosystems, which cannot communicate with each other, has arisen. Muzzy and Anderson (n.d.) stated in a ConsenSys research paper that: "We would be left with a scattered collection of siloed blockchains, each supported by a weak network of nodes and susceptible to attack, manipulation, and centralisation." Developing solutions for interoperability and cross-chain communication can be referred to as Blockchain 4.0 mentioned in Section 2.1. Interoperability is needed in areas that are often in need of multiple networks, each providing specific value and proper communication so that data from, for instance private networks can be routed to other relevant networks for transaction (Meijer, 2020). This way, blockchain may reach its full potential in e.g., supply chains, or other complicated value chains. A comprehensive framework for blockchain interoperability done by WEF and Deloitte suggests that: "this specific challenge is not only a technology problem but also a problem in governance, data ownership, and commercial business models in terms of how they incentivize ecosystem stakeholders to collaborate with each other" (Pawczuk et al., 2020), meaning interoperability is also an organizational problem where the parties in for instance values chains. The different parties are required to synchronize culture, goals, directives, routines, and processes using technology that is compatible. Facilitating an *incentive mechanism* by using smart contracts and microtransactions may therefore be necessary when shifting towards Blockchain 4.0 to utilize the full potential of blockchain technology within value chains. Several reports give an in-depth description of different solutions to interoperability and Blockchain 4.0, as well as projects like ChainLink, Polkadot, Cosmos, Hybrix, and Wanchain are worth mentioning.

2.11 Blockchain in a business perspective

Blockchain might be used to assist businesses to decrease fraud, mistakes, and the expense of paper-intensive operations while also enabling collaboration across numerous entities and enterprises to deliver more efficient and effective services to customers. Companies may deliver new value-added services and upgrade their IT by using Blockchain.

Blockchain allows for decentralized and transactional data exchange across an extensive network of untrustworthy parties. It allows new methods to organize economic activities and new distributed software architectures to agree on a "single source of truth" without relying on a single (and centralized) integration point (Weking et al., 2020; Lo et al., 2017). This can increase efficiency, foster trust, reduce friction, and serve as a foundation for new business models. When opposed to traditional techniques, blockchain offers both advantages and disadvantages as a database and computing platform. Blockchain may be the best option for some use cases, while conventional technology will be the best option for others.

The distinction between permissionless and permissioned networks has important consequences in the supply-chain context (2.4). As seen from Appendix A, blockchain for businesses are generally permissioned (private or consortium) and prioritize; identity over anonymity, selective endorsement over proof-of-work, and assets over cryptocurrency. Nevertheless, each type of blockchain, whether it is private, consortium, or public, could be applied in certain scenarios to gain better advantages and effectiveness. Business runs on information, and the faster it is received and the more accurate it is, the better. With that in mind, IBM states that blockchain is ideal for sharing and delivering that information (Miles, 2017), as it is stored on an immutable ledger that only can be accessed by members granted permission to join the network. It may also prevent the loss of items and records. The information is received much faster due to the fact that central authorities (which may act maliciously) are eliminated from the process (Casino et al., 2019). Another important role by being part of a blockchain consortium is that organizations can share development costs and time with each other rather than each company building its own solutions from scratch. This can lead to shorter development times and economies of scale, allowing smaller organizations to benefit from the same systems as larger ones (Yafimava, 2019).

Gonczol et al. (2020) surveyed in order to assess the applicability and existing applications of blockchains in the supply chain domain, the stage of research, and the maturity of the projects. Here it was revealed that most industries and companies applying the technology regarding the technical details of their systems are kept silent. This is problematic because it impedes the progress of technology. As a result, many companies are hesitant toward blockchains and consider them hype for the elite companies. This is consistent with findings related to psychological behavior adopting new technologies in a survey done by Wong et al. (2021), and is supported by personal communication with supply chain industry leaders.

2.12 Enterprise blockchains

Enterprise blockchains are permissioned blockchains (2.4) and are used to streamline large-scale corporate activities and processes. They are more suited to the demands of businesses than public blockchain networks since the exposure of their data may be restricted to participants of the network only.

Section 2.7 listed a few technological challenges regarding transaction rules, determinism, and conflict prevention. Different blockchains typically address these key challenges in different ways, which means that selecting a platform (enterprise blockchain) for a particular application must begin with a thorough understanding of its trust model, the sorts of transactions it includes, and the expected conflict patterns.

Many blockchain platforms have been developed to match enterprises better. However, a survey done by SHF research ((Gupta et al., 2020)) shows that the two blockchains dominating the market for enterprises are *Hyperledger Fabric* (38%) and *Ethereum* (23%).

The primary difference between Hyperledger and Ethereum is the purpose for which they were created. The Ethereum Virtual Machine (EVM) executes smart contracts for decentralized and mass-consumption applications. In contrast, Hyperledger uses blockchain technology for solely (intra- and inter-) organization purposes and provides pluggable component implementations with high confidentiality, robustness, and scalability levels. Hyperledger also features a modular design that allows businesses to utilize it in various ways. Their key differences are summarized in Table 2.5.

Feature	Ethereum	Hyperledger Fabric
Confidentiality	Public blockchain	Permissioned Blockchain
Purpose	Client-side B2C applications	Enterprise-level B2B applications
Governance	Ethereum Developers	Linux Foundation
Participation	Anyone	Organizations having Certificate of Authorization
Programming Language	Solidity	Golang, JavaScript, or Java
Consensus Mechanism	POW- Proof of Work Mechanism	Pluggable consensus mechanism
Speed of Transactions	More	Less
Cryptocurrency	Ether	None

Table 2.5: Key differentiators: Ethereum vs. Hyperledger Fabric (Veskus and Milani, 2018)

2.13 Alliance of blockchain, big data, and machine learning (ML)

Big data, artificial intelligence (AI), and machine learning (ML) change how large enterprises conduct business and decision-making.

There is, however, a high degree of centralization and proprietary of ML models and large datasets. Predictions from models and ML are often sold on a per-query basis, and published models can quickly become outdated without the effort to acquire more data and re-train them.

There are two primary components to incorporating AI into organizational processes and making a real economic effect: *model* and *data*. Real-world business requirements can be transformed into relevant mathematical AI models for scientific analysis using modeling methodologies. These AI models are trained with data in order for them to generate accurate predictions based on new data (Figure 2.11). While modeling approaches are critical in developing AI systems (Zhou et al., 2014), data is becoming increasingly important in the performance of current data-driven AI solutions.

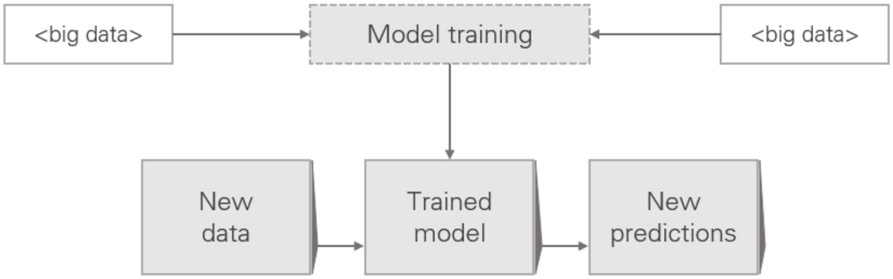


Figure 2.11: Data-driven AI technologies; model training

ML is a subset of AI. ML automates analytical model building. It can identify hidden data insights using approaches from neural networks, statistics, operations research, and physics without explicitly scripting where to seek or what to infer. ML algorithms aim to improve task performance by using examples or experience. ML may, for example, establish efficient data input connections and reconstruct a knowledge methodology. The more data used in this data-driven methodology, the better ML works. This is comparable to how humans improve their performance in a task as they gain more experience (Vieira et al., 2020). The primary outcome of ML is a measure of generalizability, which is the capacity of the ML algorithm to make the correct predictions when new data is provided, based on learned rules from previous exposure to comparable data (Domingos, 2012). More specifically, data involve a set of examples, which a group of characteristics describes, usually called features.

ML systems operate at two processes: learning (used for training) and testing. These characteristics are often combined into a feature vector, which can be binary, numeric, ordinal, or nominal, to aid the former process (Lopez-Arevalo et al., 2020). During the learning phase, this vector is used as an input. In brief, the machine learns to perform the task from experience by relying on training data within the learning phase. It ends once the learning performance is satisfactory (expressed through mathematical and statistical relationships). The model that is developed through the training process can be used to classify, cluster, or predict.

Figure 2.12 depicts an overview of a typical machine learning system. Often, *pre-processing* is necessary to transform the obtained complex raw data into an acceptable state. Pre-processing generally comprises the following:

(a) Data cleaning for removing inconsistent or missing items and noise,

(b) data integration, when many data sources exist, and

(c) data transformation, such as normalization and discretization Anagnostis et al. (2020).

The *extraction feature* seeks to find or create the most informative subset of features, which will then be used to execute the learning model during the training phase (Zheng and Casari, 2018). The feedback loop allows for tweaks to the extraction feature unit and the pre-processing unit, which enhances the learning model's overall performance.

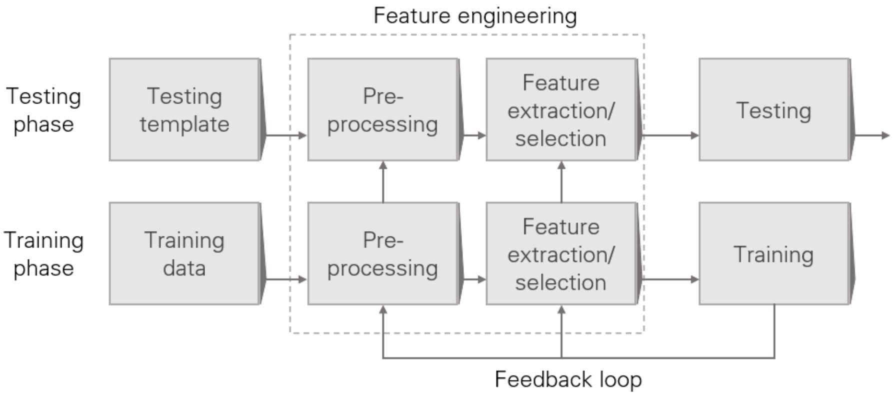


Figure 2.12: A typical machine learning system depicted graphically

According to research (Simeone, 2018; Choi et al., 2020), ML can be categorized into following learning types:

- **Supervised learning:** The input and output are known, and the computer tries to select the optimal route to go from one to the other.
- **Unsupervised learning:** No labels are given; thus, the learning algorithm must construct structure from the data on its own.
- **Semi-supervised learning:** uses a mixture of labeled and unlabeled data as input.
- **Reinforcement learning:** Decisions are made towards finding out actions that can lead to a more positive outcome, while it is solely determined by trial and error method and delayed outcome.

Banko and Brill (2001) investigated the impact of data size on the performance of machine learning models for *natural language disambiguation*. It was discovered that big training data sets considerably improve the performance of various machine learning approaches. The best model with limited data is around x% better than the worst model (e.g., a data size of 10^5), but the performance increases (significantly) when provided big data (e.g., a data size of 10^9), resulting in y% >> x%. Jones and Recchia (2009) also showed that more data outperforms smarter algorithms by comparing *pointwise mutual information* with *latent semantic analysis*.

These studies show that data is essential for organizations to deploy AI/ML technologies to improve their operations. However, because of the necessity to obtain a massive quantity of data and have the adequate processing capacity to handle the data, there are still essential challenges to develop successful data-driven methods. In many cases, these challenges are solved depending on dominant cloud computing providers. However, while commercial cloud vendors might provide valuable data analytics platforms, they can also suffer from a lack of transparency, security, and privacy protection.

Adding blockchain as another data layer to Big Data analytics can ensure the *security* of the data, as it cannot be forged due to the network architecture. It can also provide more *value* due to the structured, abundant, and complete data, making it an ideal source for further analysis.

Mendis et al. (2018) proposed a decentralized and secure computing infrastructure that enables effective and privacy-preserving collaboration between data creators to overcome the challenges of acquiring large datasets while having sufficient computing power to handle the data. Blockchain technology was the foundation of the infrastructure and it could potentially be used to develop a collaborative and cross-organizational market where data creators can secure their data ownership while contributing to machine learning tasks. This makes big data and machine learning/analytics more accessible which benefits all network participants. Figure 2.13 shows how Mendis et al. (2018) improve the distributed machine learning architecture presented in (b) and achieve the decentralized and cooperative machine learning architecture shown in (c).

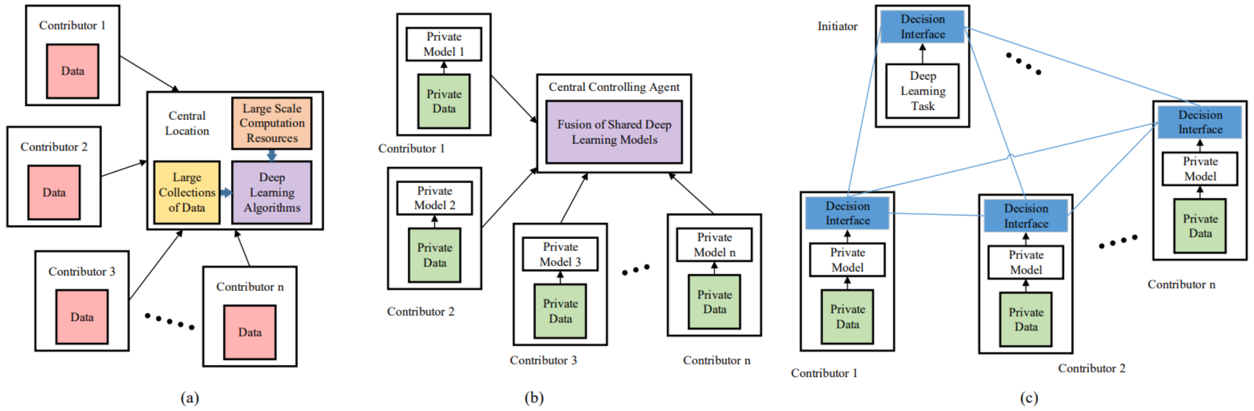


Figure 2.13: (a) Centralized machine learning architecture where data are collected to a centralized server with high processing and storage capability; (b) Distributed machine learning architecture where partial of training is distributed to the data contributors and the training process is fully controlled by a central controlling agent; (c) Autonomous cooperative and decentralized machine learning architecture with no central agents facilitated by blockchain service infrastructure. (Adapted from Mendis et al. (2018))

2.14 Alliance of Blockchain and IoT

As seen in Figure 2.14 (a), the most basic IoT design is a three-layer architecture: the perception, network, and application layers.

(i) The perception layer is the physical layer, which includes sensors for perceiving and acquiring data about the surroundings. It detects certain physical factors or recognizes other smart objects in the vicinity.

(ii) The network layer is responsible for connecting to other smart things, network devices, and servers. Its capabilities are also utilized in the transmission and processing of sensor data.

(iii) The application layer is in charge of providing the user with application-specific services (Sethi and Sarangi, 2017).

The blockchain layer, shown in Figure 2.14 (b), uses the technological characteristics of the blockchain to efficiently handle the challenges of big data management, trust, security, and privacy that have plagued the IoT's growth. This layered architecture enables scalable device coordination, developing an efficient, trustworthy, secure distributed IoT network, and deploying a massive network of devices by providing trust, ownership records, transparency, and communication support for the IoT (Qiu et al., 2018). Data-intensive applications can protect user privacy, and businesses can share and access IoT data without central control and management.

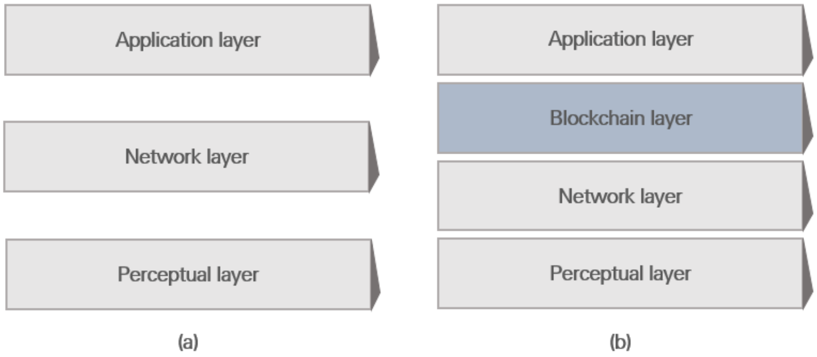


Figure 2.14: (a) Architecture of IoT, (b) architecture of blockchain and IoT fusion model

2.15 Off-chain data and storage

Any non-transactional data that is too large or costly to store efficiently on the blockchain or requires the ability to be updated or deleted is considered *off-chain* data. This includes docs, jpegs, pdfs, sizeable text documents, et cetera. A blockchain is not a silo application in which, for example, business A only sees data from business A. The data must be exchanged among all blockchain nodes to be on the blockchain or referenced by the blockchain. Therefore, sensitive data should be stored off-chain so that it can be deleted if need be (IBMCorp, 2018).

2.16 Blockchain in supply chains

Blockchain emerged as a leading technology layer for financial applications. However, in recent years, the attention has shifted to include applying this technology in other domains. Blockchain used in the supply chain is one of the topics widely discussed in the literature and is believed to deliver real return on investment shortly after implementation. (Esmaeilian et al., 2020; Sunny et al., 2020; Chang et al., 2019; Reyna et al., 2018). Due to blockchain technology's innate distributed and immutable features, the adoption of blockchains in supply chains can be considered one of the most promising recent applications to generate real value motivation for corporations. In many ways, the appearance of blockchain has been viewed as a game-changer for the supply chain sector. In principle, blockchain may benefit the supply chain sector in terms of efficiency, automation, connection, decision-making, and innovation. Consequently, this application area has recently begun to move into the startup world, gaining interest among industry practitioners and venture capitalists across the supply chain sector. A sample of 40 different blockchain companies targeting supply chain improvement is found in Appendix A. Information from each is retrieved to understand how they direct blockchain technology towards different use cases in a supply-chain context. A general description of the company profile, area of focus, industry segment, access rights, choice of platform, and project status was examined. The supply chain pain points addressed in startups are mainly about provenance counterfeits, track and trace, compliance, and data transparency.

By implementing this technology, a preferred foundation of trust and the benefits arising from disintermediation can be utilized. Accordingly, blockchain can be used to record and track transactions and assets. This enhances the transparency and verification of information, payments, and process flow, hence providing timely tracking of products and services (Perboli et al., 2018; Dutta et al., 2020). Implementing blockchain also provides various opportunities to alter underlying business models to increase system efficiency, corporate performance, and monitoring capabilities (Weking et al., 2020).

However, there has been little indication that these startups have gone into mass production (Appendix A). Blockchain must be able to scale and perform in extensive networks of entities or nodes to be valuable in supply chains. It must respect privacy, and the manner businesses transact. To prevent significant disruption and cost, it must also allow light integration or incremental development with current systems (source: personal communication with FiiZK Digital managers).

3 Norwegian aquaculture industry and supply chain overview

3.1 Industry evolution and overview

Norway has a unique position for the production of farmed salmon with natural advantages such as deep fjords, satisfactory current conditions, and oxygen-rich water with a favorable temperature. From the 1970s until today, the industry has undergone significant development where production and value creation have multiplied. In addition, production and value creation have increased, and significant technological and regulatory changes have occurred. As a result, the industry has become a relatively large industry in the Norwegian economy in a short time. Norway is now the world's second-largest exporter of fishery commodities (measured in USD) and tops the ranking of countries with the highest per capita production and exports.

Most aquaculture companies in Norway are small and medium-sized companies that play an essential role in the local communities in which they operate. They contribute to both jobs and value creation along the entire Norwegian coast. Nevertheless, they are becoming fewer and fewer.

In 1991, the restrictions on ownership were relaxed, and the majority interest requirements to have local connections were abolished. The regulatory easing was followed by an industry consolidation with fewer and larger companies through acquisitions and mergers. Since then, there have also been greater opportunities to collect multiple permits at the same site, leading to larger sites.

The markets for Norwegian salmon were again hit by a sharp decline in the early 2000s, with new bankruptcies and financial problems in many companies, which triggered significant structural changes.

The period from 2005 has been marked by significant changes in terms of regulations, technology, and biological and health status. In 2005, the maximum permitted biomass (MTB) was introduced as a production regulation to replace feed quotas as a regulation tool. This changed the way operations were organized and gave the industry a significantly expanded production capacity.

The aquaculture industry has gone from having many small owners to becoming one of Norway's most important export industries that delivers products to a global market. Today, both the ownership and the company structure in the industry are significantly more concentrated. In current times, several aquaculture companies have been listed on the Norwegian stock exchange and thereby gained broad ownership by both Norwegian and international investors. Most of the 100 Norwegian fish farming companies are companies with Norwegian majority ownership and few main shareholders. About 50 percent of the production capacity is currently owned by four companies, which are dominated by four ownership environments. In comparison, the ten largest fish farming companies in 1990 accounted for about 8 percent of total production (Regjeringen, 2019).

The Norwegian salmon industry is at the top globally in terms of technology, digitization, research, and regulations. Norway is home to the world's largest salmon farming enterprises and the most advanced players in technology solutions. In addition, Norway offers the best and most available biological data collections on mortality, illnesses, treatments, and development. Value creation in Norwegian aquaculture has almost doubled between 2013 and 2020, despite stagnating production volumes. Most of the increased value creation directly results from increased sales prices (which also doubled) and profitability (Tveterås et al., 2019).

Norway's position as the main competency and innovation hub for the salmon industry is a result of the salmon farming sector's historical and influential presence along the coast. Knowledge development and innovation occur in collaboration between aquaculture companies, suppliers, and research environments. Norwegian salmon has the greatest EBIT per kg of any other farmed seafood species, which has created the path for further expenditures in technology, innovation, and skill.

The industry has a great chance to maintain its position as the leading knowledge cluster, allowing future growth to be supported by the innovation benefits that clusters often give. However, it will not occur on its own. Instead, it will necessitate continuing investments in research and development, data gathering and analysis, cooperation across and within value chain segments, and a regulatory framework that balances rigorous standards with a proactive desire to focus on possibilities (EY, 2019).

3.2 Evolution of supply chain management (SCM)

Supply Chain Management (SCM) is essential for every business entity. It includes procurement, warehousing, inventory control, production, distribution, order fulfillment, planning, design, implementation, and control of a company's logistics activities.

The never-ending cycle of growing supply chain expenses affects every entities' bottom line, and cost reduction is crucial for competitiveness. Consequently, producers, retailers, and distributors have acknowledged supply chain cost reduction as a key concern. Furthermore, adequate supply chain performance offers strategic value that may lead to reduced financial payback period, increased productivity and profitability, and significant gains in global competitive advantage (Attaran, 2012).

Supply chains evolve and change in size, shape, and configuration and how they are coordinated, controlled and managed. An increasing degree of integration of formerly fragmented tasks marks the evolution of supply chain management (Figure 3.1) (MacCarthy et al., 2016):

The traditional supply chain is a network of enterprises collaborating to create and deliver goods and services. Various SCM tasks, including transportation, storage, and procurement, were fragmented in the 1960s. Since then, traditional supply networks have made considerable development. Companies and supply chain professionals have integrated several supply chain operations and implemented numerous changes that have increased organizational agility and productivity. They shortened the number of suppliers, implemented information systems to track the flow of products and services, and improved and consolidated procurement procedures (Attaran, 2020). This course continued further into the mid-90s when globalization encouraged functional integration and the emergence of logistics in the true sense where all the supply chain elements became part of a single management perspective.

Since the turn of the millennium, modern information and communication technology has taken the stage, resulting in complete integration. Integrated management and control of information, finances, and goods flows created a new range of production and distribution systems. The focus of the supply chain management function shifted to advanced planning processes such as analytical demand planning, which ensures integrated operations from customers to suppliers.

3.3 The increasing web of interactions in a modern supply chains

Due to expansion, globalization, and the rising need for sustainable practices, modern supply chains have been evolving into containing more connected, dynamic, and demand-driven interactions (see Figure 3.2). Commercial processes are carried out through global ecosystems of suppliers and collaborators and advance toward more outsourcing of manufacturers and suppliers.

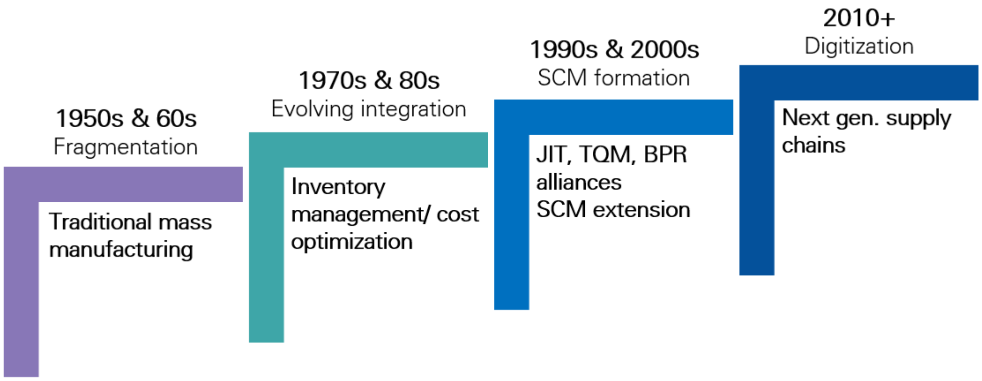


Figure 3.1: SCM evolution (based on (MacCarthy et al., 2016))

Supply chains are also becoming more agile, adaptable, and resilient, allowing faster and more flexible responses to changing customer requirements, and aquaculture supply chains are no exception. The number of actors in today's supply chains is increasing, and they interact in more interdependent and frequently indirect ways (IBM, 2010). New and more flexible alternatives have developed as the age of the vertically integrated business has faded (Bitran et al., 2006), and new connectedness, cooperation, and co-creation are directly enabled by continuous innovation and the worldwide diffusion of new technology and tools across numerous enterprises. However, today's supply chain systems' centralized operation and indivisible systems have changed relatively slowly. The majority of today's supply chains are controlled by centralized monolithic ERP systems that focus on internal operations with the sole goal of supporting that business. Although these systems have been in use for the past 20 years, they carry high capital costs and lack flexibility to changes. Changes to centralized ERP systems may require the use of outsourced developers or consultants. It is also tough to innovate with these systems to use emerging smart technologies like IoT, Industry 4.0, machine learning, and artificial intelligence. Business efficiency decreases because potentially critical interactions are not directly monitored, making cooperation and real-time solutions impossible (Shorthouse and Xie, 2020). As a result, the supply chain network becomes harder to manage, becoming more expensive to maintain, more challenging to monitor and control, less efficient, and vulnerable to disruption, fraud, and diversion.

Note that these value webs can be very successful when adequately engaged, including cost reduction, improved service levels, reduced interruption risks, and feedback-driven learning and innovation. This trend will intensify as new technologies create more data, give greater transparency, and enable increased interaction with even the tiniest suppliers and partners. The transition may provide new obstacles, but it also presents an incredible potential for innovative and strategic developments in creating the future of business (Kelly and Marchese, 2015).

The symbolic logic of the word "chain" depicts perfectly a sequence of distinct linkages through which items are purchased, have value added to them, and then sold to the next value-adder—until an end buyer consumes them. However, value is increasingly being produced not only within organizations but also in the many interactions and connections that exist between them. More iterative and innovation-oriented cooperation is increasingly supplementing linear procurement sequences.

"Companies don't compete - supply chains do" (Taylor, 2011)

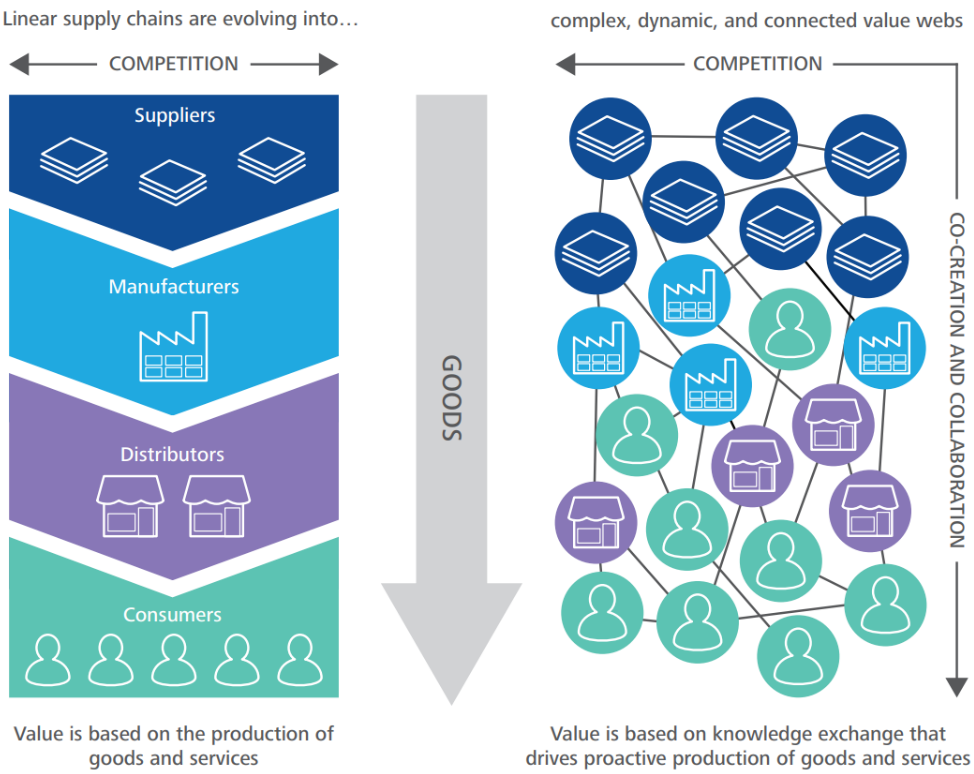

Linear supply chains are evolving into…
COMPETITION
Suppliers
Manufacturers
Distributors
Consumers
GOODS
complex, dynamic, and connected value webs
COMPETITION
CO-CREATION AND COLLABORATION
Value is based on the production of goods and services
Value is based on knowledge exchange that drives proactive production of goods and services

Figure 3.2: Supply chains evolve into value webs. Source: Deloitte Analysis

Supply chains are interconnected and integrated by processes. The central aspect accompanying integration in the supply chain is information sharing. Information sharing is evidence of trust and wiliness for further cooperation and is the basis for achieving a common competitive advantage for all cooperating business partners. The quicker response to the demand, the higher the competitive advantage of the supply chain (Nowicka, 2018).

3.4 Aquaculture supply chain overview

Like the general global supply chain, the aquaculture production cycle and supply chain consists of many parts, participants, and stakeholders. The main supply chain processes that are considered relevant for this study are briefly presented in this section and can be viewed in Figure 3.3 starting with broodstock selection and then following the supply chain all the way to the consumers.

Broodstock initially undergoes different selection processes (e.g., family and individual selections) before the final selected are allowed to produce eggs for the farmers. The selection process is based on information from numerous measured traits, in which the growth feature is most emphasized. In some cases, after the topmost broodstock candidates are selected, DNA samples are performed to search for genetic markers such as *quantitative trait locus* (QTLs). AquaGen (2021) name this *double selection* as broodstock undergoes selection twice by two methods that complement and reinforce each other.

When the broodstock selection is finalized, the hatchery process may begin. This is the process of covering fertilized eggs all the way until they are prepared to be released into the seawater. The process

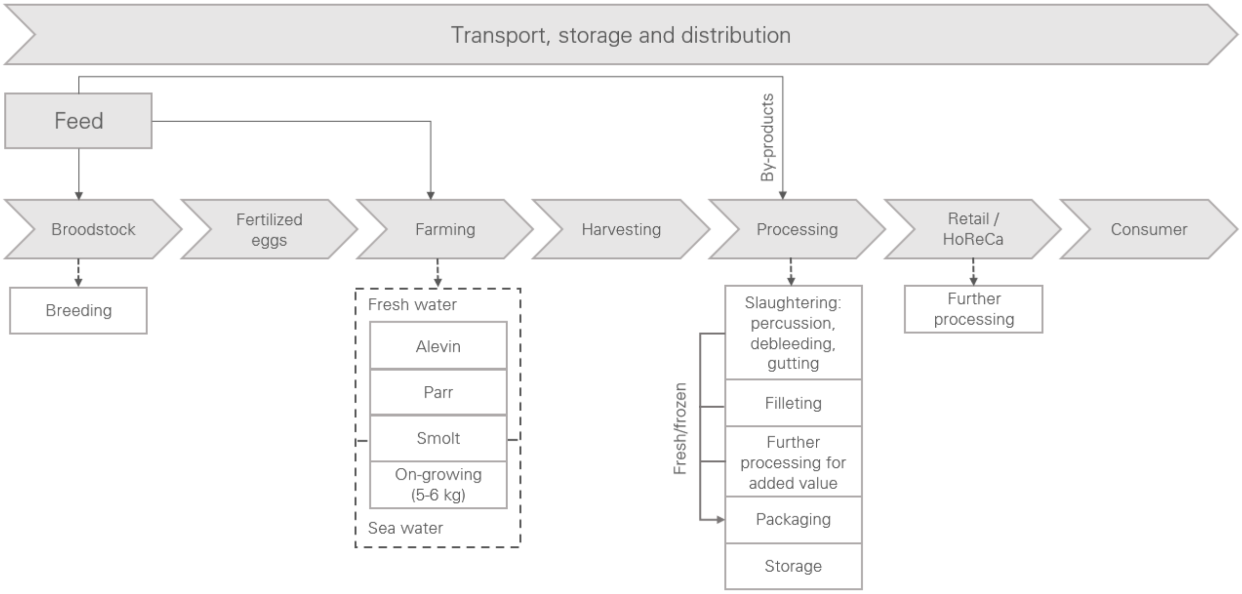


Figure 3.3: Aquaculture supply chain (adapted from Marvin et al. (2020))

includes; collecting and fertilizing eggs, fertility sampling, incubating the eggs, otolith marking, feeding, smoltification, and returning adults. After the smoltification process, the fish is transported by wellboats to the production site, where they spend time growing until ready to be harvested (FAO, n.d.; PWSAC, 2020).

After 12-24 months, when the salmon weighs about 4-6 kilos, it is harvested (Mowi, 2020). The salmon is then transported by wellboats to a processing facility where it is slaughtered, filleted, packed, and stored. It is then transported at a cooling temperature through a cold chain until it reaches retail or *HoReCa* and consumers. A simple cold chain scenario is presented in Figure 3.4.

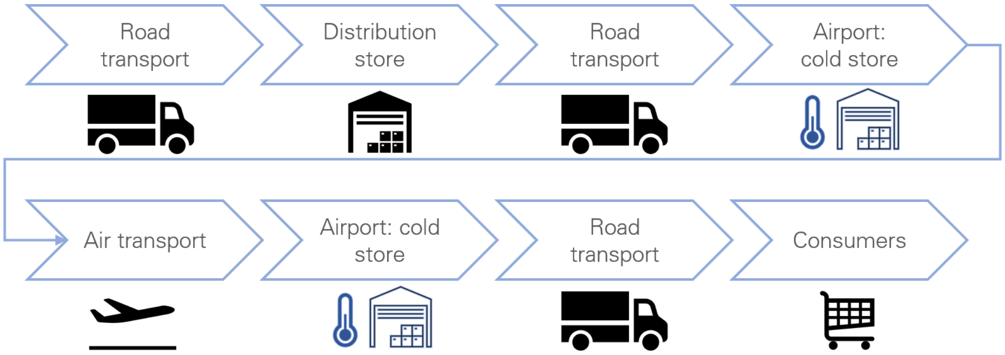


Figure 3.4: Cold chain scenario

There are several possible ways to organize the value chain for the production and distribution of salmon. Figure 3.5 shows the value chain for aquaculture and illustrates alternative forms of organization and ownership along the chain. The arrows show the supplier of salmonoids in different stages and product forms between entities in the value chain. It does not include salmon feed, wellboat services, and input goods, which would make the figure even more complicated. The arrows show possible routes for salmonids and salmon products from smolt to finished product. The figure also shows many opportunities to vary between deliveries internally in integrated value chains and deliveries in markets with different liquidity and transparency.

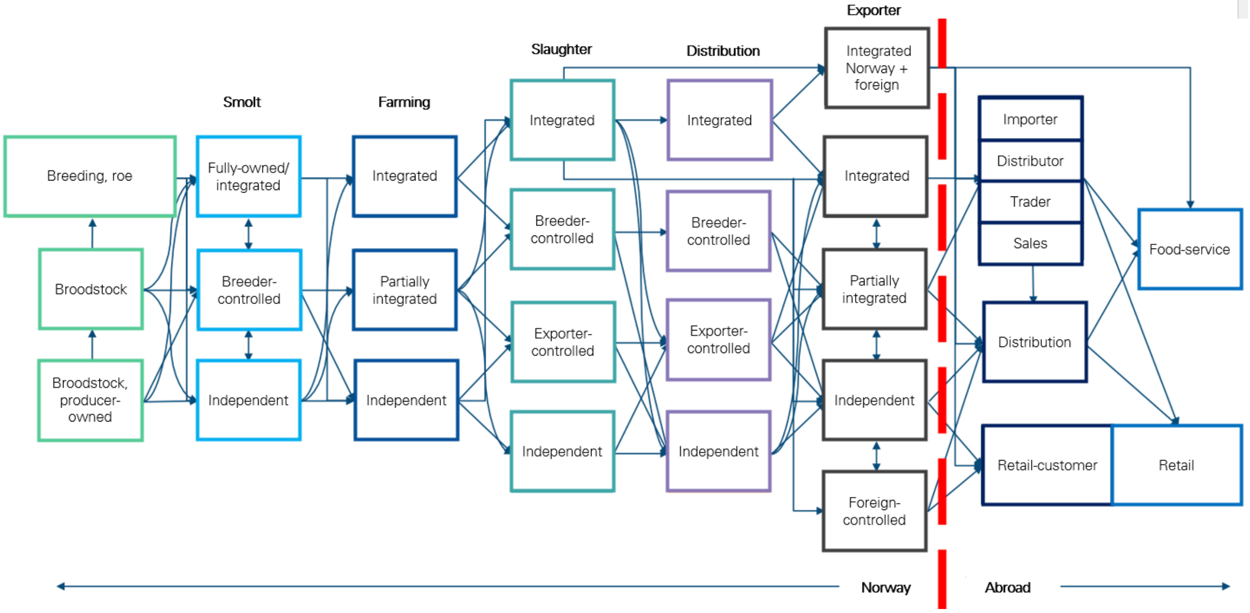


Figure 3.5: Different forms of organization and channels in the value chain for salmonids (adapted from Tveterås et al. (2019))

3.5 Sustainability goals, regulations

Of the UN's 17 sustainable development goals (SDG), goals 2, 3, 9, 13, and 14 have great relevance for the Norwegian aquaculture industry.

2 ZERO HUNGER
3 GOOD HEALTH AND WELL-BEING
9 INDUSTRY, INNOVATION AND INFRASTRUCTURE
13 CLIMATE ACTION
14 LIFE BELOW WATER

Figure 3.6: UN's sustainability goals: 2, 3, 9, 13, amd 14

- **Goal 2:** End hunger, achieve food security and improved nutrition and promote sustainable agriculture.
- **Goal 3:** Ensure healthy lives and promote well-being for all at all ages.
- **Goal 9:** Build resilient infrastructure, promote inclusive and sustainable industrialization, and foster innovation.
- **Goal 13:** Take urgent action to combat climate change and its impacts.

- **Goal 14:** Conserve and sustainably use the oceans, seas, and marine resources for sustainable development.

These SDGs contribute to introducing stricter regulations in the aquaculture industry, which contributes to the industry facing several challenges to satisfy the triple bottom line of economic development, social development, and environmental protection. In the aquaculture industry, there are several special regulations for the industry. These lay the foundations for how the companies run their business. For instance, stagnation in production volume is related to strict regulations resulting from disease problems (Industri, 2017)—environment and sustainability considerations are prioritized over market considerations.

When fish farming companies meet strict industry regulations, opportunities often arise for the supplier industry. Changes in regulations and framework conditions stimulate changes in the operation and development of new solutions and standards (Maurset, 2018).

This thesis aims to shed light on opportunities that can contribute to getting one step closer to reaching SDG 9: Looking into how decentralized systems can help foster collaboration, innovation, and competence and how this can create more resilience in today's aquaculture supply chains, making them more independent of centralized and heavy ERP systems controlled by monolithic enterprises.

3.6 Supply chain data sharing

Traditionally, data has been viewed as an internal resource and not something that has value for others (Janssen et al., 2012*b*). Today, aquaculture enterprises often keep their data to themselves and only share what is necessary for outsiders to perform a single service (Bjørgan et al., 2019). Janssen et al. (2012*a*) derived many benefits and barriers for sharing data and can be found in Appendix C.

Many established companies rely on large amounts of data that can give rise to valuable insights. Nevertheless, it is estimated that about 70% of business data is never used because it is difficult to see how the company can directly profit from it (Martinsen and Tetzchner, 2018). However, this data can also produce value for other partakers who want to build products or find new insights and can be a driver of innovation.

The direct exchange of goods, services, and data between enterprises in a business-to-business (B2B) scenario is a concept that makes sense from a supply chain perspective. The GS1 (2019) Global Traceability standard references a variety of data capture and data sharing technologies and related GS1 standards, including GS1 barcodes, EPC/RFID, GDSN, EDI, and EPCIS. The GS1 EPCIS standard enables disparate applications to create and share visibility event data within and across enterprises, allowing supply chain partners to share important product information such as physical movements, status, and an overview of the product's journey through the supply chain. Each participant that has implemented EPCIS can publish events to the discovery service, which is in charge of locating each product.

Multiple standards have been proposed to extend the GS1. Byun and Kim (2015), for instance, broadens the reach of EPCglobal to suit supple chains better by capturing data from IoT sensors in addition to barcodes. In short, Byun and Kim (2015) created an EPCIS with modifications to store sensed data events and an interface to communicate the data with other IoT applications. There are few incentives in the supply chain to communicate product data, and according to research by Kürschner et al. (2008), there is no desire to share the EPC or EPCIS addresses. However, information exchange between supply chain organizations is critical, and security must be assured to facilitate it. Currently, security measures consist solely of centralized controlled access rights. This is inadequate, especially when participants of the EPCglobal network engage with businesses unaware of their existence. Therefore, a pay-per-information (one-to-one contract) pricing mechanism for these unknown parties was also proposed by Kürschner et al. (2008).

Du et al. (2012) took a slightly different approach, proposing a Partnership-Data-Process (PDP) to enhance the desire to share information throughout a supply chain, arguing that contracts alone are insufficient to achieve information sharing success. As a result, they also featured trust, cooperation, and reliance. The PDP model emphasizes the connection between supply chain partners, a key element when sharing data. Du et al. (2012) divided the model into two categories: Template-based Information Sharing (TIS) and Proactive Information Sharing (PIS). The first is information subject to contractual restrictions, while the second is information they share with their partners when needed. The survey found that a supply chain can only obtain a high level of data sharing by employing effective partnerships if it has a TIS agreement for data sharing, but growing the partnership is not enough to produce a high level of PIS.

4 Problem Statement

Today's aquaculture supply chains experience a high business and technological disconnect. In other words, companies are operating in functional self-interested silos as a result of the traditional way of doing business. Thus, there is an existing gap between the current technological infrastructure and business operations and relationships.

Consider the case of a patient who presents with pain in his lower back. The chiropractor performs a physical examination where several pain points are identified. The chiropractor then proceeds to tell the patient that the different pain points are all a result of an inflammation in his spine.

Similar to the patient's case, the lack of trust in aquaculture supply chains creates challenges to the current way of doing business. Thus, it constitutes an obstacle to further growth and competitiveness. However, to understand the magnitude of this problem, an examination of the symptoms is crucial.

4.1 Trust in a supply chain

Trust is a crucial link between internal and external parties in the supply chain. Internal cross-functional success is contingent on the establishment and maintenance of trust. Similarly, various external supplier agreements are bound by trust. In the 1990s, the function of trust in supply networks became apparent. Trust was established as a prerequisite for sharing knowledge and assets and, nevertheless, critical to the success of a strategic collaboration (Fawcett et al., 2004).

Many studies have examined the role of trust in the supply chain (Fawcett et al., 2004; Gour et al., 2013; Vogel, 2015; Tyndall et al., 1998). However, while most supply chain entities understand the value of trust as an operational and strategic tool, many experience difficulties integrating trust into buyer-supplier relationships (BSRs) (Villena et al., 2011; Stuart et al., 2012). Ineffective systems, inadequate integration of systems and processes, and a refusal to exchange essential information are all factors that contribute to a lack of information connections. Although the importance of trust in supply chain networks is widely discussed, there are few practical examples of application and operationalization of the concept (Fawcett et al., 2004).

A collaborative approach to end-to-end supply chain visibility (traceability and transparency) is ideal for increasing trust and long-term working relationships among stakeholders. In addition, the ability to store information within a secure, real-time data repository of traceability information would allow all parties to gain a deeper understanding of the situation, such as what happened, when, where, why, and by whom. (Sarpong, 2014).

4.2 End-to-end visibility

The continuous business developments, regulatory requirements, consumer demand, geopolitical and trade issues, commodity price uncertainty, and cyberattacks lead to disruptions in the supply chain and growing expenses that affect every supply chain participant's bottom line. Furthermore, diffusion through media and market globalization resulted in a lack of consumer confidence and increased concerns about the origin and the condition in which the salmon reach the end consumer. As a result, producers, retailers, and distributors have acknowledged supply chain cost reduction as a critical concern. However, cost savings and their consequences must be considered in a holistic context of the entire supply chain. Otherwise, reckless cost-cutting in one area might lead to unintended consequences.

Therefore, data-driven methods and effective collaboration among stakeholders to achieve end-to-end (E2E) visibility are prerequisites for reducing costs and achieving optimal supply chain efficiency.

As organizations develop new goods, add new partners, expand to new geographical sites, and endeavor to satisfy ever-changing regulatory and consumer needs, global supply chains require improved levels of visibility. Supply chain visibility helps companies evaluate opportunities and responses in multi-tiered and extensively regulated supply chains. However, the difficulties demanded in tracking and measuring inputs and outputs at numerous supply chain levels and interactions can make data collecting problematic due to unreliable and unstructured datasets.

However, E2E visibility has become increasingly challenging due to commercial privacy requirements on upstream and downstream distribution networks. Many companies in today's aquaculture supply chains lack global information beyond their *Tier-1* suppliers and customers, and the default behavior is to work in self-interested information silos (see Figure 4.1). This creates limitations to innovation, analytical insight, and collaborative solutions that can benefit the entire supply chain. Inefficiencies in process speed, communication, transactions, and KPI insights, combined with uncoordinated data, lead to poor decision-making and force companies to add additional resources, such as inventories, machine time, human resources, and more to handle unforeseen changes in deliveries and demand. As a result, the entire supply chain incurs additional expenses.

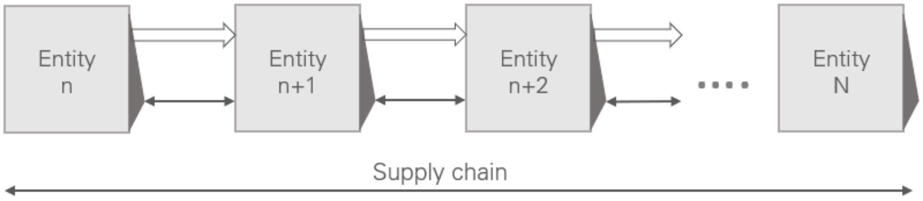


Figure 4.1: Information flow in a supply chain today

Information flow and process workflows in supply chain management often require information and services to be delivered to each relevant stakeholder on a short-time basis due to the lean/just-in-time structure often used in today's global supply chains. However, due to closed silos, and lack of E2E visibility, information traveling upstream and downstream must go through several companies in the supply chain before reaching the intended destination. This creates breaks in continuity, or "gaps", in communication and information exchange. This results in decreased supply chain resilience and flexibility to adapt and react to market changes and take action towards unforeseen circumstances.

COVID-19 demonstrated how many companies lacked responsiveness due to insufficient E2E visibility and the lack of knowledge of supply chain linkages' exposure to global shocks and disruptions. For example, canceled international passenger flights created logistical problems and increased air freight costs for high-value seafood products such as farmed Atlantic salmon. In addition, canceled shipments left producers and distributors without a market for perishable products or a shortage of freezer space (Love et al., 2021).

Similarly, liquidity gaps can threaten companies within a supply chain that experiences disruptions. The average waiting time for a B2B invoice payment, according to Statista (2021), is approximately 40 days, meaning a supply chain with ten gaps would have to wait almost 400 days before the whole transaction is complete. This leads to large sums being tied up at any given time, especially in more layered supply chains with a topology more similar to a network. It also leads to much available equipment (machines, factories, vessels, people, et cetera) being tied up and unused. In case of disruptions and unpredictable or delayed payments, the liquidity gaps expand, creating significant ripple effects and consequences for all supply chain participants. The amount of liquidity held up between companies and their suppliers hit a record high in 2020 as the COVID-19 crisis escalated, and the average number of days set as a payment term for B2B transactions in various countries in Europe between 2019 and 2020 was raised by staggering 25% (Appendix D). Therefore, speed and cost in the economic system are crucial to increasing the supply chain's resilience.

Even though COVID-19 is not a typical risk event, it highlights the importance of continual E2E assessment, optimization, and monitoring when unforeseen events occur. Other events that may cause significant supply chain disruptions, such as geopolitical tension and trade issues, sanctions, commodity price uncertainty, cyberattacks, extreme weather, et cetera, are expected to increase.

A collaborative approach to supply chain traceability is ideal for fostering higher trust and long-term working relationships among stakeholders. The ability to store product information within a secure, real-time data repository of traceability information would allow all parties to establish what happened when, where, why, and by whom when any issue crops up (Sarpong, 2014). This increases the responsiveness and higher supply chain resilience.

4.3 Data-enabled decision-making

With visibility comes knowledge. Data-enabled decision-making plays a vital role in aquaculture supply chain management. However, there are many barriers to extensive data sharing (depicted in Appendix C), and despite the widespread use of data capturing methods in the aquaculture supply chain, significant obstacles restrict data-driven decision-making. First, all this data must be transformed into usable information to create action, but many actions still occur manually, tied down on paper, and the information exchange between supply chain participants is heavily dominated by email, often with PDF attachments. The data obtained through these methods are frequently erroneous and incomplete. As a result, decisions based on this information are sub-optimal. Accurate and secure information exchange is essential for an effective supply chain. A supply chain containing many different databases and, therefore, many versions of truth is subject to high data reconciling costs, miscommunication, and manipulation, especially in an era of deep fakes, edited photographs, and constantly expanding ways of corruption and theft of wealth and data.

Furthermore, many data-gathering technologies, such as sensors, smartphones, and GPS, produce data in various unstructured and heterogeneous forms that do not follow any semantics. This requires pre-processing (2.13) and makes integration and data exchange in the aquaculture supply chain complicated and time-demanding (source: FiiZK Digital executives).

Finally, effective data-driven methods are challenging to achieve due to the requirement of large datasets and computational effort. Existing data-capturing technology cannot handle many data captures simultaneously due to the limited central calculation capacity and computing power required to handle the data. On a supply chain management level, data-driven decision-making models require a variety of data for various tasks such as optimizing production, planning and scheduling, reducing waste, et cetera.

In recent years, the aquaculture supply chains have been affected by a stagnation of production volume and sustainability concerns, suggesting that cost reduction and alterations in the current production regime are critical for future competitiveness. Therefore, an industry transition toward more data-driven decision-making is indispensable to assure long-term value creation by optimizing production while minimizing risk and environmental impact (EY, 2019). However, most industry players lack the scope of quality data and capacities required to address the myriad of industry challenges. Therefore, data exchange, experience exchange, and collaboration are crucial to providing excellent knowledge and innovative solutions. Enterprises must acquire and combine structured data and information from several sources and utilize it effectively to gain analytical insight. This often requires enterprises to upgrade their infrastructure and data structure by utilizing open systems and technical solutions. However, the lack of common data standards, measurements, integrations, and *trust mechanisms* are common obstacles to any extensive collaboration (Janssen et al., 2012*b*).

4.4 Today's operational environment

Both end-to-end visibility and data-driven decision-making are restricted due to the underlying supply chains' current operational environment and data-sharing barriers.

Today, most supply chains are managed by centralized ERP (enterprise resource planning) software. This software manages companies' financials, supply chains, operations, commerce, reporting, manufacturing, human resource activities, and day-to-day business activities. All relationships, information, and data in an ERP system are stored in a single, central repository (database). This centralization is key to the success of an ERP – data entered in one part of the company can be immediately available to other parts of the company. ERPs remove the burden of manual processes and enables a digital way of working. However, this is only a reasonable solution on a supply chain level when most of the supply chain resides within a single authority boundary. Entities within the supply chain can make decisions based on this information, but only in the existence of a trust model creating confidence in the central data store.

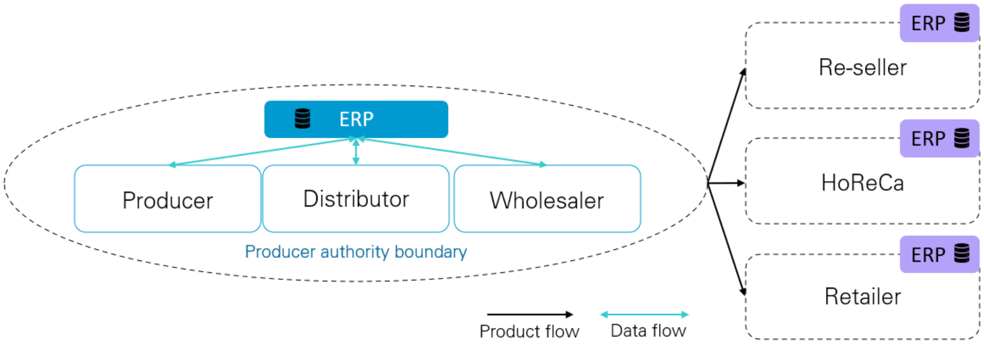


Figure 4.2: Centralized SCM with centralized ERP system

As shown in Figure 4.2, information is stored within a single *authority boundary* to which relevant stakeholders have access. The main problem with this approach is that there is no cross-boundary trust between the authority boundary and the customers. Each customer may or may not have their own ERP systems for managing their supply chain under their own authority boundaries. As the customers are located outside the producer's authority boundary, the customer must either (1) trust and gain access to the producer's ERP system or (2) have the supplier export the data securely into the customer's ERP system.

When a business uses an ERP system, integration tools such as Electronic Data Interchange (EDI) can often be utilized to bridge the technical gap. However, it comes at a high cost in terms of difficulty, cost-effectiveness, and performance. Especially in an era of digitalization where organizations frequently change internal and external system landscapes (Saarikko et al., 2020). If bridging the technical gap fails, businesses revert to the broad usage of manual procedures throughout the supply chain, resulting in evident inefficiencies and potential for errors and fraud.

Nevertheless, there is no evidence or conveyed trust mechanism; even with these possibilities, it is assumed that there is an underlying trust between the supplier and the customer.

Both alternatives pose several operational challenges in addition to the fundamental trust concerns. First, suppose the producer decides to give the customer access to their ERP system. In that case, the provider must safeguard all data accounts and guarantee that only essential and relevant data is accessible to the customer. This is problematic as it might lead to a security breach now that customers who have not been thoroughly vetted have access to the supplier's internal systems. The second option involves directly exporting data to the customer's ERP system, which is difficult since the data between the two ERP systems are frequently incompatible. Nevertheless, before being stored in the customer's ERP system, the data must be verified and converted to the correct format.

A more geographically and authoritatively decentralized aquaculture supply chain is depicted in Section 3.4, Figure 3.5. The figure illustrates the fundamental structure of multiple supply networks today. Due to cost, labor expertise, and other constraints, aquaculture supply chains are frequently spread across numerous partners and are more decentralized. These partners are typically trustworthy and on long-term contracts but not necessarily owned and run by the parent firm, which adds to their decentralized character.

Moreover, decentralized partners can lead to heterogenous EPR system issues. Figure 4.3 shows a simplified example of this.

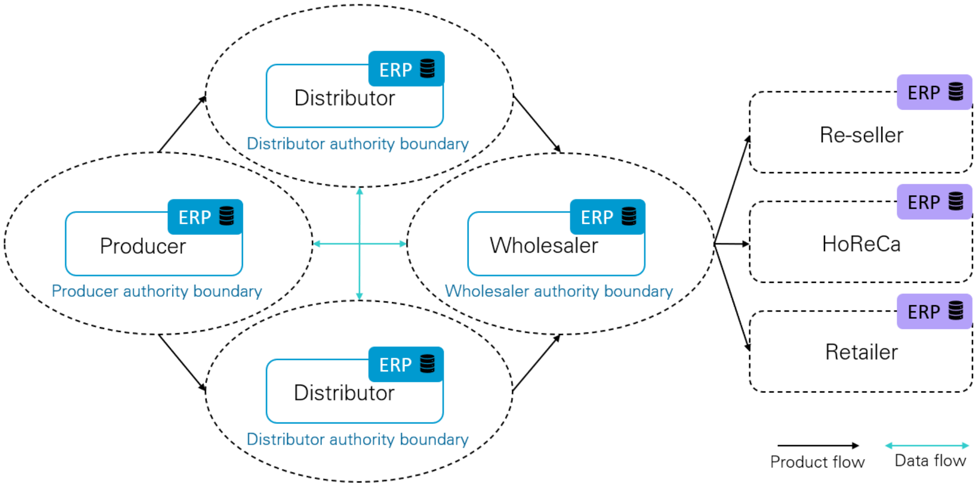

ERP
Distributor
Distributor authority boundary
ERP
Producer
Producer authority boundary
ERP
Wholesaler
Wholesaler authority boundary
ERP
Distributor
Distributor authority boundary
ERP
Re-seller
ERP
HoReCa
ERP
Retailer
Product flow
Data flow

Figure 4.3: Decentralized SCM with centralized ERP systems

Each authority boundary in Figure 4.3 indicates that these supply chain partners are in charge of their own ERP systems. The previously discussed trust concerns also transpire in this scenario. However, the level of intensity surpasses if competitors partner with the same suppliers. Thus, the conflicting relationships create a substantial lack of trust. This is also exacerbated by customers not being within the exact authority boundaries and, therefore, broadening the number of trust mechanisms to maintain.

4.5 Technological bloat

As technological bloat (when an organization invests in numerous software tools) occurs, and human comprehension declines, many aquaculture companies' quality, cost, and delivery metrics are at risk of deteriorating. Even when well-managed and optimized, each new feature, vendor, database, or system might limit a company's capacity to add the next feature, vendor, database, or system while maintaining the current ones. According to personal communication with aquaculture industry executives, this is a common problem, leading to reluctance and mistrust of new systems.

Often, when a business uses an API or ERP system, integration tools such as Electronic Data Interchange (EDI) can be utilized to bridge the technical gap. However, it comes at a high cost in terms of difficulty, cost-effectiveness, and performance. Especially in an era of digitalization where organizations frequently change internal and external system landscapes (Saarikko et al., 2020). If bridging the technical gap fails, businesses revert to the broad usage of manual procedures throughout the supply chain, resulting in evident inefficiencies and potential for errors and fraud.

Of course, businesses use Enterprise Architecture (EA) to avoid such difficulties, and enterprise architects are responsible for designing and deploying coherence and simplicity across the company. However, decisions are frequently based on quick money rather than on potentially costly maintenance tasks or operational changes that do not deliver an apparent, intelligible return in the short term. On the other hand, Enterprise architects can seldom compel decisions about corporate-wide retirement, conversion, acceptance, and installation of systems, regardless of the short- or long-term technical value of the collective financing that will be recouped in the end.

Therefore, businesses require solutions that allow diverse operational groups to agree on a single, trusted version of the data and a single set of technologies to support each business capability when challenges occur due to the proliferation of redundant systems.

4.6 TLDR: Multiple sources of truths

Isolation, operational separation, and lack of communication among supply chain entities are frequent challenges that pose inefficiencies. Aquaculture supply chains require *end-to-end visibility* and *data-driven decision-making models* to meet regulators' and customers' demands. However, supply chains are built upon self-interested data silos. Therefore, collaboration and cross-boundary data exchange become challenging due to increased commercial privacy requirements on upstream and downstream distribution networks.

"It all comes down to trust"

Today's operational environment consists of siloed and centralized ERP systems lacking cross-boundary trust mechanisms that are either overly expensive or technically infeasible. The "source of truth" is held by a single entity; entities beyond the primary authority boundary must acquire access to the truth holder's ERP or export data securely from the truth holder's ERP to their own systems. The first option increases the truth holder's technical and financial load. It also increases overall risk because the (many) additional accounts are now present in the truth holder's centralized domain. The second option necessitates technical conversions due to incompatibility between different ERP systems. Both options must be accepted without proof since there is no common *trust mechanism* (Figure 4.4).

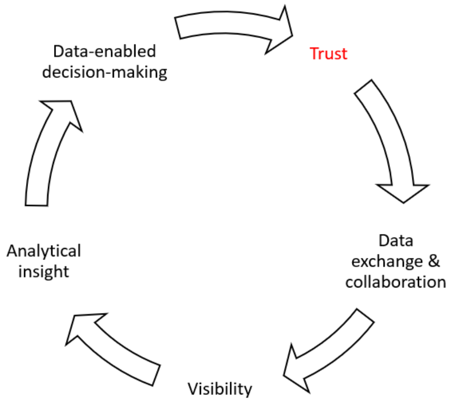


Figure 4.4: The position of trust to enable complete E2E visibility and collaboration (supported by findings in Baah et al. (2021); Kim and Shin (2019); Chen et al. (2022); Qian and Papadonikolaki (2020))

As there are no common trust mechanisms, the various supply chain participants' ability to gain analytical insight is severely limited, and cross-boundary data sharing becomes undesirable. This ultimately results in multiple sources of truths that are subject to manipulation. In addition, it creates limitations to the aquaculture industry's common ground in developing technology and techniques that enable long-term growth. Functional silos must therefore be broken down to enable organizations to connect to their complete supply network to enable end-to-end visibility, collaboration, agility, and optimization.

Hence, the decision-making process must be improved throughout the supply chain to determine solutions to these issues. Doing so requires analytical insight based on extensive and high-quality datasets from multiple sources. However, a foundation of trust is crucial to persuade companies to disclose this data. To generate trust, transparency and traceability (visibility) must be present. Furthermore, disclosing data contributes to increased collaboration to create more sustainable solutions and innovation opportunities. In this context, sustainable solutions entail satisfying the triple bottom line by fostering a trustless and decentralized network for industry stakeholders to detach from monolithic enterprises and build a resilient supply chain.

5 Method

5.1 Towards Industry 4.0

Collaboration between suppliers, producers, and consumers is critical for increasing transparency across and within a supply chain (Tjahjono et al., 2017). Industry 4.0 highlights a worldwide networks of machines in a smart environment that can autonomously exchange information and control one another.

Figure 5.1 depicts the technology life cycle and lists obsolete, mature, and emerging technologies that can benefit the way aquaculture supply chains transact, store, and utilize information. Emerging technologies such as cloud computing, AI, big data, blockchain, and IoT, are categorized as Industry 4.0 technologies.

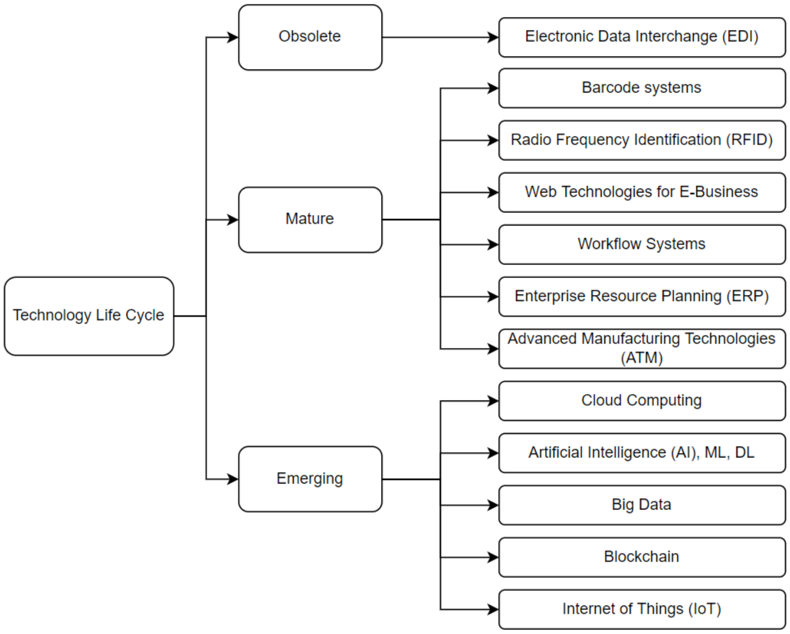

Technology Life Cycle
Obsolete
Electronic Data Interchange (EDI)
Mature
Barcode systems
Radio Frequency Identification (RFID)
Web Technologies for E-Business
Workflow Systems
Enterprise Resource Planning (ERP)
Advanced Manufacturing Technologies (ATM)
Emerging
Cloud Computing
Artificial Intelligence (AI), ML, DL
Big Data
Blockchain
Internet of Things (IoT)

Figure 5.1: Technology lifecycle towards Industry 4.0 (adapted from Núñez-Merino et al. (2020))

These methods (technologies) can be used interchangeably, and there is no definitive answer on how to combine them in the best possible way. Nevertheless, decision-makers in aquaculture enterprises need to evaluate *how* the information should be stored, exchanged, and utilized to break down the functional silos, enable extensive data exchange, and foster collaboration and innovation to meet the regulatory demands in the aquaculture industry.

Aquaculture enterprises and supply chains must evaluate what matters most, (1) disintermediation and robustness, or (2) confidentiality and performance. In principle, this is whether to use decentralized blockchains or centralized databases.

5.2 Databases Vs. Blockchain

This section will explain the key differences between databases and blockchain and decide on whether to use databases or blockchain as a method to solve the problem explained in Section 4.

5.2.1 What is a Database?

A database is a repository of structured information organized into tables. The most important aspects of a database are the rules about the stored data. These rules help ensure that the information remains rational and consistent for the benefit of organizations. The rules in today's most popular databases take several different forms (solid IT gmbh, 2022), such as: *the database schema* defines the economy of information that is permitted in each column, *check constraints* enforce a relationship between column values in each row, *foreign keys* enforce a relationship between tables, and *unique keys* a particular column must have a different value in every row (Greenspan, 2015).

A database does not solve the problem of *trust* when businesses want to share a database across boundaries.

If two or more companies want to share a database (with write-access) that none of them control, all companies can be relied upon by everyone. Frequently, the companies have different incentives, they do not necessarily trust each other, and they may even be fierce competitors. The solution has almost always been the same: introduce a trusted intermediary that manages the database centrally, provides accounts to all partakers, and ensures that the operations' pre-established rules are followed.

In many cases, every party maintains a copy of their database and spends much time performing *data validation* and *reconciliation*, making sure their databases agree (Halaburda, 2018). This leads to inefficiencies and additional costs. The requirements of a read/write database to be shared between parties without a central authority are similar to those integrated in a blockchain, however, they are difficult to achieve, and it so happens that blockchains seem to be the best solution for sharing a database between untrustworthy parties.

5.2.2 What is a Blockchain?

As explained in Section 2; A blockchain is a decentralized, digital ledger that records and preserves all transactions between users on a network. Transaction records (also known as 'blocks') are timestamped and cryptographically encrypted, ensuring that they are kept in a linear, chronological sequence. This creates a transparent, immutable collection of all protected records against alteration, eliminating the need of intermediaries controlling the transactions. All participants in a blockchain network keep real-time copies of the Blockchain on their server nodes. For redundancy, a party will frequently have many nodes carrying copies.

Blockchain combines a long list of old ideas in a new way, including: *peer-to-peer techniques*, grouping transactions into *blocks* (2.2), *one-way cryptographic hash functions* (2.6), a *multi-party consensus algorithm* (2.5), and *public-key cryptography* (2.6.3).

Blockchains can **restrict the transformations that a transaction can perform**. This breakthrough makes the difference when sharing a database between untrustworthy parties.

While blockchains offer certain benefits, they also have significant drawbacks. In other words, the selection between a blockchain and a traditional database, like other technological decisions, is based on a set of trade-offs. It is important to note that; **if trust and robustness are not an issue, there is nothing a blockchain can do that a regular database cannot.**

5.2.3 Disintermination: advantage blockchains

The main benefit of blockchain is that it allows a database to be shared directly across trust boundaries without the need for a central administrator and application logic to enforce the transactions (2.2). Several nodes can independently verify and process transactions in the blockchain while the blockchain consensus mechanism keeps the nodes in sync.

Disintermediation is valuable because the data in a database is tangible. A database's contents are kept in the memory and disk of a specific computer system. This means that anybody with the credentials to that system can destroy or corrupt the inside data. As a result, once businesses put the data into a traditional database, they become reliant on the human organization that houses that information. Nevertheless, several organizations have acquired this trust: banks, governments, universities, and tech giants, to mention a few. So, what exactly is the issue? If an organization is in charge of a crucial database, it will require many personnel and processes to ensure that the database is not tampered with, which costs time and money 2.

As a result, blockchains provide a solution to replace these organizations with a secure distributed database due to sophisticated cryptography. Using computer systems' ever-increasing capabilities to give a new means of replacing humans with code is usually a lot less expensive once developed and debugged. Due to sophisticated cryptography, blockchains can replace these organizations with a secure distributed database 2.

5.2.4 Confidentiality: advantage databases

Confidentiality is one of the downsides of a blockchain because every transaction in a blockchain is independently verified and processed by each node. A node may accomplish this because it has complete visibility into the state of the database, modifications requested by a transaction, and digital signatures that verify the transactions' provenance. However, the total transparency provided by each node can therefore be a deal-breaker for many business applications.

A blockchain can only be write controlled if the regular database is read and write controlled. There are, however, a few strategies available for mitigating this problem. This ranges from simple ideas like transacting under multiple blockchain addresses to more advanced cryptographic techniques such as confidential transactions and *zero-knowledge proofs*. Nevertheless, the more information required to hide on a blockchain, the heavier the computational burden becomes to generate and verify transactions Chowdhury et al. (2018).

5.2.5 Robustness: advantage blockchains

The built-in redundancy of blockchains provides excellent fault tolerance. As each node executes each transaction, no single node is critical to the database's overall performance (2.2). The nodes are connected in a peer-to-peer network and the blockchain assures that nodes having gone down for power or other hardware failures always catch up with their missed transactions.

Traditional databases also offer a variety of replication options. However, there is no need for configuration in a blockchain; connect a few blockchain nodes, and they will autonomously stay in sync. Nodes can also be added and removed from the network without any precaution. Finally, transactions to any node will propagate to all the other nodes instantly and absolute.

With regular databases, high availability is achieved by costly infrastructure and *disaster recovery*. While the primary database runs on high-end hardware that is constantly checked for problems, transactions are replicated to a backup system in a different physical location. If the primary database fails, all activity is promptly moved to the backup database, which takes over as the primary. After the failed system has been fixed, it is configured to function as the new backup system if and when it is needed. While this is achievable, it remains costly (Choy et al., 2000).

5.2.6 Performance: advantage databases

The average time for a transaction to be validated and stored in all peer nodes is substantially larger for blockchains than centralized databases. This is because a blockchain has to do everything as a regular database plus three additional burdens: *signature verification*, *consensus mechanisms*, and *redundancy*, which satisfies all the nodes. Greenspan (2015) explained them well.

- **Signature verification**: A public-private cryptography system like *ECDSA* must be used to sign every blockchain transaction digitally. Because transactions travel between nodes peer-to-peer, their origin cannot be established otherwise. The development and verification of these signatures are computationally demanding and can be a critical bottleneck when implementing Blockchain. In contrast, once a link to centralized databases has been created, there is no need to check each request that comes across it manually.
- **Consensus mechanisms**: In a distributed database like a blockchain, work must be put in to ensure that all nodes in the network agree. Depending on the consensus process, this might include a lot of back-and-forth communication and deal with forks and rollbacks. While centralized databases must deal with conflicting and aborted transactions, these are significantly less common when transactions are queued and completed in one spot.
- **Redundancy**: This is not about the performance of a single node but rather the entire amount of processing required by a blockchain. Unlike centralized databases, which process transactions once (or twice), a blockchain requires each node in the network to execute transactions separately. As a result, more labor is being done to achieve the same result.

5.2.7 The bottom line

Naturally, there are additional methods to compare blockchains with traditional databases. Table H.1 summarizes the key differentiators of a traditional database and a Blockchain. But when it comes to deciding whether or not to implement a blockchain in the long run, businesses have to decide what is most crucial to their use case. What is the relationship between disintermediation and robustness, and performance and confidentiality?

In a GEP survey of 400 C-suite executives at European and US global companies, 64% reported revenue losses between 6% and 20% in 2020, which GEP calculated to be as much as $4tn. Around 38% of firms with revenue greater than $1bn said there had been "significant damage to the company's brand reputation" due to supply chain disruptions from Covid-19. A third (33%) added disruption meant their "operational costs increased." **The report from GEP also stated that 61% of respondents agree that "redundancy and resilience in their company's supply chain are more important than speed and efficiency"**. This is to a very high degree comparable to to the robustness (5.2.5) and disintermediation (5.2.3) that Blockchain provide.

The chart in Figure 5.2 demonstrates an overlapping effect with regards to supply chains and the public and fully decentralized blockchain advantages.

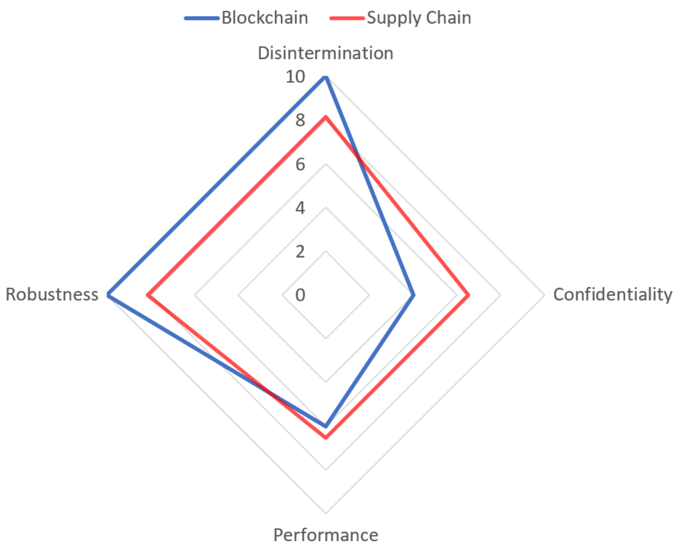


Figure 5.2: Supply chain requirements (normalized) based on the GEP survey compared to the blockchain's advantages in disintermination, robustness.

Blockchains are a trade-off that achieves disintermediation at the expense of confidentiality.

Determining blockchain suitability and applicability always comes down to this specific trade-off. However, this trade-off is not always easy to discover with the untrained eye. Gourisetti et al. (2020) proposes a blockchain application framework (BAF) designed to ingest detailed user requirements to perform a weighted evaluation that is built on mathematical constructs to determine the ideal combination of blockchain that is appropriate for an application. The BAF is divided into five domains, 18 subdomains, and about 100 controls (Figure 5.3).

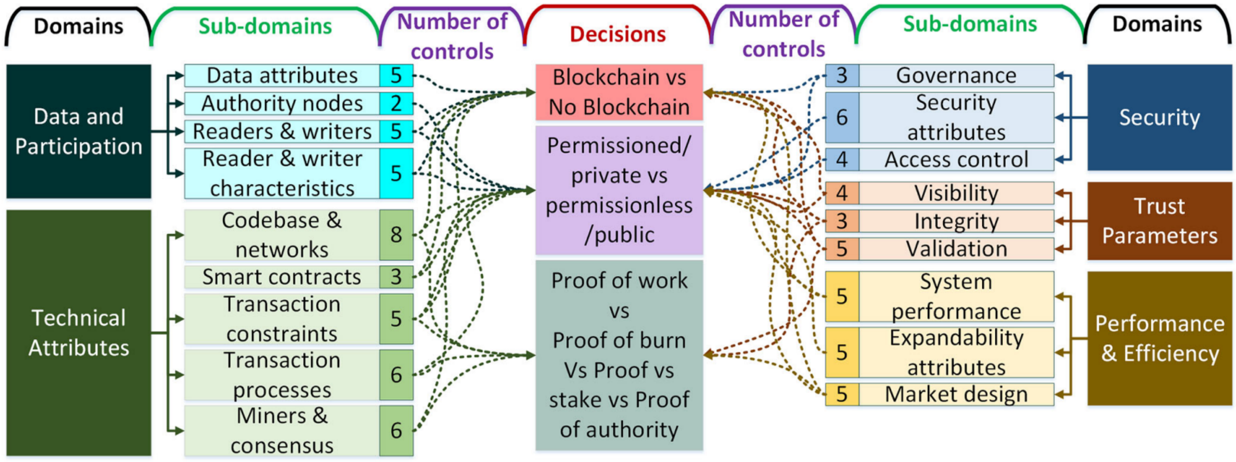


Figure 5.3: Architectural overview of the blockchain application framework. Adapted from Gourisetti et al. (2020)

According to the BAF model, permissioned proof of authority (PoA) blockchains, such as Hyperledger Fabric, would be ideal for supply chain management. Gourisetti et al. (2020) also notes that Proof-of-work consensus can also be sufficient because supply chain management does not have high-performance requirements.

5.3 Method of choice: Blockchain

All the identified problems in Section 4, and the weaknesses discovered in current solutions propagate from one crucial root cause: the problem of developing and integrating proper trust mechanisms. Research shows that the value captured from blockchain technology is its ability to create trustless and decentralized networks.

Therefore, this thesis concludes with blockchain technology as the preferred method of choice.

6 Model

This section presents two interconnected models that can work simultaneously and independently. The models' design aims to close ubiquitous business- and technology-driven gaps in aquaculture supply chains and is based on literature review and industry actors' value propositions.

(1) The first model is a blockchain-based SCM model and can be viewed in Section 6.1. The model is similar to an ERP from a user perspective, but the back-end design is entirely decentralized. This facilitates new actors to engage in the supply chain network and contribute with customized and decentralized applications (dApps) while securing complete end-to-end visibility, resilience, and supply chain agility.

(2) The second model proposed in Section 6.2, is a decentralized and collaborative machine-learning paradigm that applies to aquaculture supply chains, enterprises, researchers, entrepreneurs, scientists, and machine learning enthusiasts.

The design of these models aims to provide insight into how today's aquaculture supply chains along the Norwegian coast can evolve in a more decentralized direction. This allows for extensive collaboration, innovation, and competence in the domain and makes aquaculture supply chains along the Norwegian coast independent of expensive and centralized systems controlled by monolithic enterprises.

6.1 Blockchain-based supply chain management model (BSCM)

Figure 6.1 presents a high-level architecture for the proposed blockchain-based supply management model (BSCM). The BSCM is divided into four connected layers; the physical, application, connection, and blockchain. Aquaculture supply chain participants and industry stakeholders can access the blockchain layer through their customized-built decentralized applications (dApps, 2.1), which are connected to either NFTDTs or an API, depending on whether the user is uploading, sourcing, or downloading data. The blockchain layer includes on-chain resources, smart contracts, and off-chain resources. dApps ensures that the user interface and experience (UI/UX) are as intuitive as if they were interacting with a centralized application. However, the key differentiators and value-added lie in the decentralized back-end structure. The following subsections will provide more details on the layers and components.

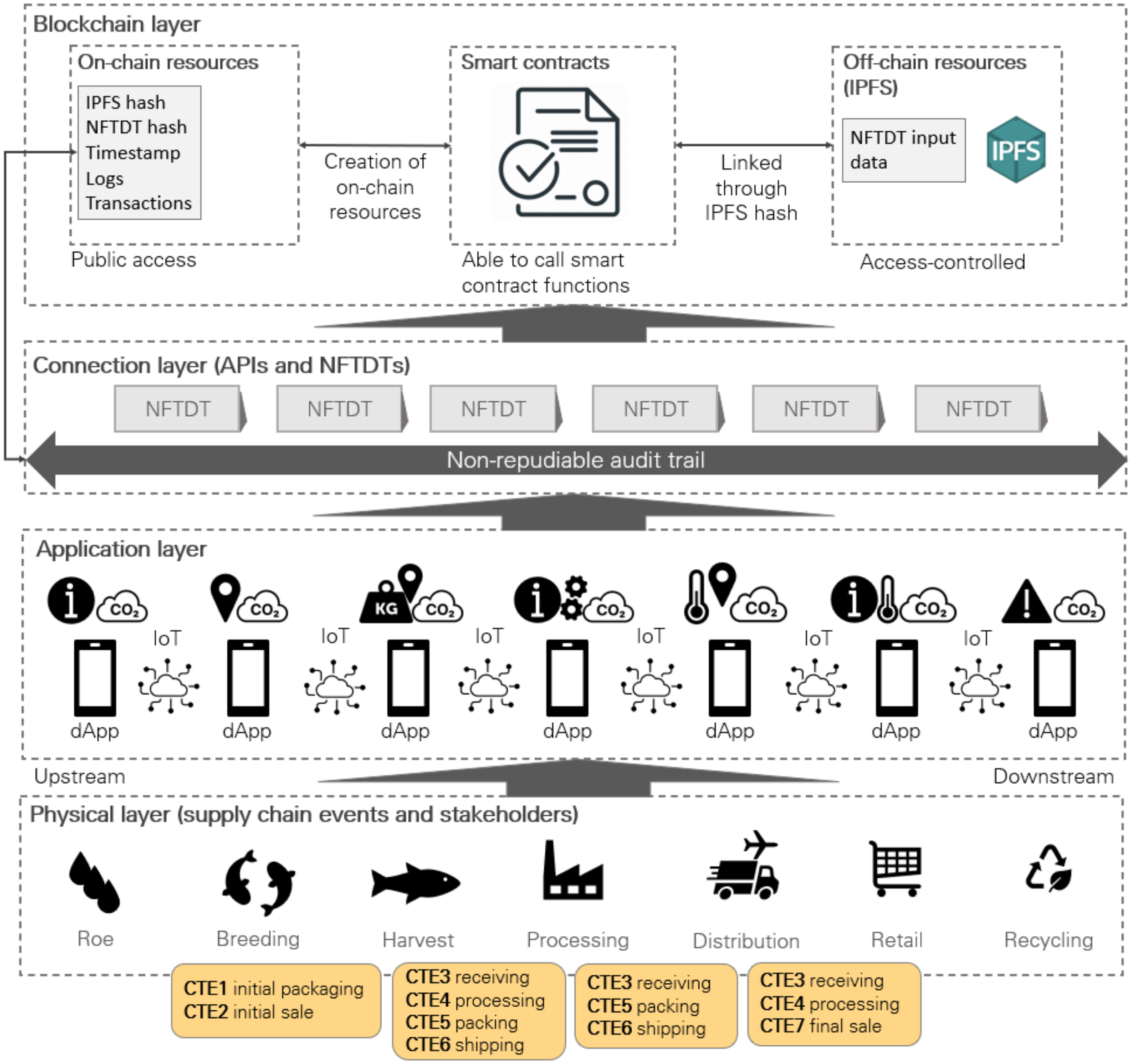


Figure 6.1: A high-level architecture for the proposed blockchain-based SCM model (inspired from Chen et al. (2017); Musamih et al. (2021)) with Critical Tracking Events (CTE) examples from GS1 (2019).

6.1.1 Physical layer: CTEs and KDEs

The *physical layer* covers the entire physical supply chain end-to-end (E2E) and includes all *Critical Tracking Events* (CTE) conducted by supply chain entities and industry stakeholders. In general, all actions that can be digitized or recorded, supplemented with information, or relevant data points, such as *Key Data Elements* (KDE) (Appendix B), are included in this layer. According to the GS1 (2019) *Traceability Guidelines For Fish, Seafood, and Aquaculture*, CTEs are necessary actions for ensuring E2E traceability and go beyond recording commercial transactions between trading partners. The purpose is to provide a detailed view of the physical events, including the final sale to the end consumer.

6.1.2 Application layer: dApps and IoT

The application layer consists of dApps and IoT sensors. The dApps make it possible for the participants of the BSCM model to interact with the blockchain layer, uploading, sourcing, and downloading documents. The IoT's purpose is to enrich the NFTDTs with real-time quality data. The data from the IoT devices flows directly to the NFTDTs without any human input. As a result, data manipulation becomes very challenging, while record keeping and provenance tracking become straightforward. Further benefits of the alliance between IoT and blockchain technology is discussed in Section 2.14.

6.1.3 Connection layer: NFTDTs and non-repudiable audit trails

The *NFTDTs* positioned in the connection layer are characterized as the interaction between digital twins (DT) and non-fungible tokens (NFT). NFTDTs are based on a proof-of-concept (PoC) conducted by Nielsen et al. (2020). DTs are virtual representations serving as the real-time digital counterpart of physical events, products, assets, and commodities. NFTs are non-interchangeable units of data, as aforementioned in Section 2.8. Combining them creates NFTDTs, which is essential for making physical commodities trackable and exchangeable on the blockchain. The NFTDTs will act as a virtual "proof of authenticity" that is significantly more difficult to counterfeit or steal than a piece of paper.

After securely enriching the NFTDTs with data, they are transferred in parallel with the actual commodity through smart contracts. After receiving the NFTDT, the final recipient of the physical object may verify the chain of custody back to its provenance. Thus, the BSCM model ensures that the real-world chain of custody is perfectly replicated by a series of transactions validated and logged to the blockchain. This creates a *non-repudiable digital audit trail*. The audit trail enables complete E2E visibility and communication between all the stakeholders in the supply chain network, making real-time decision-making and automated and secure business messages such as orders, deliverance, custom clearance, and settlements feasible. As a result, a foundation for more efficient and secure downstream and upstream information exchange can be achieved. This eliminates the communication gaps discussed in Section 4.2) and provides a ground for improved supply chain agility.

When provenance is tracked on a blockchain shared by all parties in a supply chain, no single entity or small group of organizations can tamper with the chain of custody, giving end-users increased trust in their answers. In other words, this model creates one fully transparent *single source of truth* which makes upstream and downstream tracing feasible. Truths are recorded as immutable facts. This generates an extra security (and value) layer to the data, assuring the integrity of the data.

The NFTDTs are a powerful component when combined with digital signatures (2.6.3) and programmable logic to ensure that stored and shared data is, in fact, immutable and trusted. Third parties or machine learning algorithms can enforce validation, and illogical deviations can be detected. This adds an incentive to upload credible data in the first place, resulting in complete transparency and quality data. Exportable and verifiable proof for customers, regulators, and authorities, such as customs registries, certificates, accountability, or evidence of sustainable practices, are examples of applications.

Norwegian Seafood Trust (personal communication) stated that complete transparency is the main contributing factor hindering fraud and actors from engaging maliciously due to various aspects such as, e.g., self-interest and competitive advantage. Analytic models can aid researchers in determining where data came from, who the original owner was, how it was updated over time, and whether any alterations were coordinated. Therefore, hostile actors will likely not engage in a blockchain-based system and will be "weeded" out accordingly.

Table 6.1 provides a list of data that qualifies as CTEs according to GS1 (2019). They are based on trade item master data, CTEs (B), and personal communication with aquaculture industry actors. Note that all the data logged on the blockchain are timestamped. However, for the data not recorded in real-time, the time of the CTEs should be included when recorded so that the digital audit trail stays reliable.

Supply chain events	**NFTDT input data**
Fertilized eggs	DNA, environmental conditions, output emissions (See E.1)
Broodstock	Transfer date, fertilization data, PH value, feed, environment, output emissions
Breeding	Feeding events, length of feeding pauses or interruptions, environmental conditions, mortality rate, output emissions, location
Growth	Weights, size distribution, medical conditions, vaccines, lice, temperature, feeding events, lengt of feeding pauses or interruptions, transport events, output emissions
Harvest	Time, location, weight and size distribution, biomass, output emissions
Processing	Time, location, process description, temperatures, emissions, output emissions, freeze date, best before data or use by date
Distribution	Temperature (cold chain 3.4), location, timestamp, output emissions, locations
Retail	Temperature, location, waste, output emission, taste, quality, feedback
Recycling	Recycling data, waste, reuse, life cycle assessment (E.1)

Table 6.1: Supply chain events and data eligible for blockchain storage (based on personal communication with FiiZK Digital and GS1 (2019))

6.1.4 Blockchain layer: on-chain resources, smart contracts, and IPFS

The BSCM model presented in Figure 6.1 allows network participants to store data on a distributed network and make it readily available while assuring data integrity and authenticity. Committed data on the blockchain cannot be retrospectively altered to promote a story due to the technology's intrinsic transparency and immutability (2.3).

Due to limitations such as *gas fees*, the cost of memory in various blockchains, commercial privacy requirements, and the demand for access-controlled data, there must be a distinction between (1) insensitive and small inputs and (2) sensitive and extensive inputs.

(1) Insensitive and small inputs that can be compressed easily, such as text or NFTDT data input from Table 6.1, can be directly stored on the public blockchain without inducing a high cost. Text can easily be compressed using vocabulary dictionaries or commonly shared encoders such as the *Universal Sentence Encoder*.

(2) Sensitive and extensive inputs, such as documents, pictures, and complex models requiring extensive data samples, would be very costly and infeasible to store directly onto the blockchain and must be encrypted and stored off-chain (2.15), with a hash logged to the blockchain.

The *Inter Planetary File System* (IPFS) will be used as off-chain storage in the BSCM model to stay true to its decentralized nature. The IPFS is a content-addressable peer-to-peer hypermedia distribution protocol and a *decentralized storage* (DS) network based on blockchain technology. In other words, IPFS is a network transport protocol for storing and sharing data permanently while distributing and connecting all computing devices on the same file system in a distributed peer-to-peer fashion where the network's nodes create distributed file system. The file system combines features of prior peer-to-peer file systems such as DHTs, BitTorrent, Git, and SFS. Each file is hashed (2.6.1), and a digital fingerprint is formed before being uploaded to the network. IPFS deletes files with the same hash value over the network; checks the hash values to see which files are replicated redundantly and removes redundant files from the root cause. The file's hash value may be used to locate the file on the network and locate the desired file (Wang et al., 2018).

The IPFS can be utilized to manage access to off-chain data. Each time a data object is accessed, it can be verified using stored hash values, proving that it is the same object as the one stored initially. Through IPFS and blockchain, each object or file is stored in multiple nodes to ensure that one node's loss does not result in significant data loss as long as the node is down. Once a node rejoins the decentralized storage after recovery, a mechanism automatically synchronizes the off-chain references and rebalances the off-chain data. According to IBMCorp (2018), these are all requirements for secure and access-controlled data storage.

Figure 6.2 explains the back-end structure when users submit and download data from IPFS. Smart contracts (2.8) plus an incentive mechanism (6.1.5) is necessary and their role will be discussed.

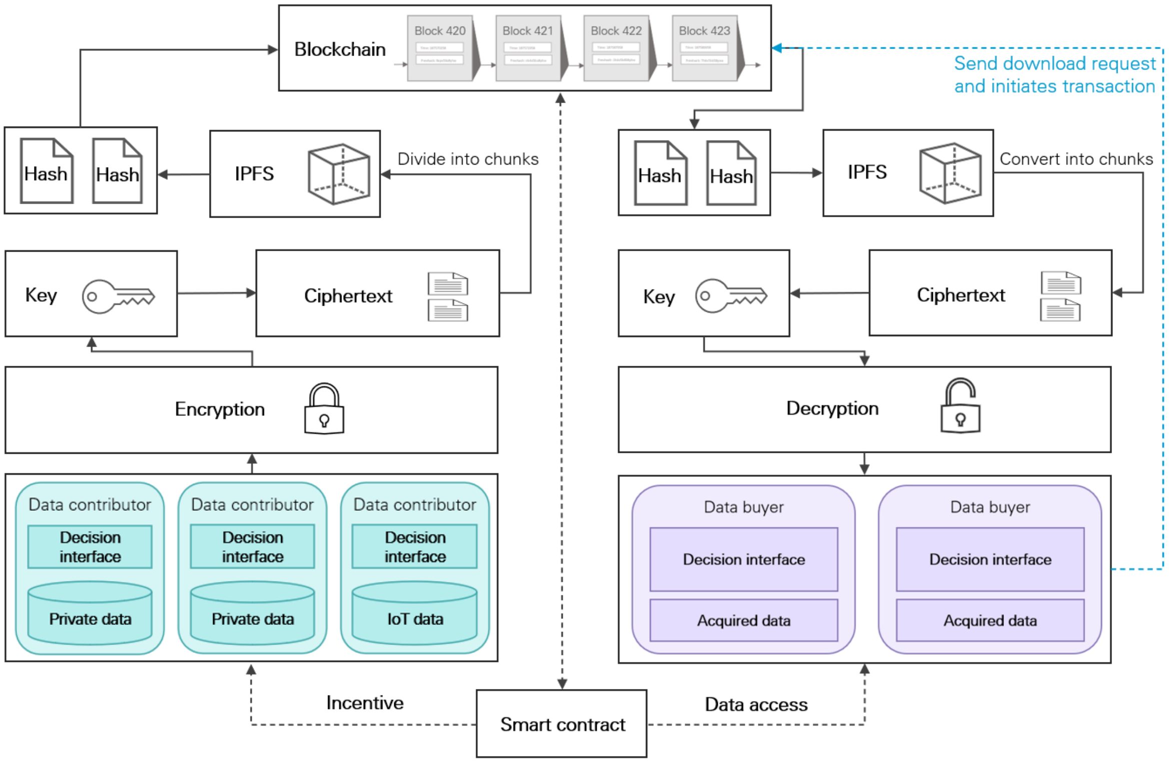


Figure 6.2: Access-control and IPFS file upload and download (inspired from Naz et al. (2019))

The IPFS system stores the uploaded off-chain data (2.15). This is usually data that are infeasible to store on the blockchain directly due to their size (IoT data, product data, documents, et cetera). The resulting hash value is encrypted before being recorded in the blockchain as ciphertext (see figure 6.2). Access control is determined through smart contracts; permissions for acquiring the unique hash leading to the content located on IPFS. The smart contract has predefined conditions. When a node or supply chain entity requires access to data, a transaction must be initiated first, which is then verified by other blockchain nodes on the network. If the verification succeeds and the predefined access rules are satisfied, permission is granted.

6.1.5 Incentive mechanism and micropayments

The ability to share and validate the information in a blockchain model becomes stronger with the number of parties involved and engaging in the network. However, in the process of data sharing, there are still three problems to be solved: unwillingness to share, fear of sharing, and inability to share. Unwillingness is deeply affected by the formation of mutual-trust relationships and the economic utility of data sharing (Xuan et al., 2020). Another reason for not sharing is that some companies do not benefit from the data or from sharing it, leaving them empty-handed only with a restructuring cost.

This subsection proposes a dynamic and monetized incentive mechanism (IM) based on blockchain smart contracts that can utilize user participation, enabling more participants to benefit from data sharing.

The IM requires blockchain smart contracts to automatically distribute incentives to the participants engaging and sharing quality data to the blockchain. It also requires a token economy to enable cryptocurrency micropayments (2.9). The IM validates the request to add data and can be triggered to provide micropayments (cryptocurrencies/stable coins) to those who share quality data. Micropayments encourage information sharing by allowing companies to sell tiny chunks of data. All exchanged data can be cryptographically signed, encrypted, and logged into the blockchain network.

Smart contracts can be used to create trusted and verifiable supply chain automation among supply chain entities. Automation means converting supply chain processes into algorithms and deploying them with the blockchain framework. This is required to achieve business agility, consistency, and efficiency. On the other hand, cross-boundary automation must be founded on a universal trust mechanism, a critical component of intercompany supply chain collaborations (Kwon and Suh, 2004).

In the blockchain-based SCM model presented in 6.1, the data creators/contributors will own all the data stored on the blockchain. The creator can then decide: (1) if and whom they will share the information with (access-control) or (2) if they are selling that information to another party (incentive mechanism).

This can be facilitated through functions enabling, e.g., subscription opportunities on different sets of information, which will make it easy to share and purchase information. Figure 6.3 shows *Company C* purchasing information from *Company B*, while *company A* and *D* either lack access or is not purchasing any data.

Smart contracts enable legal, automated, secure, and guaranteed transactions without the participation of a third party, therefore increasing speed and efficiency and lowering costs. Smart contracts execute micropayments automatically, which facilitates incentives for the different parties to share information/-data actively and streamlining and increasing collaboration and transparency across and within the supply chain.

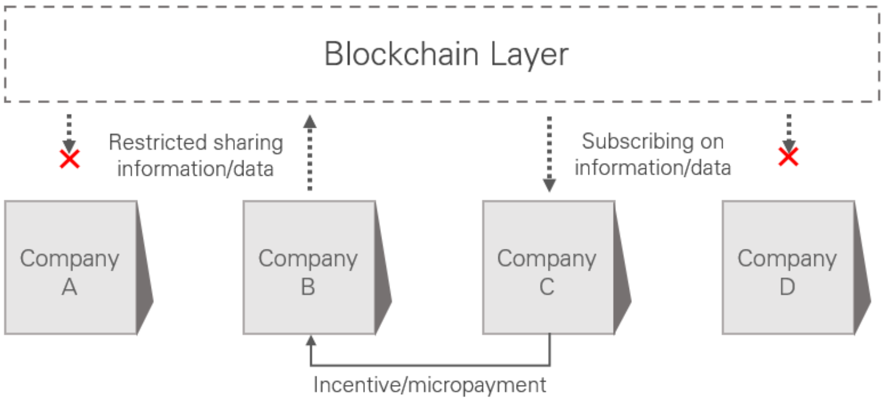


Figure 6.3: Monetized information incentive model

Example 1 (under normal circumstances): A data contributor (distributor) that wishes to sell its information (e.g., location, the temperature of the fish, etc., measured in real-time through sensors) to its peers within the supply chain/blockchain network. Now, consider a stakeholder (data purchaser) subscribing to this specific information due to ETA and quality assurance reasons. Every time the subscriber views the data issued by the contributor, a smart contract automatically transfers small amounts of cryptocurrencies to the contributor. The contributor generates additional income, while the data purchaser gets valuable information.

Example 2 (in case of deviations): The contributor (distributor) is bound by contract to transport the Atlantic salmon at a given temperature range (e.g. [0°, 2°]). A stakeholder may now ensure that this criterion is met by monitoring the transport or coding the criteria directly into a smart contract. In case of any deviations from the predetermined interval criterion, a smart contract may automatically notify or issue a penalty (based on the level of temperature deviation) to the contributor. The penalty can be a small sum of crypto-tokens. The smart contract pseudo-code presented below shows how this can function in practice:

```
while temp $< 2$ && temp $> 0$ do
    SendTempPenalty(temp)                ▷ Sends penalty based on temperature
    Thread.sleep $(60 * 1000)$           ▷ Waits 1 minute to check temp again
end while
```

All terms and conditions can be digitized, stored, and tracked in the blockchain. Smart contract will then be triggered when terms and conditions are met (e.g., pricing, quantity, quality, temperature, time, et cetera), releasing payment to the relevant supplier. In case of deviations (like in example 2) where the conditions are not entirely met, the smart contract can issue predetermined penalties or actions. Smart contracts are briefly discussed in 2.8. Electronic transactions replacing human interaction can also improve audibility and transparency in the flow of products for all parties involved (Chapman, 2019).

6.1.6 The bottom line

Incorporating blockchain-based solutions into aquaculture supply chains will increase security, transparency, and responsiveness. It can ultimately lead to an end-to-end transformation into a hyper-efficient, cost-saving, and risk-reducing Demand Chain.

6.2 A collaborative ML paradigm

One of the most common aims of an organization's analytics efforts is predictive analytics. Large enterprises may already have datasets that are sufficient to make accurate predictions (2.13). On the other hand, small and medium-sized enterprises, new industry actors, entrepreneurs, and data scientist are unlikely to have enough data to make reasonable projections.

Purchasing data from an aggregator was formerly a standard method of obtaining enough data for helpful analysis. Each data acquisition request is costly, and the information is often restricted. The use of blockchains can revolutionize how companies access data. As more businesses use blockchain technology, analysts may be able to use the additional data to enable more businesses to apply predictive analytics with less reliance on localized data.

A collaborative Machine learning (ML) paradigm is, therefore, proposed in to optimize production processes using captured quality data from a decentralized network of contributing nodes. The more data collected, the more informed decisions can be made. The data can, for instance, tell which locations are best suited for production concerning the surrounding environment, give greater insight into whether the fish thrive in the cage, provide accurate predictions on biomass, disease outbreaks, lice infestation. It can also connect to the blockchain-based supply chain model presented in Section 6.1 and optimize the supply/value chain, while enabling economies of scale, allowing smaller organizations to benefit from the same systems as larger ones.

An overview of the proposed blockchain-powered and decentralized machine learning collaboration paradigm is illustrated in Figure 6.4. The proposed paradigm intends to facilitate effective collaboration across and within the aquaculture supply chain and stakeholder environment. Accessible and distributed nodes can complete data-driven tasks requiring high processing power and massive datasets.

The individual nodes (participants) can play five roles; ML task initiator, B2MLan converter, data contributor, model contributor, and verification contributor, each accountable for their behavior. A blockchain network node may also simultaneously act in all the roles, but the paradigm is designed to distribute the roles across various nodes. The schematic diagram showing workflows for each node is shown in G.

(a) **ML task initiator:** in charge of identifying and announcing valuable ML tasks, such as objectives, constraints, model structure concepts, and financial incentives issued automatically on blockchain smart contracts. Entities within the aquaculture supply chain will typically take this role. They describe the data-driven applications using coherent and precise business language by filling out pre-structured forms and documents.

(b) **Business to model language (B2MLan) converter:** in charge of converting the ML task's business language into coding language and technical requirements suitable for ML models (data input, evaluation metrics, output, et cetera) and locking the requirements to the blockchain through smart contracts. The technical requirements disseminate across the distributed network in a peer-to-peer fashion. At the same time, smart contracts notify all network participants of a new task through the blockchain application layer (Figure F.1).

(c) **Data contributor:** in charge of feeding the model contributors with relevant data (which is specified in the technical requirements). Before deciding to engage, they can assess the smart contract's incentive and determine if it is a fair trade—engaging means sharing their dataset off-

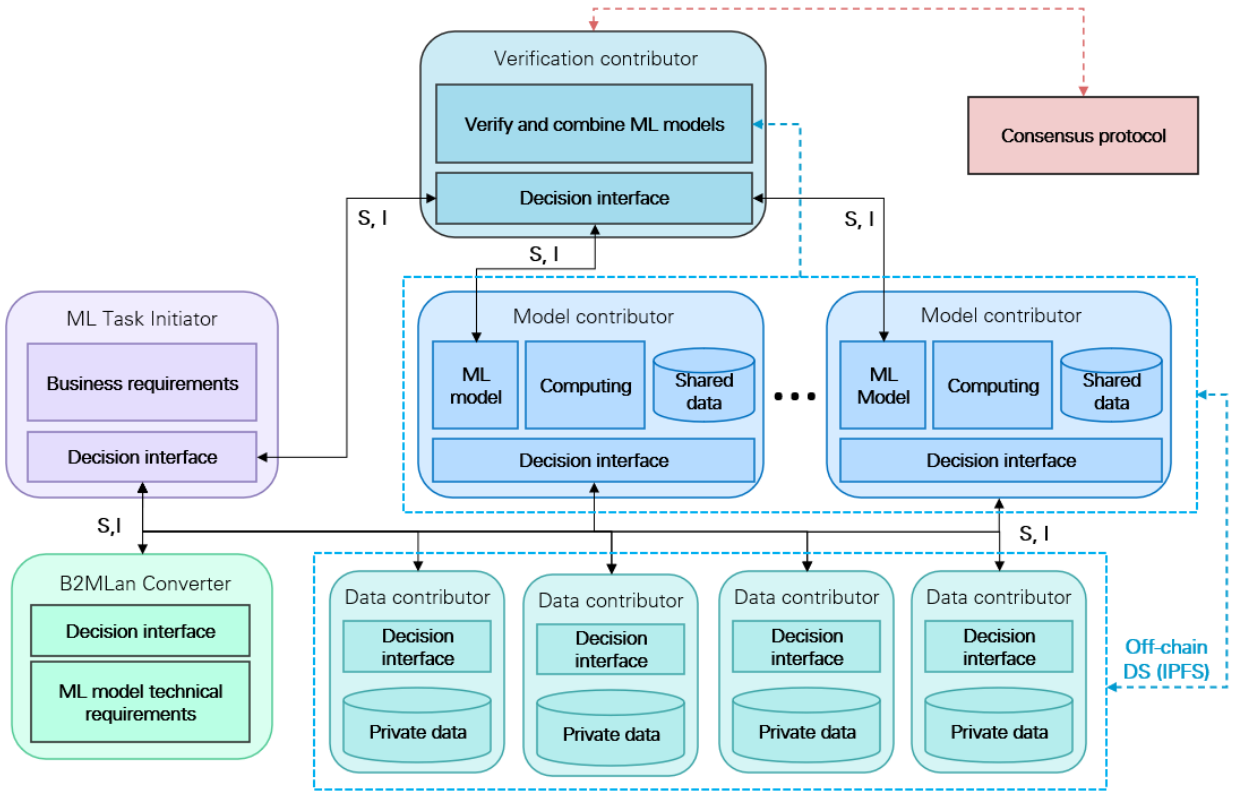


Figure 6.4: Overview of the decentralized ML collaboration paradigm. S - Smart contract, I - Incentive. Inspired from Mendis et al. (2018); Sim et al. (2020); Justin and Harris (2019)

chain on the decentralized storage (DS) IPFS. All uploaded file hashes will be mapped to the specific user on the blockchain. DS and cryptographic techniques will be used to safeguard the shared data and the contributors' interests.

(d) **Model contributor:** responsible for creating and training appropriate ML models based on specific business requirements, technical constraints, and shared datasets. The model contributors train the ML models locally for a given data-driven task using either (1) a specific local data asset, (2) the data shared by the associated ML task initiator, (3) data shared by the data contributors, or (1), (2), and (3) combined. After the *Cumulative Accuracy Profile* (CAP) score is above 80 percent, the local ML models can be classified as successfully trained if the criteria established through smart contracts by the ML task contributors and B2MLans are met. The completion can then be locked (published) onto the blockchain, and the ML model can be shared with the consensus-selected verification contributors via the DS.

(e) **Verification contributors:** provide hardware resources and verify and validate the contributions of the locally trained learning models. Verification contributors are selected through majority voting and proper consensus protocol (2.5). The contributions are verified according to the requirements defined by the B2MLan. They also check whether it contributes to higher accuracy when conducting a model fusion. Once the timeframe allocated to the data-driven task expires, the verification contributor combines all the verified locally trained models to create a fused model deployed to solve the data-driven task.

A transaction between the ML Task initiator and the associated verification contributor is formed for the verified fused ML model. All the contributors are compensated financially, and the ML task initiator gains access to the learning model from IPFS. This is facilitated through a proper and fair incentive mechanism built on immutable blockchain smart contracts. The incentive mechanism defines the rewards proportional to the business value gained from the fused model and is distributed relative to the level of participation after the loop in Figure 6.4 has completed. This way, participants are highly incentivized to collaborate and make contributions.

6.3 Alliance of the BSCM model and the collaborative ML paradigm

The BSCM model in Section 6.1 and collaborative ML paradigm in Section 6.2 can also function together, creating an insight-driven and predictive supply chain network. Each supply chain entity operating as a data contributor can allow its data to be used for ML training in the collaborative paradigm against additional incentives.

By utilizing a more significant amount of data, unknown interrelations and connections may be found and optimized to streamline the entire chain, providing more insight for accurate forecast plans, trend analyses, and demand predictions. Analytics and ML-training outcomes from the supply chains' blockchain data can assist in identifying possible ROI sources and initiate a chance to add value.

6.4 Other benefits and cost savings by implementing the BSCM model

Table 6.5 identifies various feasible value-adding factors and use cases that can be made a reality when connecting the supply chain to a decentralized blockchain. This will open up a new market for industry stakeholders and actors contributing to developing new services and innovative solutions on the decentralized network.

The economic impact of blockchain implementation from a monetary and quantitative perspective is usually kept silent by industry actors who have implemented it. This is a recurring problem that is often addressed in the literature. However, there is a general agreement in the literature that costs related to record processing, data reconciliation, labor, and ERP systems are reasonable starting points when assessing the ROI of a blockchain-based solution (Catalini and Gans (2020); Milani et al. (2016); Wang et al. (2021); Banerjee (2018); Halaburda (2018), ACT-IAC, IBM, et cetera). These are costs defined as direct savings when switching from a database (typically centralized ERP systems) to a decentralized blockchain solution.

The direct cost reductions resulting from reconciliation costs and record processing can be seen from the perspective of three specific use cases in the blockchain: (1) dispute resolution, (2) supply chain visibility, and (3) identity management.

The level of cost savings can be based on these three use cases and varies on the number of records managed by a company/supply chain, the average cost for data reconciliation, the percentage of records conflicting resolutions, ERP systems cost, the average cost to resolve conflicts, and data reconciliation cost.

The equation proposed below can calculate the total cost savings, TCS resulting from improvement in supply chain efficiency. While table 6.2, 6.3, and 6.4 summarizes key inputs and calculations when determining the potential costs and return on investment (ROI) when implementing a BSCM model based on the one proposed in Section 6.1.

$$TCS = A_{total} + B_{total} + C_{total}$$

, where

A_{total} - Total data reconciliation savings
B_{total} - ERP system licence cost reduction
C_{total} - Labor cost savings

Ref	**Metric**	**Calculation**
$A1$	Total records	Input
$A2$	Percentage of disputing records	Input
$A3$	Number of records that need to be reconciled	$A1 * A2$
$A4$	Average cost for resolving conflicts/disputes	Input
$A5$	(Reduction in percent regarding conflicting records with BSCM model)	Input
$A6$	**Reduction in the amount of conflicts**	$A3 * A4 * A5$
$A7$	Avg cost of processing records	Input
$A8$	Reduction in cost per record	Input
$A9$	**Reduced cost of records processing**	$A1 * A7 * A8$
A_{total}	**Total record processing savings**	$A6 + A9$

Table 6.2: Cost savings wrt more record processing

Reference	**Metric**	**Calculation**
$B1$	Avg ERP system cost	Input
$B2$	Percentage ERP system replaced by BSCM model	Input
B_{total}	**ERP system licence cost reduction**	$B1(1 - B2)$

Table 6.3: ERP system cost reduction

REF.	**METRIC**	**CALC.**
$C1$	Number of working hours reconciling records and conflict resolution	Input
$C2$	Avg compensation per hour	Input
$C3$	Opportunity cost (resources that could be spent elsewhere instead)	Input
C_{total}	**Labor cost savings**	$C1 * C2 * C3$

Table 6.4: Labor cost reduction

Benefit	**Description**
Consumer communication, mislabeling, and fraud	The BSCM model improves information sharing with consumers, protects the brand's reputation, reduces counterfeited commodities and mislabeling, and compiles an inventory of relevant energy and material inputs environmental releases (Appendix E). This can improve revenue and reduce costs (due to reduced risk of fraud). A complete record of the seafood E2E from the NFTDT input data (Table 6.1) can thus create a competitive advantage for early adopters of the technology.
Increased revenue	Adopters may increase their revenue due to new market opportunities, new insight, developed innovative solutions, rapid time-to-market, et cetera.
Provenance tracking	The BSCM model allows consumers to back-trace the entire value chain of the salmon securely and efficiently. The consumers may also give instant feedback to the producer. This strengthens the position of the producer towards consumers.
Standardization	Blockchain's innovative approach to data generation and sharing across entities may improve uniformity in how users gather data and fill out forms. Blockchains can aid in the adoption of agreed-upon data management standards. Data-handling standards will drastically reduce the effort spent cleaning and managing data (Casino et al., 2019). Purifying and cleansing data often involves a considerable time commitment and cost in the analytics process.
Time-to-market	Standardization through blockchain can make it easier to construct models with a rapid time-to-market.
Responsiveness and agility	Real-time transactions on the blockchain enable fast decision-making, leading to improved supply chain agility (Wong et al., 2021). .
Information exchange	Breaking down functional silos enables many benefits from a supply chain perspective, such as more transparency, more visibility, improved access to data, stimulation of collaboration and innovation, better decision-making, economies of scale, and efficiency, to name a few. A more extensive list can be viewed in Table C.1.
Reduction of Cybersecurity threats	Reduced risk of data tampering, data loss, data hijacking.
More efficient collaboration	Opening up data through visibility and one single transparent source of truth (non-repudiable audit record) facilitates collaboration between data consumers and data scientists.
Food safety and quality	According to GS1 (2019), the increasing globalization demands seafood to be healthy, sustainable, and safe. The BSCM model can help aquaculture companies speed up recalls ensuring that food posing a health concern is withdrawn from the market as soon as possible. food safety and effective product recalls.
Economies of scale	The decentralized nature of the BSCM model enables economies of scale, allowing smaller organizations to benefit from the same systems as larger ones.
Standardization	A prerequisite for obtaining high-quality data can be done efficiently through this blockchain-based model. Committing data to the blockchain can be done automatically through sensors and IoT devices or manually through application software specifically designed for the stakeholder. Light-touch integrations (e.g., API between blockchain and production control system) is also possible.
Collaboration with regulators	Due to the immutable and trusted data from the BSCM model, increased collaboration with regulators and other authorities allow supply chain stakeholders to ensure that products comply with legal regulations regarding the capturing and sharing of traceable information in the seafood industry, such as EU Council Regulations (EC) 1224/2009 and EC 404/2011.
Environmental footprint	Due to traceability and the non-repudiable audit trail in the BSCM model, efficient and complete Life Cycle Assessments can be conducted (E.1)

Table 6.5: Value-adding benefits resulting from implementing BSCM model

7 Discussion, conclusion, and further work

7.1 Discussion

Further discussion requires a determination of blockchain's technology form. In other words, whether blockchain poses as a complementary or substitute technology in the aquaculture industry. The three forms of technology are public (permissionless), consortium (permissioned), and private (internal). This thesis focuses heavily on blockchain in the public form. However, the utilized form may depend on the industry, company, and objective. Due to the core problem of trust in supply chains, it was reasonable to use a decentralized approach to develop a holistic overview of the problem and solution.

It is also vital to examine the extent challenges, and implications impact the research process. The research process is subject to limitations due to data scarcity. As previously stated, blockchain has recently entered the aquaculture industry. Thus, a lack of available data increased the difficulty of the research process. In addition, companies with integrated blockchain solutions are reluctant to release the following data. However, aquaculture companies also hesitated to share the necessary data. Although this emphasizes the scope of the identified problem, it created an obstacle to proceeding with the initial partnership entered on the premise of this thesis. As a result, a proof of concept could not be conducted due to preoccupation and hesitation in data sharing.

Furthermore, an unexpected implication of knowledge stagnation in literature heavily impacted the speed of the research process. Similarly, the development of new valuable findings consisted of a highly technical format. Thus, technical barriers created significant time delays, which could have been utilized more efficiently.

Moreover, the strengths of this thesis offer valuable insight for industry players. The thesis offers an in-depth and comprehensive literature review of blockchain technology and the aquaculture industry. Before understanding the value delivered by blockchain technology, it was challenging to identify the problem in aquaculture supply chains. However, performing an extensive examination of the value-added created a new understanding of the challenges with the current supply chains. The interview respondents in these companies experienced a similar issue. Thus, the respondent's lack of knowledge surrounding blockchain's value makes it difficult to recognize the problem. Therefore, the findings in this thesis contribute to increased competency by reducing the information gap.

7.2 Conclusion and Further Work

As demonstrated blockchain offers valuable solutions to reduce the need for trust in the supply chain. Creating a decentralized solution where every participant benefits develop opportunities for efficient collaborations and innovative solutions. The strategic aspect of the proposed model and solution can potentially change SME competitiveness and viability in an industry dominated by a few large companies. The value-added of blockchain in the Norwegian aquaculture industry is found in the supply chain. Incorporating blockchain-based solutions into aquaculture supply chains will increase security, transparency, and responsiveness. It can ultimately lead to an end-to-end transformation into a hyper-efficient, cost-saving, and risk-reducing Demand Chain. However, due to data limitations, a proof of concept must be conducted in further work.

References

Anagnostis, A., Papageorgiou, E. and Bochtis, D. (2020), 'Application of artificial neural networks for natural gas consumption forecasting', *Sustainability* **12**(16), 6409.

AquaGen (2021), 'Salmon eggs 2020/2021'.
URL: *https://aquagen.no/en/products/salmon-eggs/product-documentation/*

Attaran, M. (2012), 'Critical success factors and challenges of implementing rfid in supply chain management', *Journal of Supply Chain and Operations Management* **10**, 144–167.

Attaran, M. (2020), 'Digital technology enablers and their implications for supply chain management', *Supply Chain Forum: An International Journal* **21**.

Baah, C., Acquah, I. S. K. and Ofori, D. (2021), 'Exploring the influence of supply chain collaboration on supply chain visibility, stakeholder trust, environmental and financial performances: a partial least square approach', *Benchmarking: An International Journal* .

Bae, J. and Lim, H. (2018), Random mining group selection to prevent 51% attacks on bitcoin, *in* '2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W)', pp. 81–82.

Bai, C. (2019), State-of-the-art and future trends of blockchain based on dag structure, *in* Z. Duan, S. Liu, C. Tian and F. Nagoya, eds, 'Structured Object-Oriented Formal Language and Method', pp. 183–196.

Banerjee, A. (2018), Chapter three - blockchain technology: Supply chain insights from erp, *in* P. Raj and G. C. Deka, eds, 'Blockchain Technology: Platforms, Tools and Use Cases', Vol. 111 of *Advances in Computers*, Elsevier, pp. 69–98.
URL: *https://www.sciencedirect.com/science/article/pii/S0065245818300202*

Banko, M. and Brill, E. (2001), Scaling to very very large corpora for natural language disambiguation, *in* 'Proceedings of the 39th Annual Meeting of the Association for Computational Linguistics', Association for Computational Linguistics, pp. 26–33.
URL: *https://aclanthology.org/P01-1005*

Becker, G. (2008), 'Merkle signature schemes, merkle trees and their cryptanalysis', *Seminararbeit Ruhr-Universität Bochum* .
URL: *https://www.emsec.ruhr-uni-bochum.de/media/crypto/attachments/files/2011/04/becker_1.pdf*

Bentov, I., Lee, C., Mizrahi, A. and Rosenfeld, M. (2014), 'Proof of activity: Extending bitcoin's proof of work via proof of stake [extended abstract]y', *SIGMETRICS Perform. Eval. Rev.* **42**(3), 34–37.
URL: *https://doi.org/10.1145/2695533.2695545*

Bitran, G. R., Gurumurthi, S. and Sam, S. L. (2006), 'Emerging trends in supply chain governance'.

Bitstamp and CoinMetrics (2020), 'The rise of stable coins'.

Bjørgan, E. J., Nordby, T. S. and Pettersen, S. M. (2019), Forutsetninger for datadeling i oppdrettsnæringen, Master's thesis, Nord universitet.

Bodkhe, U., Tanwar, S., Parekh, K., Khanpara, P., Tyagi, S., Kumar, N. and Alazab, M. (2020), 'Blockchain for industry 4.0: A comprehensive review', *IEEE Access* **8**, 79764–79800.

Bulterin, V. (2015), 'On public and private blockchains', *Ethereum Foundation Blog* pp. 1–1.
URL: $https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/$

Buterin, V. (2013), 'Ethereum white paper: A next generation smart contract & decentralized application platform'.
URL: *https://github.com/ethereum/wiki/wiki/white-paper*

Byun, J. and Kim, D. (2015), Oliot epcis: New epc information service and challenges towards the internet of things, *in* '2015 IEEE International Conference on RFID (RFID)', IEEE, pp. 70–77.

Carminati, B. (2009), *Merkle Trees*, Springer US, Boston, MA, pp. 1714–1715.

Casino, F., Dasaklis, T. K. and Patsakis, C. (2019), 'A systematic literature review of blockchain-based applications: Current status, classification and open issues', *Telematics and Informatics* **36**, 55–81.
URL: *https://www.sciencedirect.com/science/article/pii/S0736585318306324*

Catalini, C. and Gans, J. S. (2020), 'Some simple economics of the blockchain', *Communications of the ACM* **63**(7), 80–90.

Chang, S. E. and Chen, Y. (2020), 'When blockchain meets supply chain: A systematic literature review on current development and potential applications', *IEEE Access* **8**, 62478–62494.

Chang, S. E., Chen, Y.-C. and Lu, M.-F. (2019), 'Supply chain re-engineering using blockchain technology: A case of smart contract based tracking process', *Technological Forecasting and Social Change* **144**, 1–11.
URL: *https://www.sciencedirect.com/science/article/pii/S0040162518305547*

Chapman, M. T. (2019), 'Blockchain technology for business: A lenovo point of view'.
URL: *https://lenovopress.com/lp1221.pdf*

Chen, P.-K., He, Q.-R. and Chu, S. (2022), 'Influence of blockchain and smart contracts on partners' trust, visibility, competitiveness, and environmental performance in manufacturing supply chains', *Journal of Business Economics and Management* pp. 1–19.

Chen, S., Shi, R., Ren, Z., Yan, J., Shi, Y. and Zhang, J. (2017), A blockchain-based supply chain quality management framework, *in* '2017 IEEE 14th International Conference on e-Business Engineering (ICEBE)', pp. 172–176.

Chen, Y. (2018), 'Blockchain tokens and the potential democratization of entrepreneurship and innovation', *Business Horizons* **61**(4), 567–575.
URL: *https://www.sciencedirect.com/science/article/pii/S0007681318300375*

Chiesa, A., Green, M., Liu, J., Miao, P., Miers, I. and Mishra, P. (2017), Decentralized anonymous micropayments, *in* J.-S. Coron and J. B. Nielsen, eds, 'Advances in Cryptology – EUROCRYPT 2017', Springer International Publishing, Cham, pp. 609–642.

Choi, R. Y., Coyner, A. S., Kalpathy-Cramer, J., Chiang, M. F. and Campbell, J. P. (2020), 'Introduction to machine learning, neural networks, and deep learning', *Translational Vision Science & Technology* **9**(2), 14–14.

Chowdhury, M. J. M., Colman, A., Kabir, M. A., Han, J. and Sarda, P. (2018), Blockchain versus database: a critical analysis, *in* '2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)', IEEE, pp. 1348–1353.

Choy, M., Leong, H. V. and Wong, M. H. (2000), 'Disaster recovery techniques for database systems', *Communications of the ACM* **43**(11es), 6–es.

Christidis, K. and Devetsikiotis, M. (2016), 'Blockchains and smart contracts for the internet of things', *IEEE Access* **4**, 1–1.
URL: *https://ieeexplore.ieee.org/document/7467408*

Chumbley, A., Moore, K. and Khim, J. (2021), 'Merkle tree'.
URL: *https://brilliant.org/wiki/merkle-tree/*

Cohan, U. W. (2021), 'The double spending problem and cryptocurrencies'.
URL: *https://ssrn.com/abstract=3090174*

Croman, K., Decker, C., Eyal, I., Gencer, A. E., Juels, A., Kosba, A., Miller, A., Saxena, P., Shi, E., Gün Sirer, E., Song, D. and Wattenhofer, R. (2016), On scaling decentralized blockchains, *in* J. Clark, S. Meiklejohn, P. Y. Ryan, D. Wallach, M. Brenner and K. Rohloff, eds, 'Financial Cryptography and Data Security', Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 106–125.

Dean, S. (2021), '$69 million for digital art? the nft craze explained'.
URL: *https://www.latimes.com/business/technology/story/2021-03-11/nft-explainer-crypto-trading-collectible*

Demush, R. (n.d.), 'How companies can leverage private blockchains to improve efficiency and streamline business processes'.
URL: *https://perfectial.com/blog/leveraging-private-blockchains/#modal*

Dolgui, A., Ivanov, D., Potryasaev, S., Sokolov, B., Ivanova, M. and Werner, F. (2020), 'Blockchain-oriented dynamic modelling of smart contract design and execution in the supply chain', *International Journal of Production Research* **58**(7), 2184–2199.
URL: *https://ideas.repec.org/a/taf/tprsxx/v58y2020i7p2184-2199.html*

Domingos, P. (2012), 'A few useful things to know about machine learning', *Communications of the ACM* **55**(10), 78–87.

Du, T. C., Lai, V. S., Cheung, W. and Cui, X. (2012), 'Willingness to share information in a supply chain: A partnership-data-process perspective', *Information & Management* **49**(2), 89–98.

Du, W. D., Pan, S. L., Leidner, D. E. and Ying, W. (2019), 'Affordances, experimentation and actualization of fintech: A blockchain implementation study', *The Journal of Strategic Information Systems* **28**(1), 50–65.
URL: *https://www.sciencedirect.com/science/article/pii/S0963868717302664*

Dutta, P., Choi, T.-M., Somani, S. and Butala, R. (2020), 'Blockchain technology in supply chain operations: Applications, challenges and research opportunities', *Transportation Research Part E: Logistics and Transportation Review* **142**, 102067.
URL: *https://www.sciencedirect.com/science/article/pii/S1366554520307183*

Esmaeilian, B., Sarkis, J., Lewis, K. and Behdad, S. (2020), 'Blockchain for the future of sustainable supply chain management in industry 4.0', *Resources, Conservation and Recycling* **163**, 105064.
URL: *https://www.sciencedirect.com/science/article/pii/S0921344920303815*

EY (2019), 'The norwegian aquacultyre analysis 2019'.

Eyal, I. and Sirer, E. G. (2014), 'How to disincentivize large bitcoin mining pools'.
URL: *https://hackingdistributed.com/2014/06/18/how-to-disincentivize-large-bitcoin-mining-pools/*

Fang, W., Chen, W., Zhang, W., Pei, J., Gao, W. and Wang, G. (2020*a*), 'Digital signature scheme for information non-repudiation in blockchain: a state of the art review', *EURASIP Journal on Wireless Communications and Networking* **2020**.

Fang, W., Chen, W., Zhang, W., Pei, J., Gao, W. and Wang, G. (2020*b*), 'Digital signature scheme for information non-repudiation in blockchain: a state of the art review', *EURASIP Journal on Wireless Communications and Networking* .

FAO (n.d.), 'National aquaculture sector overview norway'.
URL: *http://www.fao.org/fishery/countrysector/naso_norway/en*

Fawcett, S., Williams and Magnan, G. (2004), 'Supply chain trust is within your grasp', *Supply Chain Management Review* **8**, 20–26.

Frankenfield, J. (2020), 'Merkle tree'.
URL: *https://www.investopedia.com/terms/m/merkle-tree.asp*

Frankenfield, J. (2021), 'Hard fork (blockchain)'.

Gonczol, P., Katsikouli, P., Herskind, L. and Dragoni, N. (2020), 'Blockchain implementations and use cases for supply chains – a survey', *IEEE Access* **PP**, 1–1.

Gour, P., Singh, R. and Sohani, N. (2013), 'Interpretive structural modeling of information sharing barriers in indian manufacturing firms', *Journal of Supply Chain Management Systems* **Volume 2**, 26–32.

Gourisetti, S. N. G., Mylrea, M. and Patangia, H. (2020), 'Evaluation and demonstration of blockchain applicability framework', *IEEE Transactions on Engineering Management* **67**(4), 1142–1156.

Greenspan, G. (2015), 'Private blockchains are more than "just" shared databases'.

Gregorio, M. D. (2017), 'Blockchain: A new tool to cut costs', *PwC Middle East* pp. 1–1.
URL: *https://www.pwc.com/m1/en/media-centre/articles/blockchain-new-tool-to-cut-costs.html*

Group, B. (2016), Proof of stake versus proof of work white paper.

Group, B. and Garzik, J. (2016), Public versus private blockchains part 1 : Permissioned blockchains.

GS1 (2019), 'Gs1 foundation for fish, seafood and aquaculture traceability guideline'.

Gupta, S. S. (2017), 'Blockchain', *IBM Onlone (http://www. IBM. COM)* .

Gupta, S. et al. (2020), 'Hfs top 10 enterprise blockchain services 2020'.

Göbel, J. and Krzesinski, A. (2017), Increased block size and bitcoin blockchain dynamics, *in* '2017 27th International Telecommunication Networks and Applications Conference (ITNAC)', pp. 1–6.

Halaburda, H. (2018), 'Blockchain revolution without the blockchain?', *Communications of the ACM* **61**(7), 27–29.

Heilman, E. (2014), One weird trick to stop selfish miners: Fresh bitcoins, a solution for the honest miner (poster abstract), Vol. 8438, pp. 161–162.

Heilman, E., Kendler, A., Zohar, A. and Goldberg, S. (2015), Eclipse attacks on bitcoin's peer-to-peer network, *in* '24th USENIX Security Symposium (USENIX Security 15)', USENIX Association, Washington, D.C., pp. 129–144.
URL: *https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/heilman*

Hoenicke, J. (2021), 'Crypto mempool'.
URL: *https://jochen-hoenicke.de/queue/*

Huynh, T. T., Nguyen, T. D. and Tan, H. (2019), A survey on security and privacy issues of blockchain technology, *in* '2019 International Conference on System Science and Engineering (ICSSE)', pp. 362–367.

Hyperledger (2020), 'Blockchain network', *Hyperledger Fabric v2* pp. 1–1.
URL: *https://hyperledger-fabric.readthedocs.io/en/release-2.2/network/network.html*

IBM (2010), 'The smarter supply chain of the future: Insights from the global chief supply chain officer study'.
URL: *https://www.ibm.com/downloads/cas/AN4AE4QB*

IBMCorp (2018), 'Why new off-chain storage is required for blockchains'.
URL: *https://www.ibm.com/downloads/cas/RXOVXAPM*

Idrees, S. M., Nowostawski, M., Jameel, R. and Mourya, A. K. (2021), 'Security aspects of blockchain technology intended for industrial applications', *Electronics* **10**(8).

Industri, N. (2017), 'Veikart for havbruksnæringen', *Sunn vekst* .

Janssen, M., Charalabidis, Y. and Zuiderwijk, A. (2012*a*), 'Benefits, adoption barriers and myths of open data and open government', *Information Systems Management* **29**(4), 258–268.

Janssen, M., Charalabidis, Y. and Zuiderwijk, A. (2012*b*), 'Benefits, adoption barriers and myths of open data and open government', *Information Systems Management* **29**, 258–268.

Jones, M. N. and Recchia, G. (2009), 'More data trumps smarter algorithms: Comparing pointwise mutual information with latent semantic analysis', *Behavior Research Methods* **41**.

Justin, D. and Harris, B. (2019), Decentralized & collaborative ai on blockchain, *in* 'Proceedings of the 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA', pp. 14–17.

Karame, G. O., Androulaki, E. and Capkun, S. (2012), Double-spending fast payments in bitcoin, *in* 'Proceedings of the 2012 ACM Conference on Computer and Communications Security', CCS '12, Association for Computing Machinery, New York, NY, USA, p. 906–917.
URL: *https://doi.org/10.1145/2382196.2382292*

Kelly, E. and Marchese, K. (2015), 'Supply chains and value webs'.
URL: *https://www2.deloitte.com/us/en/insights/focus/business-trends/2015/supply-chains-to-value-webs-business-trends.html/*

Khan, M. A. and Salah, K. (2018), 'Iot security: Review, blockchain solutions, and open challenges', *Future Generation Computer Systems* **82**, 395–411.
URL: *https://www.sciencedirect.com/science/article/pii/S0167739X17315765*

Khan, S. N., Loukil, F., Ghedira-Guegan, C., Benkhelifa, E. and Bani-Hani, A. (2021), 'Blockchain smart contracts: Applications, challenges, and future trends', *Peer-to-Peer Networking and Applications* .

Kim, H. and Laskowski, M. (2016), Towards an ontology-driven blockchain design for supply chain provenance.

Kim, J.-S. and Shin, N. (2019), 'The impact of blockchain technology application on supply chain partnership and performance', *Sustainability* **11**(21), 6181.

Kosba, A., Miller, A., Shi, E., Wen, Z. and Papamanthou, C. (2016), Hawk: The blockchain model of cryptography and privacy-preserving smart contracts, *in* '2016 IEEE Symposium on Security and Privacy (SP)', pp. 839–858.

Kotha, R. (2017), 'Security risks with public and private blockchains', *Cryptyk* pp. 1–1.
URL: *https://www.cryptyk.io/security-risks-public-private-blockchains/*

Kürschner, C., Condea, C., Kasten, O. and Thiesse, F. (2008), Discovery service design in the epcglobal network, *in* 'The Internet of things', Springer, pp. 19–34.

Kuzincow, J. and Ganczewski, G. (2015), 'Life cycle management as a crucial aspect of corporate social responsibility', *Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu* .

Kwon, I.-W. G. and Suh, T. (2004), 'Factors affecting the level of trust and commitment in supply chain relationships', *Journal of Supply Chain Management* **40**(1), 4–14.
URL: *https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1745-493X.2004.tb00165.x*

Lamport, L., Shostak, R. and Pease, M. (2019), *The Byzantine Generals Problem*, Association for Computing Machinery, New York, NY, USA, p. 203–226.
URL: *https://doi.org/10.1145/3335772.3335936*

Laurent, P., Chollet, T., Burke, M. and Seers, T. (2019), 'The tokenization of assets is disrupting the financial industry'.
URL: *https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/financial-services/lu-tokenization-of-assets-disrupting-financial-industry.pdf*

Lipton, A., Levi, S. and Skadden (2018), 'An introduction to smart contracts and their potential and inherent limitations', *Harvard Law* .
URL: *https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations/*

Lo, S. K., Xu, X., Chiam, Y. K. and Lu, Q. (2017), Evaluating suitability of applying blockchain, *in* '2017 22nd International Conference on Engineering of Complex Computer Systems (ICECCS)', pp. 158–161.

Lopez-Arevalo, I., Aldana-Bobadilla, E., Molina-Villegas, A., Galeana-Zapién, H., Muñiz-Sanchez, V. and Gausin-Valle, S. (2020), 'A memory-efficient encoding method for processing mixed-type data on machine learning', *Entropy* **22**(12), 1391.

Love, D. C., Allison, E. H., Asche, F., Belton, B., Cottrell, R. S., Froehlich, H. E., Gephart, J. A., Hicks, C. C., Little, D. C., Nussbaumer, E. M., Pinto da Silva, P., Poulain, F., Rubio, A., Stoll, J. S., Tlusty, M. F., Thorne-Lyman, A. L., Troell, M. and Zhang, W. (2021), 'Emerging covid-19 impacts, responses, and lessons for building resilience in the seafood system', *Global Food Security* **28**, 100494.
URL: *https://www.sciencedirect.com/science/article/pii/S2211912421000043*

Luo, G., Shi, M., Zhao, C. and Shi, Z. (2020), 'Hash-chain-based cross-regional safety authentication for space-air-ground integrated vanets', *Applied Sciences* **10**(12).
URL: *https://www.mdpi.com/2076-3417/10/12/4206*

MacCarthy, B., Blome, C., Olhager, J., Srai, J. and Zhao, X. (2016), 'Supply chain evolution – theory, concepts and science', *International Journal of Operations & Production Management* **To appear**.

Magazine, B. (2020), 'What is the bitcoin block size limit?'.
URL: *https://bitcoinmagazine.com/guides/what-is-the-bitcoin-block-size-limit*

Martinez, J. (n.d.), 'Understanding proof of stake: The nothing at stake theory'.
URL: *https://www.gemini.com/cryptopedia/double-spend-attacks-bitcoin*

Martinsen, T. and Tetzchner, C. (2018), 'Big data-deling - en undersøkelse av hvordan selskaper kan skape verdi ved deling av big data'.
URL: *https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/2577821*

Marvin, H., Asselt, E., Kleter, G., Meijer, N., Lorentzen, G., Johansen, L.-H., Hannisdal, R., Sele, V. and Bouzembrak, Y. (2020), 'Expert driven methodology to assess and predict the effects of drivers of change on vulnerabilities in a food supply chain: Aquaculture of atlantic salmon in norway as a showcase', *Trends in Food Science & Technology* **103**.

Maurset, I. S. (2018), Lakseprisens effekt på norske havbruksleverandører, Master's thesis, Høgskolen i Molde-Vitenskapelig høgskole i logistikk.

Meijer, C. R. D. (2020), 'Blockchain and interoperability: key to mass adoption'.
URL: *https://www.finextra.com/blogposting/18972/blockchain-and-interoperability-key-to-mass-adoption*

Mendis, G. J., Sabounchi, M., Wei, J. and Roche, R. (2018), 'Blockchain as a service: An autonomous, privacy preserving, decentralized architecture for deep learning', **abs/1807.02515**.
URL: *http://arxiv.org/abs/1807.02515*

Micali, S. and Rivest, R. L. (2002), Micropayments revisited, *in* B. Preneel, ed., 'Topics in Cryptology — CT-RSA 2002', Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 149–163.

Milani, F., García-Bañuelos, L. and Dumas, M. (2016), 'Blockchain and business process improvement', *BPTrends newsletter (October 2016)* .

Miles, C. (2017), 'Blockchain security: What keeps your transaction data safe?'.
URL: *https://www.ibm.com/blogs/blockchain/2017/12/blockchain-security-what-keeps-your-transaction-data-safe/*

Mingxiao, D., Xiaofeng, M., Zhe, Z., Xiangwei, W. and Qijun, C. (2017), A review on consensus algorithm of blockchain, *in* '2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)', pp. 2567–2572.
URL: *https://ieeexplore.ieee.org/abstract/document/8123011*

Morkunas, V. J., Paschen, J. and Boon, E. (2019), 'How blockchain technologies impact your business model', *Business Horizons* **62**(3), 295–306.
URL: *https://www.sciencedirect.com/science/article/pii/S0007681319300096*

Mowi (2020), 'Salmon farming industry handbook'.

Musamih, A., Salah, K., Jayaraman, R., Arshad, J., Debe, M., Al-Hammadi, Y. and Ellahham, S. (2021), 'A blockchain-based approach for drug traceability in healthcare supply chain', *IEEE Access* **9**, 9728–9743.

Muzzy, E. and Anderson, M. (n.d.), 'Avoiding blockchain balkanization'.
URL: *https://consensys.net/research/avoiding-blockchain-balkanization/*

Na, D. and Park, S. (2021), 'Fusion chain: A decentralized lightweight blockchain for iot security and privacy', *Electronics* **10**(4).
URL: *https://www.mdpi.com/2079-9292/10/4/391*

Nakamoto, S. (2008), 'Bitcoin: A peer-to-peer electronic cash system'.

Nayak, K., Kumar, S., Miller, A. and Shi, E. (2016), Stubborn mining: Generalizing selfish mining and combining with an eclipse attack, *in* '2016 IEEE European Symposium on Security and Privacy (EuroS P)', pp. 305–320.

Naz, M., Javaid, N. and Iqbal, S. (2019), Research Based Data Rights Management Using Blockchain Over Ethereum Network, PhD thesis.

Nielsen, C. P., da Silva, E. R. and Yu, F. (2020), 'Digital twins and blockchain – proof of concept', *Procedia CIRP* **93**, 251–255. 53rd CIRP Conference on Manufacturing Systems 2020.
URL: *https://www.sciencedirect.com/science/article/pii/S2212827120307381*

Nowicka, K. (2018), 'Trust in digital supply chain management', *Logistics and Transport* .

Núñez-Merino, M., Maqueira-Marín, J. M., Moyano-Fuentes, J. and Martínez-Jurado, P. J. (2020), 'Information and digital technologies of industry 4.0 and lean supply chain management: a systematic literature review', *International Journal of Production Research* **58**(16), 5034–5061.

Pass, R. and shelat, a. (2015), Micropayments for decentralized currencies, pp. 207–218.

Pawczuk, L., Massey, R. and Schatsky, D. (2018), 'Breaking blockchain open: Deloitte's 2018 global blockchain survey'.
URL: *https://www2.deloitte.com/content/dam/Deloitte/cz/Documents/financial-services/cz-2018-deloitte-global-blockchain-survey.pdf*

Pawczuk, L., Nielsen, J. M., HangSin, P. K. and Hewett, N. (2020), 'Inclusive deployment of blockchain for supply chains: Part 6 – a framework for blockchain interoperability', *World Economic Forum / Deloitte* .

Perboli, G., Musso, S. and Rosano, M. (2018), ‘Blockchain in logistics and supply chain: A lean approach for designing real-world use cases’, *IEEE Access* **6**, 62018–62028.

Pillai, B., Biswas, K. and Muthukkumarasamy, V. (2020), ‘Cross-chain interoperability among blockchain-based systems using transactions’, *The Knowledge Engineering Review* **35**, e23.

Poon, J. and Dryja, T. (2016), The bitcoin lightning network: Scalable off-chain instant payments.
URL: *https://lightning.network/lightning-network-paper.pdf*

PWSAC (2020), ‘Hatchery process’.
URL: *https://pwsac.com/about/hatchery-process/*

Qian, X. A. and Papadonikolaki, E. (2020), ‘Shifting trust in construction supply chains through blockchain technology’, *Engineering, Construction and Architectural Management* .

Qiu, M., Hofmann and Qiu (2018), *Smart Blockchain*, Springer.

Regjeringen (2019), ‘Skattelegging av havbruksvirksomhet’.
URL: *https://www.regjeringen.no/no/dokumenter/nou-2019-18/id2676239/?ch=4*

Ren, Z. and Zhou, P. (2019), ‘What does “scalability” really mean in blockchain?’.
URL: *https://medium.com/vechain-foundation/what-does-scalability-really-mean-in-blockchain-b8b13b3181c6*

Reyna, A., Martín, C., Chen, J., Soler, E. and Díaz, M. (2018), ‘On blockchain and its integration with iot. challenges and opportunities’, *Future Generation Computer Systems* **88**, 173–190.
URL: *https://www.sciencedirect.com/science/article/pii/S0167739X17329205*

Rosic, A. (2020), ‘What is hashing? [step-by-step guide-under hood of blockchain]’.
URL: *https://blockgeeks.com/guides/what-is-hashing/*

Saarikko, T., Westergren, U. H. and Blomquist, T. (2020), ‘Digital transformation: Five recommendations for the digitally conscious firm’, *Business Horizons* **63**(6).
URL: *https://www.sciencedirect.com/science/article/pii/S0007681320300975*

Sanka, A. I., Irfan, M., Huang, I. and Cheung, R. C. (2021), ‘A survey of breakthrough in blockchain technology: Adoptions, applications, challenges and future research’, *Computer Communications* **169**, 179–201.
URL: *https://www.sciencedirect.com/science/article/pii/S0140366421000268*

Sarpong, S. (2014), ‘Traceability and supply chain complexity: Confronting the issues and concerns’, *European Business Review* **26**.

Schneider, S. (2019), ‘How blockchain is making micropayments affordable, finally.’.
URL: *https://provide.services/news/how-blockchain-is-making-micropayments-affordable-finally*

Seang, S. and Torre, D. (2018), ‘Proof of work and proof of stake consensus protocols: a blockchain application for local complementary currencies’.
URL: *https://gdre-scpo-aix.sciencesconf.org/195470/document*

Sedlmeir, J., Buhl, H. U., Fridgen, G. and Keller, R. (2020), ‘The energy consumption of blockchain technology: Beyond myth’, *Business & Information Systems Engineering* .

Seibold, S. and Samman, G. (2015), 'Consensus immutable agreement for the internet of value', *KPMG* .

Sethi, P. and Sarangi, S. R. (2017), 'Internet of things: architectures, protocols, and applications', *Journal of Electrical and Computer Engineering* **2017**.

Shorthouse, D. and Xie, M. (2020), 'Blockchain designed for supply chains: Guardtime supply chain framework', *Guardtime* .

Sim, R. H. L., Zhang, Y., Chan, M. C. and Low, B. K. H. (2020), Collaborative machine learning with incentive-aware model rewards, *in* 'International Conference on Machine Learning', PMLR, pp. 8927–8936.

Simeone, O. (2018), 'A very brief introduction to machine learning with applications to communication systems', *IEEE Transactions on Cognitive Communications and Networking* **4**(4), 648–664.

solid IT gmbh (2022), 'Db-engines ranking'.
URL: *https://db-engines.com/en/ranking*

Srivastava, A., Bhattacharya, P., Singh, A. and Mathur, A. (2018), 'A systematic review on evolution of blockchain generations', **7**, 1–8.

Staff, C. (2021), 'Bitcoin sv (bsv): A bitcoin fork to realize satoshi's alleged vision'.

Stark, J. (2017), 'Making sense of cryptoeconomics', *CoinDesk Tech* pp. 1–1.
URL: *https://www.coindesk.com/making-sense-cryptoeconomics*

Statista (2021), 'Average number of days set as a payment term for business to business (b2b) transactions in various countries in europe from 2015 to 2020'.
URL: *https://www.statista.com/statistics/630045/average-b2b-payment-terms-by-country-western-europe/*

Stuart, F., Verville, J. and Taskin, N. (2012), 'Trust in buyer-supplier relationships: Supplier competency, interpersonal relationships and performance outcomes', *Journal of Enterprise Information Management* **25**.

Sunny, J., Undralla, N. and Madhusudanan Pillai, V. (2020), 'Supply chain transparency through blockchain-based traceability: An overview with demonstration', *Computers & Industrial Engineering* **150**, 106895.
URL: *https://www.sciencedirect.com/science/article/pii/S0360835220305829*

Sunyaev, A. (2020), *Distributed Ledger Technology*, Springer International Publishing, pp. 265–299.

Szabo, N. (1997), 'The idea of smart contracts'.

Taylor, V. (2011), 'Supply chain management: The next big thing'.
URL: *https://www.bloomberg.com/news/articles/2011-09-12/supply-chain-management-the-next-big-thing*

Tjahjono, B., Esplugues, C., Ares, E. and Pelaez, G. (2017), 'What does industry 4.0 mean to supply chain?', *Procedia Manufacturing* **13**, 1175–1182.
URL: *https://www.sciencedirect.com/science/article/pii/S2351978917308302*

Tudón, G. G. A. H. J. (2018), 'A memo on the proof-of-stake mechanism'.
URL: *https://arxiv.org/pdf/1807.09626.pdf*

Tveterås, R., Reve, T., Haus-Reve, S., Misund, B. and Blomgren, A. (2019), 'En konkurransedyktig og kunnskapsbasert havbruksnæring', *Handelshøgskolen BI, Oslo. Rapport* .

Tveterås, R., Reve, T., Haus-Reve, S., Misund, B. and Blomgren, A. (2019), 'En konkurransedyktig og kunnskapsbasert havbruksnæring', *Handelshøyskolen BI* .

Tyndall, G., Gopal, C., Partsch, W. and Kamauff, J. (1998), 'Supercharging supply chains : new ways to increase value through global operation excellence'.
URL: *http://worldcat.org/isbn/0471254371*

Veskus, K. and Milani, F. P. (2018), Ethereum versus fabric – a comparative analysis.

Vieira, S., Lopez Pinaya, W. H. and Mechelli, A. (2020), Chapter 1 - introduction to machine learning, *in* A. Mechelli and S. Vieira, eds, 'Machine Learning', Academic Press, pp. 1–20.

Villena, V., Revilla, E. and Choi, T. (2011), 'The dark side of buyer-supplier relationships: A social capital perspective', *Journal of Operations Management* **29**, 561–576.

Vogel, G. M. (2015), 'The trusted advisor', *Public Integrity* **17**(2), 221–222.

Vranken, H. (2017), 'Sustainability of bitcoin and blockchains', *Current Opinion in Environmental Sustainability* **28**, 1–9. Sustainability governance.
URL: *https://www.sciencedirect.com/science/article/pii/S1877343517300015*

Wang, J. and Wang, H. (2019), Monoxide: Scale out blockchains with asynchronous consensus zones, *in* '16th USENIX Symposium on Networked Systems Design and Implementation (NSDI 19)', USENIX Association, Boston, MA, pp. 95–112.
URL: *https://www.usenix.org/conference/nsdi19/presentation/wang-jiaping*

Wang, L., Luo, X. R., Lee, F. and Benitez, J. (2021), 'Value creation in blockchain-driven supply chain finance', *Information & Management* p. 103510.
URL: *https://www.sciencedirect.com/science/article/pii/S0378720621000847*

Wang, S., Zhang, Y. and Zhang, Y. (2018), 'A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems', *IEEE Access* **6**, 38437–38450.

Wang, S. et al. (2019), 'Blockchain-enabled smart contracts: Architecture, applications, and future trends', *IEEE Transactions on Systems, Man, and Cybernetics: Systems* **49**(11), 2266–2277.

Wang, Y., Tang, C., Lin, F., Zheng, Z. and Chen, Z. (2019), 'Pool strategies selection in pow-based blockchain networks: Game-theoretic analysis', *IEEE Access* **7**, 8427–8436.
URL: *https://ieeexplore.ieee.org/document/8599183*

Weking, J., Mandalenakis, M., Hein, A., Hermes, S., Böhm, M. and Krcmar, H. (2020), 'The impact of blockchain technology on business models – a taxonomy and archetypal patterns', *Electronic Markets* **30**, 285–305.

Winther, U., Hognes, E. S., Jafarzadeh, S. and Ziegler, F. (2020), 'Greenhouse gas emissions of norwegian seafood products in 2017', *SINTEF Ocean* .

Wong, L.-W., Tan, G. W.-H., Lee, V.-H., Ooi, K.-B. and Sohal, A. (2021), ‘Psychological and system-related barriers to adopting blockchain for operations management: An artificial neural network approach’, *IEEE Transactions on Engineering Management* pp. 1–15.

Xuan, S., Zheng, L., Chung, I., Wang, W., Man, D., Du, X., Yang, W. and Guizani, M. (2020), ‘An incentive mechanism for data sharing based on blockchain with smart contracts’, *Computers & Electrical Engineering* **83**, 106587.
URL: *https://www.sciencedirect.com/science/article/pii/S0045790619314855*

Yadav, S. and Singh, S. P. (2020), ‘Blockchain critical success factors for sustainable supply chain’, *Resources, Conservation and Recycling* **152**, 104505.
URL: *https://www.sciencedirect.com/science/article/pii/S0921344919304112*

Yafimava, D. (2019), ‘What are consortium blockchains, and what purpose do they serve?’.
URL: *https://openledger.info/insights/consortium-blockchains/*

Yuan, Y., Rong, C. and Zhang, J. (2018), ‘Parallel blockchain: An architecture for cpss-based smart societies’, *IEEE Transactions on Computational Social Systems* **5**, 303–310.

Zeilberger, H. (2019), ‘A simple explanation of zero knowledge proofs’.
URL: *https://medium.com/web3studio/a-simple-explanation-of-zero-knowledge-proofs-ca574092e73b*

Zha, X., Ni, W., Liu, R. P., Guo, Y. J., Niu, X. and Zheng, K. (2019), ‘Survey on blockchain for internet of things’, *Computer Communications* **136**, 10–29.
URL: *https://www.sciencedirect.com/science/article/pii/S0140366418306881*

Zhang, R. and Preneel, B. (2017), Publish or perish: A backward-compatible defense against selfish mining in bitcoin, pp. 277–292.

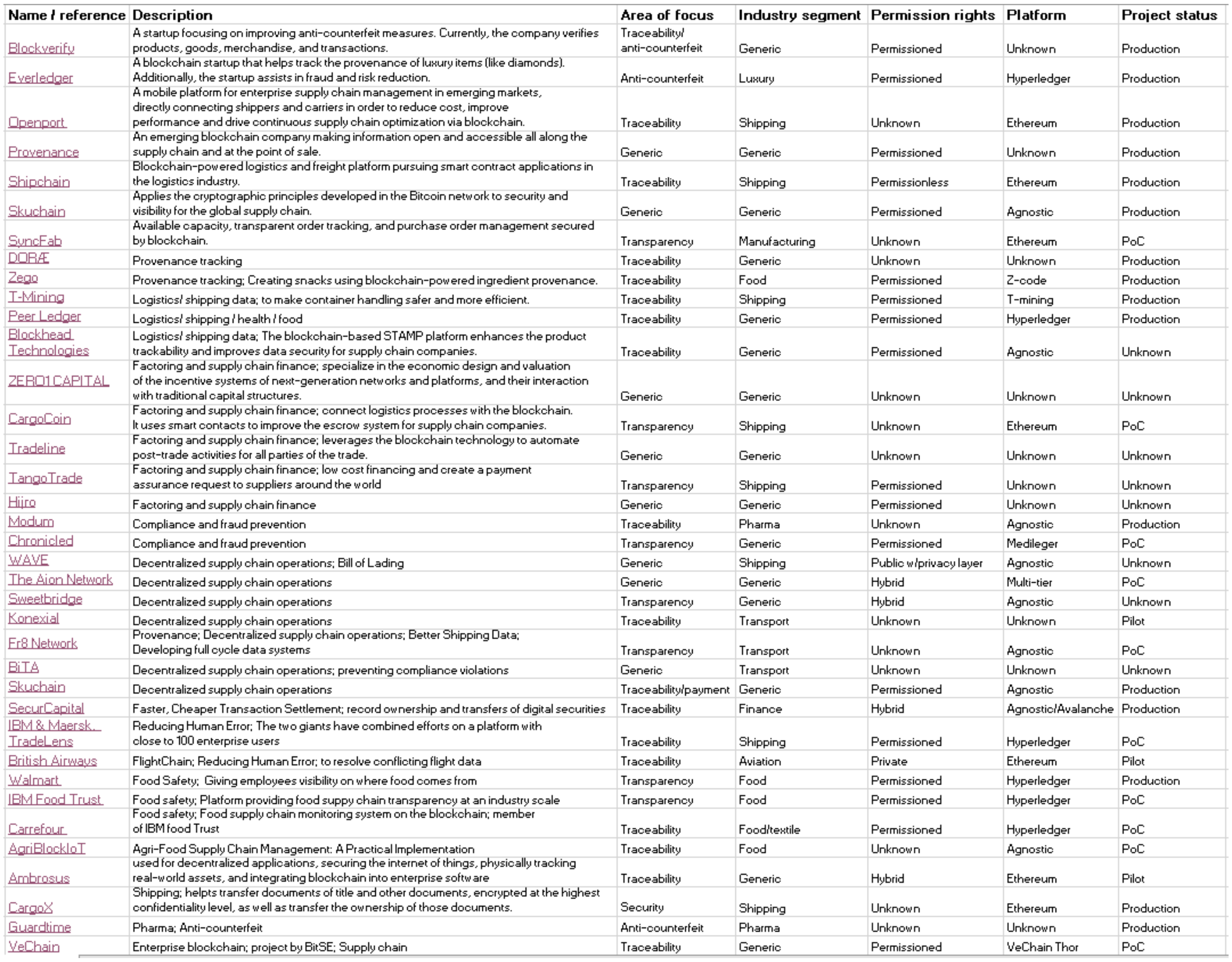
Zhang, R., Xue, R. and Liu, L. (2019), ‘Security and privacy on blockchain’, *ACM Comput. Surv.* **52**(3).
URL: *https://doi.org/10.1145/3316481*

Zheng, A. and Casari, A. (2018), *Feature engineering for machine learning: principles and techniques for data scientists*, O'Reilly Media, Inc..

Zhou, Q., Huang, H., Zheng, Z. and Bian, J. (2020), ‘Solutions to scalability of blockchain: A survey’, *IEEE Access* **8**, 16440–16455.

Zhou, Z.-H., Chawla, N. V., Jin, Y. and Williams, G. J. (2014), ‘Big data opportunities and challenges: Discussions from data analytics perspectives [discussion forum]’, *IEEE Computational Intelligence Magazine* **9**(4), 62–74.

A Appendix



Name / reference	Description	Area of focus	Industry segment	Permission rights	Platform	Project status
Blockverify	A startup focusing on improving anti-counterfeit measures. Currently, the company verifies products, goods, merchandise, and transactions.	Traceability/ anti-counterfeit	Generic	Permissioned	Unknown	Production
Everledger	A blockchain startup that helps track the provenance of luxury items (like diamonds). Additionally, the startup assists in fraud and risk reduction.	Anti-counterfeit	Luxury	Permissioned	Hyperledger	Production
Openport	A mobile platform for enterprise supply chain management in emerging markets, directly connecting shippers and carriers in order to reduce cost, improve performance and drive continuous supply chain optimization via blockchain.	Traceability	Shipping	Unknown	Ethereum	Production
Provenance	An emerging blockchain company making information open and accessible all along the supply chain and at the point of sale.	Generic	Generic	Permissioned	Unknown	Production
Shipchain	Blockchain-powered logistics and freight platform pursuing smart contract applications in the logistics industry.	Traceability	Shipping	Permissionless	Ethereum	Production
Skuchain	Applies the cryptographic principles developed in the Bitcoin network to security and visibility for the global supply chain.	Generic	Generic	Permissioned	Agnostic	Production
SyncFab	Available capacity, transparent order tracking, and purchase order management secured by blockchain.	Transparency	Manufacturing	Unknown	Ethereum	PoC
DORÆ	Provenance tracking	Traceability	Generic	Unknown	Unknown	Production
Zego	Provenance tracking; Creating snacks using blockchain-powered ingredient provenance.	Traceability	Food	Permissioned	Z-code	Production
T-Mining	Logistics/ shipping data; to make container handling safer and more efficient.	Traceability	Shipping	Permissioned	T-mining	Production
Peer Ledger	Logistics/ shipping / health / food	Traceability	Generic	Permissioned	Hyperledger	Production
Blockhead Technologies	Logistics/ shipping data; The blockchain-based STAMP platform enhances the product trackability and improves data security for supply chain companies.	Traceability	Generic	Permissioned	Agnostic	Unknown
ZERO1 CAPITAL	Factoring and supply chain finance; specialize in the economic design and valuation of the incentive systems of next-generation networks and platforms, and their interaction with traditional capital structures.	Generic	Generic	Unknown	Unknown	Unknown
CargoCoin	Factoring and supply chain finance; connect logistics processes with the blockchain. It uses smart contacts to improve the escrow system for supply chain companies.	Transparency	Shipping	Unknown	Ethereum	PoC
Tradeline	Factoring and supply chain finance; leverages the blockchain technology to automate post-trade activities for all parties of the trade.	Generic	Generic	Unknown	Unknown	Unknown
TangoTrade	Factoring and supply chain finance; low cost financing and create a payment assurance request to suppliers around the world	Transparency	Shipping	Permissioned	Unknown	Unknown
Hijro	Factoring and supply chain finance	Generic	Generic	Permissioned	Unknown	Unknown
Modum	Compliance and fraud prevention	Traceability	Pharma	Unknown	Agnostic	Production
Chronicled	Compliance and fraud prevention	Transparency	Generic	Permissioned	Medileger	PoC
WAVE	Decentralized supply chain operations; Bill of Lading	Generic	Shipping	Public w/privacy layer	Agnostic	Unknown
The Aion Network	Decentralized supply chain operations	Generic	Generic	Hybrid	Multi-tier	PoC
Sweetbridge	Decentralized supply chain operations	Transparency	Generic	Hybrid	Agnostic	Unknown
Konexial	Decentralized supply chain operations	Traceability	Transport	Unknown	Unknown	Pilot
Fr8 Network	Provenance; Decentralized supply chain operations; Better Shipping Data; Developing full cycle data systems	Transparency	Transport	Unknown	Agnostic	PoC
BiTA	Decentralized supply chain operations; preventing compliance violations	Generic	Transport	Unknown	Unknown	Unknown
Skuchain	Decentralized supply chain operations	Traceability/payment	Generic	Permissioned	Agnostic	Production
SecurCapital	Faster, Cheaper Transaction Settlement; record ownership and transfers of digital securities	Traceability	Finance	Hybrid	Agnostic/Avalanche	Production
IBM & Maersk, TradeLens	Reducing Human Error; The two giants have combined efforts on a platform with close to 100 enterprise users	Traceability	Shipping	Permissioned	Hyperledger	PoC
British Airways	FlightChain; Reducing Human Error; to resolve conflicting flight data	Traceability	Aviation	Private	Ethereum	Pilot
Walmart	Food Safety; Giving employees visibility on where food comes from	Transparency	Food	Permissioned	Hyperledger	Production
IBM Food Trust	Food safety; Platform providing food suppy chain transparency at an industry scale	Transparency	Food	Permissioned	Hyperledger	PoC
Carrefour	Food safety; Food supply chain monitoring system on the blockchain; member of IBM food Trust	Traceability	Food/textile	Permissioned	Hyperledger	PoC
AgriBlockIoT	Agri-Food Supply Chain Management: A Practical Implementation	Traceability	Food	Unknown	Agnostic	PoC
Ambrosus	used for decentralized applications, securing the internet of things, physically tracking real-world assets, and integrating blockchain into enterprise software	Traceability	Generic	Hybrid	Ethereum	Pilot
CargoX	Shipping; helpts transfer documents of title and other documents, encrypted at the highest confidentiality level, as well as transfer the ownership of those documents.	Security	Shipping	Unknown	Ethereum	Production
Guardtime	Pharma; Anti-counterfeit	Anti-counterfeit	Pharma	Unknown	Unknown	Production
VeChain	Enterprise blockchain; project by BitSE; Supply chain	Traceability	Generic	Permissioned	VeChain Thor	PoC

Figure A.1: List of several ”supply chain” blockchains

B Appendix

Key Data Elements (KDE) ensure that captured and recorded data can be interpreted by all supply chain partners. Key Data Elements define Who, What, When, Where and Why. Since a lot of the KDEs are expressed as identification keys, also master data (MD) related to these keys will be required. For a trade item class, for example, master data might include the trade item's dimensions, descriptive text, nutritional information (in the case of a food product), and so on. Although master data is static, it can change over time. It is important to refer to the master data that were in effect at the time of the Critical Tracking Event.

WHO	
GLN of party	Used to identify the fishing or farming company that did the first sale. Also used to identify buyers and sellers of fish further downstream.
WHAT	
GTIN +	Global Trade Item Number that identifies the type of trade item.
Batch/lot number	The batch/lot number associates a trade item with information the manufacturer considers relevant for traceability of the trade item. The data may refer to the trade item itself or to items contained in it. In combination with the GTIN the batch/lot number identifies a group of trade item instances.
Serial number	A code, numeric or alphanumeric, assigned to an individual instance of an entity for its lifetime. In combination with the GTIN the batch/lot number identifies exactly one trade item instance.
Quantity	The quantity of the respective trade item.
Net weight	Used to identify the net weight of the trade item. Net weight excludes any packaging materials. Has to be associated with a valid unit of measurement.
SSCC	Serial Shipping Container Code that identifies an individual logistic unit.
WHERE	
GLN of physical location	Used to identify production and inventory locations.
WHEN	
Date and time of Critical Tracking Event (CTE)	E.g. production, shipping, receiving.
WHY	
Business process of Critical Tracking Event (CTE)	Used to record the process context of the critical tracking event. Example: Shipping.
Disposition	Status of the traceable object subsequent to the CTE. Example: Available for sale, quarantined.
Transaction reference	E.g. sales note, PO reference, ...

Table B.1: Critical tracking elements (adapted from GS1 (2019))

Producer(s)	
GLN of aquaculture farm details	Identification of a party that engages in aquaculture or mariculture.
GLN of fish processor	Identification of a party that engages in fish processing.
Batch history dates	
Harvest date(s)	The date or date range period that the fish were harvested.
Production date	The production or assembly date determined by the manufacturer.
First freeze date	The first freeze date is applicable to products that are frozen directly after slaughtering, harvesting, catching or after initial processing of the product. Examples include fresh meat, meat products or fishery products. The first freeze date is determined by the organisation conducting the freezing.
Packing date	The date when the goods were packed as determined by the packager.
Sell by date	The date specified by the manufacturer as the last date the retailer is to offer the product for sale to the consumer. The product should not be merchandised after this date.
Best before date or Use by date	The use by date is the date that determines the limit of safe consumption or use of a product. The best before date signifies the end of the period under which the product will retain specific quality attributes or claims even though the product may continue to retain positive quality attributes after this date.
Catch certificate ID	This attributes contains identification number of a certificate with information demonstrating the legality of the fishery and aquaculture products concerned.
Country of export	Country from which the batch/lot was exported. This is not the same as the country of origin.
Economic zone	Economic zone in which fishery or aquaculture products were caught or cultivated.

Table B.2: Trade item master data - instance/lot level (ILMD) (adapted from GS1 (2019))

C Appendix

Category	Benefits
Political and social	More transparency
	Democratic accountability
	More participation and self-empowerment of citizens (users)
	Creation of trust in government
	Public engagementScrutinization of data
	Equal access to data
	New governmental services for citizens
	Improvement of citizen services
	Improvement of citizen satisfaction
	Improvement of policy-making processes
	More visibility for the data provider
	Stimulation of knowledge developments
	Creation of new insights in the public sector
	New (innovative) social services
Economic	Economic growth and stimulation of competitiveness
	Stimulation of innovation
	Contribution toward the improvement of processes, products, and/or services
	Development of new products and services
	Use of the wisdom of the crowds: tapping into the intelligence of the collective
	Creation of a new sector adding value to the economy
	Availability of information for investors and companies
Operational and technical	The ability to reuse data/not having to collect the same data again and counteracting unnecessary duplication and associated costs (also by other public institutions)
	Optimization of administrative processes
	Improvement of public policies
	Access to external problem-solving capacity
	Fair decision-making by enabling comparison
	Easier access to data and discovery of data
	Creation of new data based on combining data
	External quality checks of data (validation)
	Sustainability of data (no data loss)
	The ability to merge, integrate, and mesh public and private data

Table C.1: Overview of benefits of open data. Adapted from Janssen et al. (2012*a*)

Category	Barriers
Institutional	Emphasis of barriers and neglect of opportunities
	Unclear trade-off between public values (transparency vs. privacy values)
	Risk-averse culture (no entrepreneurship)
	No uniform policy for publicizing data
	Making public only non-value-adding data
	No resources with which to publicize data (especially small agencies)
	Revenue system is based on creating income from data
	Fostering local organizations' interests at the expense of citizen interests
	No process for dealing with user input
	Debatable quality of user input
Task complexity	Lack of ability to discover the appropriate data
	No access to the original data (only processed data)
	No explanation of the meaning of data
	No information about the quality of the open data
	Apps hiding the complexity but also potential other use of open data
	Duplication of data, data available in various forms, or before/after processing resulting in discussions about what the source is
	Difficulty in searching and browsing due to no index or other means to ensure easy search for finding the right data
	Even if data can be found, users might not be aware of its potential uses
	Data formats and datasets are too complex to handle and use easily
	No tooling support or helpdesk
	Focus is on making use of single datasets, whereas the real value might come from combining various datasets
	Contradicting outcomes based on the use of the same data
	Invalid conclusions
Use and participation	No incentives for the users
	Public organizations do not react to user input
	Frustration at the existence of too many data initiatives
	No time to delve into the details, or no time at all
	Having to pay a fee for the data
	Registration required before being able to download the data
	Unexpected escalated costs
	No time to make use of the open data
	Lack of knowledge to make use of or to make sense of data
	Lack of the necessary capability to use the information
	No statistical knowledge or understanding of the potential and limitations of statistics
	Threat of lawsuits or other violations
Legislation	Privacy violation
	Security
	No license for using dataLimited conditions for using data
	Dispute and litigations
	Prior written permission required to gain access to and reproduce data
	Reuse of contracts/agreements
Information Quality	Lack of information
	Lack of accuracy of the information
	Incomplete information, only part of the total picture shown or only a certain range
	Obsolete and non-valid data

Table C.2: Adoption barriers for not publicizing data. Adapted from Janssen et al. (2012*a*)

Category	Barriers
Technical	Unclear value: information may appear to be irrelevant or benign when viewed in isolation, but when linked and analyzed collectively it can result in new insights Too much information to process and not sure what to look at [Essential] Information is missing Similar data stored in different systems yields different results Data must be in a well-defined format that is easily accessible: while the format of data is arbitrary, the format of data definitions needs to be rigorously defined Absence of standards No central portal or architecture No support for making data available Lack of meta standards No standard software for processing open data Fragmentation of software and applications Legacy systems that complicate the publicizing of data

Table C.3: (Contined) Adapted from Janssen et al. (2012*a*)

D Appendix

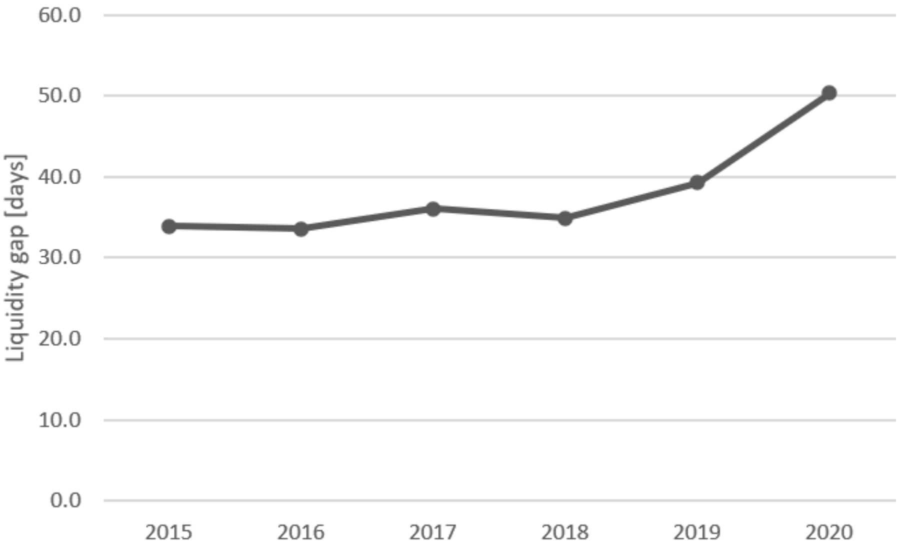


Figure D.1: Average number of days set as a payment term for business to business (B2B) transactions in various countries in Europe from 2015 to 2020. Based on data from Statista.

E Appendix

The aquaculture industry wants sustainable operations and earnings. Today, data is spread over many different systems and silos, incurring high costs in time, data collection, reconciliation, and verification. The aquaculture industry must report to regulatory bodies due to comprehensive legislation (e.g., the Pollution Control Act) and various other interest bodies. Connecting various stakeholders and aquaculture companies to the blockchain-based SCM model in Figure 6.1 brings transparency and end-to-end visibility across the supply chain. Producers, distributors, and retailers can document and commit the environmental character of their products to the blockchain. Supply chain participants and end-users/consumers can then assess environmental impacts associated with all the life cycle stages of products and materials required along the supply chain. See Figure E.1. Life Cycle Assessments (LCA) help decision-makers choose sustainable options, which is becoming increasingly crucial for corporate social responsibility (Kuzincow and Ganczewski, 2015), see the proposed solution in Appendix E. A complete record of the seafood E2E from the NFTDT input data (Table 6.1) can thus create a competitive advantage for early adopters.

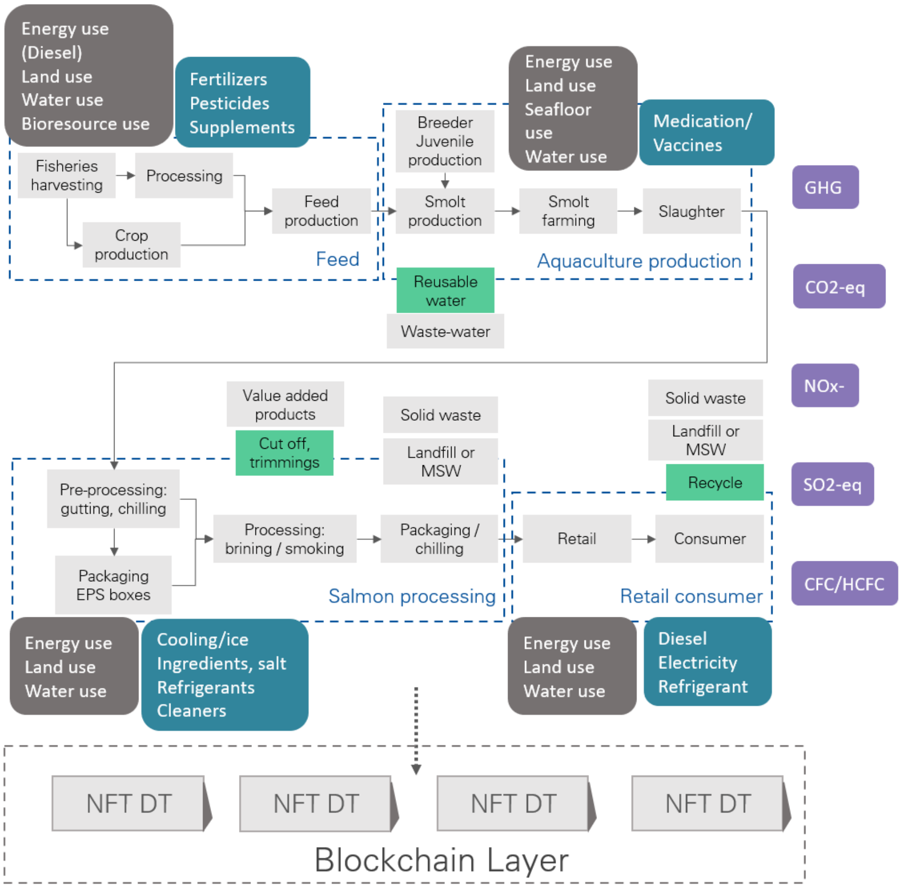


Figure E.1: Flow diagram of aquaculture salmon production and output emissions (based on Winther et al. (2020)) tracked by NFTDTs

F Appendix

The blockchain architecture and layers can be viewed in Figure F.1. The blockchain architecture will differentiate according to choice of method and implementation in terms of hardware, data, network, consensus, and application layer. Note that the different layers affect each other and are connected. The figure also shows where the transaction and information flow interaction between the supply chain and blockchain.

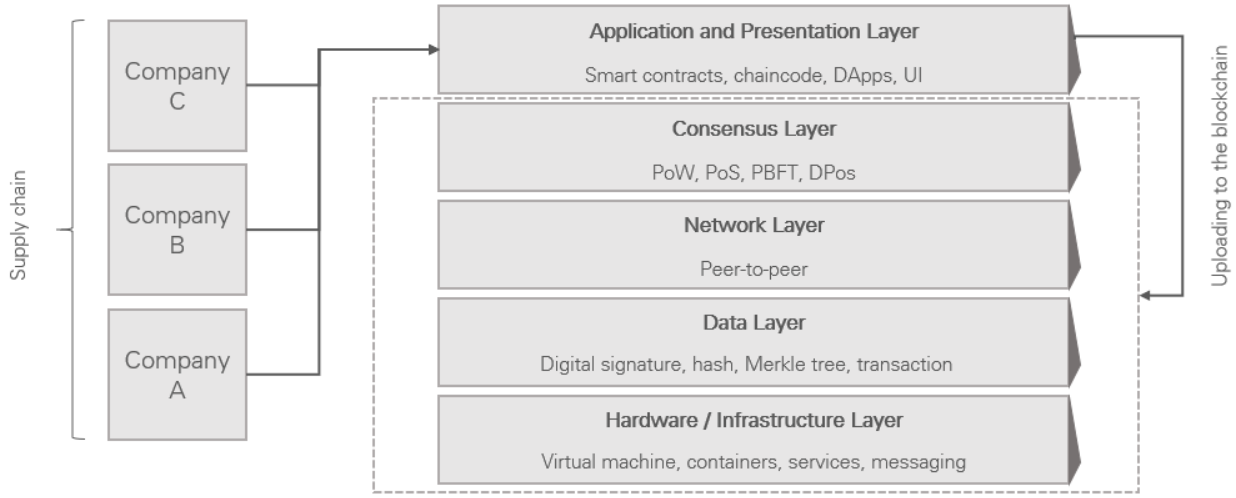

Supply chain
Company C
Company B
Company A
Application and Presentation Layer
Smart contracts, chaincode, DApps, UI
Consensus Layer
PoW, PoS, PBFT, DPos
Network Layer
Peer-to-peer
Data Layer
Digital signature, hash, Merkle tree, transaction
Hardware / Infrastructure Layer
Virtual machine, containers, services, messaging
Uploading to the blockchain

Figure F.1: Blockchain layer architecture

G Appendix

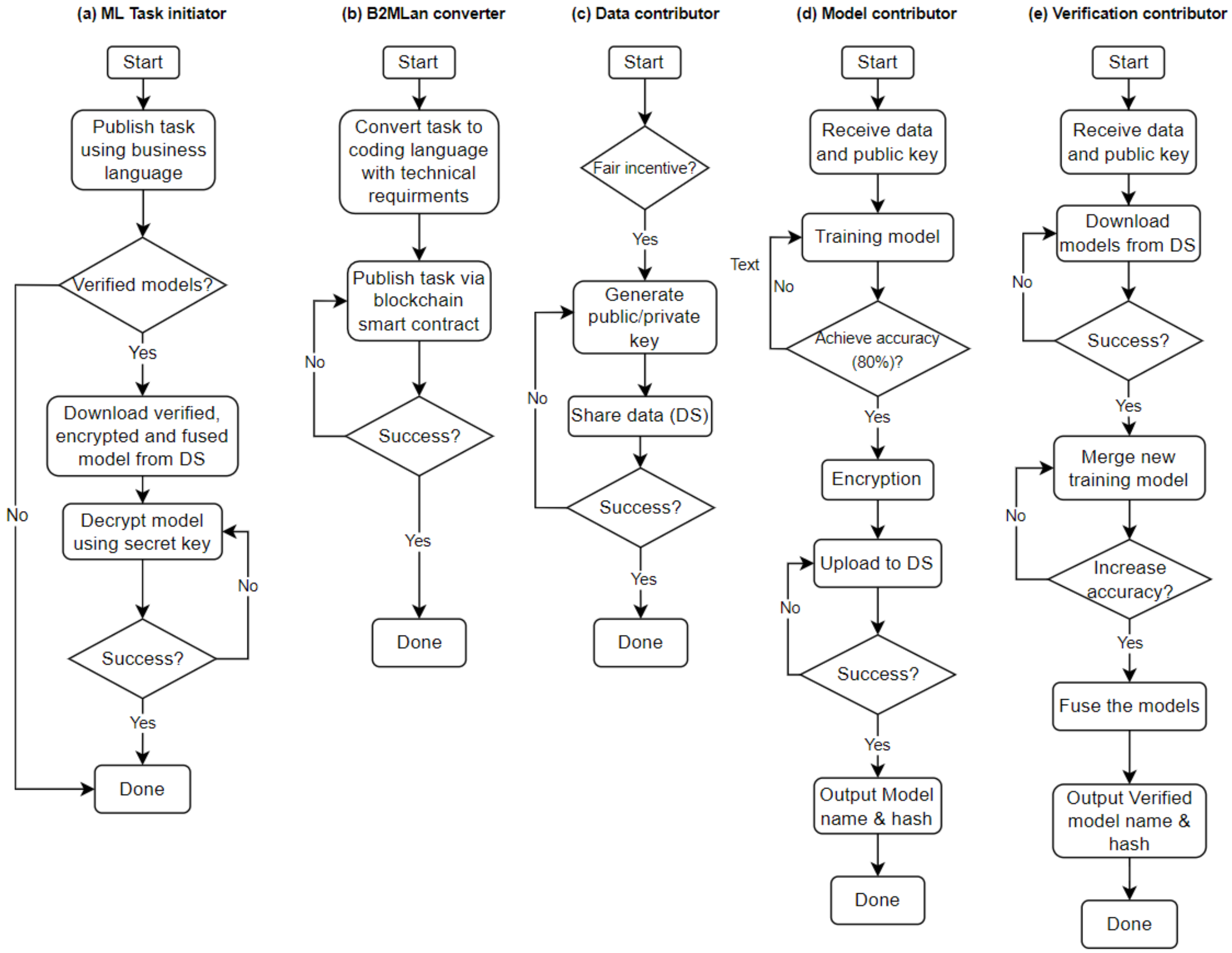


Figure G.1: Schematic diagram showing workflows for (a) ML task initiator, (b) B2MLan converter, (c) data contributor, (d) model contributor, and (e) verification contributor.

H Appendix

Differentiator	**Database**	**Blockchain**
Network	Centralized; client server based	Decentralized; peer-to-peer cross-server network
Storage	Data is stored on central server	Data is stored as blocks in each node in the network
Data Integrity	Transactions stored in a typical database system can be changed or deleted anytime, whether on purpose or as a result of hacking.	All transactions stored on a Blockchain are immutable; records can only be appended (updated), and all nodes must respectively record the event and be in consensus.
Cyber Security & Cryptography	Due to a single point of failure and the lack of cryptographic encryption by default, the system is vulnerable.	Every transaction must be digitally signed using public-private cryptography; a single point of failure cannot corrupt the system, and all data is encrypted.

Table H.1: Traditional distributed databases versus Blockchain-based DLT system: how a distributed database allows multiple parties to transfer, store, and protect sensitive data/information in a space called blocks.

NTNU

Norwegian University of
Science and Technology