Master's thesis

NTNU
Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

Terje W. Dahl

Combatting falsified and substandard pharmaceuticals in the supply chains using blockchain technology.

A review of the field and suggestions for further development.

Master's thesis in Information Security
Supervisor: Mariusz Nowostawski
June 2020

NTNU
Norwegian University of
Science and Technology

Sammendrag

Verdens Helseorganisasjon (WHO) har rapportert falske og substandard legemidler i forsyningskjedene i de fleste regioner i verden. Til tross for reguleringer og forbedret teknologi fortsetter dette problemet å representere en alvorlig helsetrussel. Den relativt nye blokkjede-teknologien har blitt foreslått brukt for å bekjempe denne trusselen. Denne oppgaven utforsker problemet ved å sammenfatte forskningen på blokkjede-basert bekjempelse av falske og substandard legemidler i forsyningskjeden. I tillegg forsøker den å integrere forskningsresultater og teori fra relevante disipliner med tanke på å kunne gi råd til utviklere og forskere i feltet.

Det er gjort et litteratursøk ved hjelp av Scopus for å samle relevante publikasjoner. Resultatene har blitt beskrevet og analysert i lys av blokkjede-teori, forsyningskjede teori og forskningsresultater fra nærliggende felt.

Feltet er lite i volum, teoretisk eller konseptuelt i natur og mangler modenhet. 'Private and permissioned' blokkjede-arkitektur dominerer. Den mangfoldige og globale legemiddelindustrien indikerer videre forskning på interoperabilitet mellom forskjellige blokkjeder. Det er ingen klare anbefalinger for en konsensus mekanisme som passer best til problemområdet. Likevel anbefales nøye vurdering av egenskapene til de forskjellige konsensusmekanismene. Utviklere som planlegger å bygge prototyper eller reelle implementasjoner i dette feltet anbefales å gå gjennom rammeverk med klare kriterier for å vurdere om blokkjede-teknologi er best egnet.

Abstract

The World Health Organization has reported falsified and substandard pharmaceuticals in the supply chains in most regions in the world. Despite regulations and improved anti-counterfeit technology, this problem continues to represent a serious threat to public health. The relatively new blockchain technology has been proposed as a factor that can help counter this threat. This thesis explores the problem by reviewing the research field of using blockchain technology to combat falsified and substandard pharmaceuticals in the supply chain. Additionally, it tries to integrate research results and theory from relevant disciplines to make suggestions to developers and researchers in the field.

A literature search using the Scopus search system was conducted to collect relevant papers. The results were described and analysed using theory of blockchain technology, supply chain management and research results from allied research fields.

The research in the field is small in volume, theoretical or conceptual in nature and lack maturity. Private and permissioned blockchain architectures are dominating. The diverse and global pharmaceutical industry suggests further research into interoperability between blockchains. There are no clear suggestions for a consensus mechanism that fits the problem best, although careful consideration of the characteristics of different consensus mechanisms are recommended. Developers planning to build prototypes or real-world implementations in this field should use frameworks with well-defined criteria before they decide if blockchain technology is the best option.

Preface

This thesis is part of a master’s degree program in information security at the Norwegian University of Science and Technology (NTNU), Faculty of Information Technology and Electrical Engineering, Department of Information Security and Communication Technology. It was carried out, part time, during autumn semester 2019 and spring semester 2020.

Acknowledgements

I would like to thank my supervisor Assoc. Prof. Mariusz Nowostawski for guidance during the work with this thesis. I would also like to thank Student-advisor Hilde Bakke for guidance in administrative matters.

Content

List of figures

List of tables

Acronyms

WHO	World Health Organisation
API	Active pharmaceutical Ingredient
SC	Supply chain
SCM	Supply chain management
FSP	Falsified and/or substandard pharmaceuticals
ERP	Enterprise resource planning
GPS	Global positioning systems
RFID	Radio frequency identifications
IoT	Internet of things
PoW	Proof-of-work
PoS	Proof-of-stake
DPoS	Delegated proof-of-stake
BFT	Byzantine Fault Tolerance
FBFT	Practical Byzantine Fault Tolerance

1 Introduction

1.1 Topic

The topic of this thesis is falsified and substandard pharmaceuticals in the supply chain (SC) and how blockchain technology can play a role in mitigating this problem.

1.2 Keywords

blockchain, supply chain, security, anti-counterfeit, pharmaceutical

1.3 Definitions of falsified and substandard pharmaceuticals used in this thesis

Literature referred to in this thesis often use slightly different definitions of falsified and substandard pharmaceuticals (FSP). The World Health Organization (WHO) has recommended the following definitions:

1.3.1 Substandard medical product

> «... these are authorized medical products that fail to meet either their quality standard or their specifications, or both.» [1]

1.3.2 Unregistered/unlicensed medical products

> «Medical products that have not undergone evaluation and/or approval by the national or regional regulatory authority for the market in which they are marketed/distributed or used, subject to permitted conditions under national or regional regulation and legislation.» [1]

1.3.3 Falsified medical producs

> «Medical products that deliberately/fraudulently misrepresent their identity, composition or source.» [1]

In this thesis only pharmaceuticals are considered. The term *falsified and/or substandard* pharmaceutical (FSP) will be used as an umbrella term for all three definitions above. When the distinctions are of importance, the specific definitions above will be used.

1.4 Problem description

The global pharmaceutical SC should ideally transport pharmaceutical products efficiently from the manufacturer to the end user without any possibility of substandard, unregistered, or falsified products reaching the user.

In 2017, the WHO published a report [1] that described a situation very different from the ideal. Substandard or falsified antibiotics were reported in every region of the world, making it a global problem. Another report from WHO [2] estimated that approximately 10,5 % of tested samples from low- and middle-income countries were either substandard or falsified.

The global pharmaceutical SC system is large and complex. There are already technologies that are used to mitigate FSP, but they have limitations. The relatively new blockchain technology has been proposed as a good fit to supply chains including supply chain security. This thesis will review the research field on how blockchain technology can be applied to the pharmaceutical SC to enhance the security and reduce the occurrence of FSP. Based on the findings and discussion, suggestions for developers and researcher trying to build blockchain-supported applications in this field will be presented.

1.5 Justification, motivation, and benefits

The presence of FSP in the supply chain represents a danger to the public if it is as prevalent as WHO has suggested. Patients risk not having any effect from a prescribed treatment. They may be poisoned by an active pharmaceutical ingredient (API) different from the expected or they may receive the wrong dose of an API. If the medication in question is a substandard or falsified antibiotic, increased antibiotic resistance may result. A large prevalence of FSP may also reduce the public's trust in healthcare and cause people to hesitate seeking help when needed. Additionally, legitimate manufacturers whose products are counterfeited risk financial loss. Any technology that can contribute to improved security will be beneficial to the health of patients around the world.

1.6 Research question

The general topic is how blockchain technology can be used to mitigate the presence of FSP in the supply chain. To narrow the focus, this thesis will try to answer the following:

- **RQ:** What research has been done on the topic of using blockchain technology to mitigate FSP in the supply chains? Secondarily, how can the results of this research, together with theory and research from allied fields, inform us about applying this technology for the specific purpose of combating FSP?

1.7 Planned contribution

The contribution of this paper is to review the field, build on what is already known, integrate this knowledge and arrive at conclusions that will be useful for developers and researchers who will implement more effective blockchain-supported solutions in the struggle against FSP.

1.8 How the rest of the thesis is structured

- Chapter 2 first presents research on the extent of FSP. Then a short introduction to research and applications on blockchain technology. A short review of research on blockchain in the supply chains and finally a brief introduction to research addressing blockchain technology in combatting FSP in the supply chains. The rest of the chapter gives background theory of blockchain technology, supply chain management and a brief description of the pharmaceutical industry.
- Chapter 3 describes the research method used. How data was collected, how the data was handled and why. Also, a short description of literature review as a research method and why comparing the results in the field with general theory about blockchains and supply chains can be beneficial.

- Chapter 4 describes the results of the literature review. General descriptions of the included papers, maturity of projects, types of blockchains, and use-cases in the proposals.
- Chapter 5 discusses the results in light of the theory and background material in chapter 2.
- Chapter 6 presents conclusions and recommendation for further work.

2 Background and theory

2.1 Related work

2.1.1 Introduction

A well-known case of a falsified pharmaceutical entering the supply chain is the Avastin event from 2012. [3] The Food and drug administration (FDA) in the US detected falsified versions of bevacizumab[1] and sent out warnings to clinicians and medical facilities. This drug, originally developed and sold by a multinational Swiss pharmaceutical company [4], is an expensive [5], injectable drug used in cancer treatment. The falsified version followed a complex route through several countries and distributers until it ended up in one of the most regulated pharmaceutical supply chains in the world. The investigation and legal proceedings that followed revealed that some of the defendants had bought and sold falsified pharmaceuticals for years and health personnel had falsified documents.

This incident illustrates weaknesses in the supply chain. Even the amateurishly made packaging and labelling did not prevent the falsified products to find their way to the patients because part of the supply chain (some distributers and health personnel) were in on the fraud and a wholesale secondary marked had developed. The high price of the product made it tempting for counterfeiters to produce and equally tempting for others to purchase at a discount price. The end user (patient) did not have an opportunity to authenticate the products. They trusted the medical services that provided the treatment. Another interesting fact about this incident is that there are still many unanswered questions about what exactly happened and who was responsible, something that illustrates poor auditing options.

2.1.2 The extent of the problem

There is a body of primary research articles that can inform us about FSP in different parts of the world.

Counterfeit labelling of erythropoietin in the USA were documented in 2012. Counterfeiters purchased 110 000 vials, changed labelling to increase the marked value and resold it on the grey market [6]. Another example from the American continent is

a study from Columbia that documented in 2017 a counterfeit multivitamin product that caused bleeding disorders in 36 patients. It turned out to contain warfarin, a well-known anticoagulant. [7].

Petersen et al. [8] collaborated with 10 faith-based organisations using a low-cost equipment (Minilab of the Global Pharma Health Fund) to test the feasibility and cost of surveillance for falsified and substandard drugs. A total of 869 samples were collected from 6 African countries and India using the 'mystery shopper' method. 21 of the 869

[1] bevacizumab is the active pharmacological ingredient (API) in Avastin

samples were confirmed to be substandard or counterfeit. Twelve samples did not contain the active pharmaceutical ingredient.

In [9] sampling of paracetamol and cotrimoxazole products from health facilities, pharmacies, ordinary shops and other vendors in the Malawian marked showed the presence of substandard and unregistered products. In another study from Malawi [10]

the researchers collected samples of anti-malarial medicines from licensed and unlicensed markets throughout Malawi that were analysed for the active pharmaceutical ingredients. All samples contained the API's, but 88,4% did not meet the requirements regarding the amount of API (either insufficient or excessive).

Tivura et al. [11] collected samples of artemisinin-based combination antimalarial drugs in central Ghana and analysing the amount of active pharmaceutical ingredients in each sample using chromatographic analysis. 256 samples were collected and approximately 35 per cent were found to be substandard. No counterfeits were detected. In another artemisinin study [12] sampling of artemisinin-containing antimalarial drugs from licensed pharmaceutical outlets were conducted during a short period February-March 2010 in the Kumasi metropolitan area of Ghana. All samples were analysed with chromatography methods. All the brands contained the active pharmaceutical ingredient, but all failed one or several quality tests and were of substandard quality.

A study in Kazakhstan from 2014 sampled four types of anti-tuberculosis drugs from the regular market and conducted quality testing (visual inspection, absorption test and thin-layer chromatography) showing no counterfeits but 19 per cent of the samples failed at least one of the three quality tests. [13] A pilot study from India [14] in 2015 sampled diclofenac products from around northern India and tested the samples using chromatographic methods. Approximately 15 per cent could be characterised as substandard.

The nine papers above were published between 2012 and 2020. Their findings involved different types of drugs. Anti-inflammatory drugs (paracetamol, diclofenac), antimicrobials (artemisinin, cotrimoxazole and others), vitamins, and hormones (erythropoietin). There were examples of both clear-cut falsified and substandard products even if the researchers used different methods, measurement equipment and slightly different definitions.

Other researchers have published reviews to estimate the prevalence of FSP in different parts of the market.

A Peruvian review published in 2016 [15] analysed data from national drug alerts in the period 1997-2014. A total of 1738 cases of falsified medicines were identified. The great majority was found in the legal supply chain. Mori et al. [16] from Tanzania focused mainly on the economic cost of substandard and falsified medicines. They analysed data from regulatory authorities and importers/distributors of pharmaceuticals in Tanzania. Data from all confiscations in the period 2005-2015 were used. More than 5 mill units (pills, capsules, phials etc) of substandard medication was counted together with more than 1 mill units of counterfeits. Most of the confiscated drugs were antibiotics/antimalarials or antiretrovirals. Chiang et al. [17] focused on counterfeit phosphodiesterase-5 inhibitors used to treat erectile dysfunction. It was not a systematic review, but the authors showed that a significant part of PDE5 use is counterfeits. Raman et al. [18] studied the health consequences of counterfeit and substandard drugs. They conducted a review of literature based on a search in the PubMed database. Their research showed that a wide range of different falsified medication had caused serious health damage and death in many different countries.

Kelesidis and Falanges in 2015 [19] reviewed the literature of substandard and falsified antimicrobial drugs. Although the authors reviewed many studies from around the world, the conclusions they could draw were of a more qualitative nature. They found few papers with sufficient methodology to determine prevalence. Some of the problems they encountered were a lack of uniformly used definitions. They did conclude that substandard and falsified drugs were a growing problem in the developing world with considerable consequences for public health. They also found that a low concentration of the active ingredient was the most common reason for low quality.

Koczware & Dressman [20] investigated the prevalence of counterfeit and substandard pharmaceuticals by reviewing published literature between 2007 and 2016 that was searchable in the PubMed database. They analysed research from many countries but could not give clear conclusions regarding worldwide prevalence «With the existing data, it is, therefore, not possible to draw any firm conclusions about the prevalence of counterfeit drugs worldwide.» [20] Several countries had no data published in the scientific literature. They also concluded that there is no scientific basis for the often-quoted global prevalence of 10% counterfeit drugs

The reviews seen together do not provide a robust estimate of the global prevalence of FSP. The often-quoted assumption that approximately 10 percent of pharmaceuticals in poor and medium poor countries are falsified or of poor quality, can be discussed. The problem of FSP is probably a 'moving target' that changes with time, place, and opportunities. Another problem is that researchers are using slightly different definitions and often quite different methods, making them difficult to compare for reviewers.

Regardless of the uncertainty of prevalence, there is sufficient documentation to conclude that FSP represents a serious threat to public health in many parts of the world. This justifies research into technologies that can reduce the problem.

2.1.3 Blockchain technology and early applications

The era of blockchains started in 2008 [21] when a pseudonymous author published a paper describing what was to become Bitcoin. It went unnoticed for some time, but gained significant attention from 2017, something that is reflected in the sharp increase in the value. [22] Bitcoin is a cryptocurrency, a form for decentralized digital money. The application of the underlying technology was focused on financial services like doing payments and storing value.

The research on blockchain technology has increased considerably. A simple search in Scopus using 'blockchain' as a keyword illustrates this in figure 2-1.

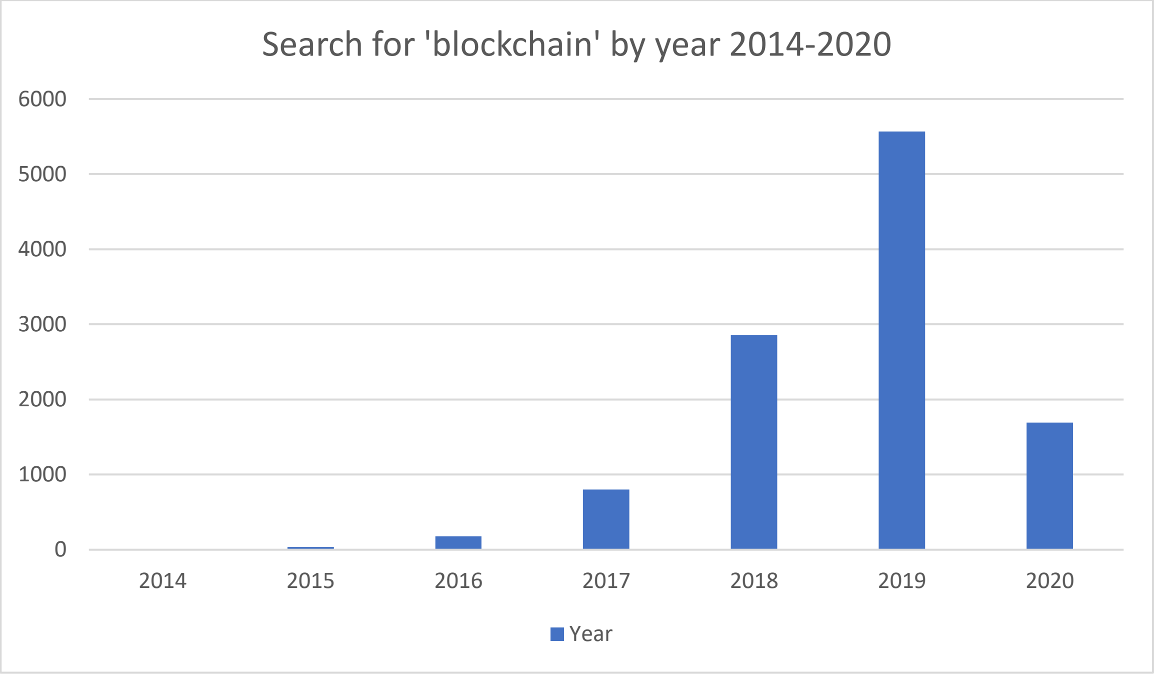

Figure 2-1 Search results for 'blockchain' in Scopus by year

Along with the increase in research there has been an increasing interest in applying this technology to problems outside of finance. When newer and more generalized blockchains like Ethereum [23] and the Hyperledger suite of technologies [24] emerged, the scope of blockchain-based applications became broader.

2.1.4 Applying blockchain technology to supply chain problems

There is already a body of research about applying blockchain technology to different types of supply chain problems.

Queiroz et al. [25] tried to look into the future of blockchain in supply chain management and pointed at the electric power industry, shipment tracking and the pharmaceutical supply chain. They considered the electric power industry as a good candidate for integration with blockchain technology: A decentralized market where producers and consumers in a smart grid negotiate without intermediaries. More generally, how blockchain technology can improve traceability and transparency in supply chains and consequently reduce insurance cost. They concluded that blockchain-supply chain integration is in its early stages but believed that the disruptive effects are already here.

Di Silvestre et al. [26] also argue for use of blockchain technology in the energy sector and points at similarities between energy and digital money.

Wang et al. [27] investigated how blockchain technology will influence future supply chains. They found that little empirical evidence exists that shows how blockchain may disrupt supply chains. They also made the observation that most solutions and proposals choose a permissioned blockchain design because supply chains often include sensitive information and permissioned blockchain can be more effective (larger throughput). They analysed areas where blockchain technology could provide the most value to the supply chain: transparency and traceability, digitalization and disintermediation, improved security through decentralization and improved efficiency through smart contracts.

Casino et al. [28] wrote about transparency and accountability as potential improvements blockchain technology could provide in supply chains. Identification of counterfeit products and enhanced track-and-trace were others. They also considered blockchain technology a good solution when multiple mistrusting parties needed to interact.

Makridakis & Christodoulou [29] emphasized cost-effectiveness through reducing bureaucracy and disintermediation.

Gurtu & Johny [30] expected that blockchain technology in supply chain management would be focused on smart contracts, supply chain finance, increased visibility/traceability and possibly improved security.

Other researchers have focused on more specialized supply chains. The use of blockchain technology in the food and agriculture supply chains have been reviewed by [31], [32], [33], [34] and [35]. Improved traceability and transparency in the food supply chain is among the advantages several find. High integrity that prevent tampering of data is another. Improved customer relations and better collaboration in the supply chains is also emphasized. Typical challenges that the researchers focused on was scalability, interoperability between different ledgers, the need for stakeholders to adapt to the technology, privacy laws and security at the sensor level.

The transport and logistic sectors were reviewed by [36] and [37]. In the transport sector the authors saw blockchain technology as something that could improve trust and data sharing among supply chain actors, but also mentioned the many papers describing potential solutions and very few real-world implementations. Challenges in logistic sector regarding use of blockchain technology was scalability, energy consumption, privacy and immature technology.

A few papers have reviewed blockchain-supported supply chains from an IoT perspective. Lao et al. [38] did a survey on IoT in blockchain systems. Part of their review was relevant for supply chains. They analysed the architecture of IoT-blockchains, compared different consensus algorithms and communications protocols, and finally analysed traffic models of peer-to-peer and blockchain systems. They argued how certain groups of consensus mechanisms fits different use cases in a IoT blockchain. [39] surveyed security issues and blockchain-based solutions for IoT and IIoT (industrial internet of things). Part of this comprehensive survey discusses supply chains and how blockchain technology can be an improvement to existing systems: It can be an immutable alternative to using a centralized database, preventing tampering. It can improve traceability and transparency in a supply chain. Middlemen can be eliminated, thus saving cost. Payments can be conducted within the supply chain using cryptocurrencies. Another potential advantage is better fault tolerance.

2.1.5 Using blockchain technology to combat FSP

The central issue in this thesis is the use of blockchain technology to combat FSP in the supply chains. This is placed in the intersection of other fields that have more research volume. The field is relatively new. In 2016 Mettler et al. [40] discussed briefly the use of blockchain technology to fight counterfeit drugs. In the period 2017-2020 a small number or research papers have been published, including a review [41] that summarize different types of technologies, including blockchains, that can be used to combat FSP in the supply chain. Some design proposals have been made but are mostly of a simplified and theoretical nature. Little has reached real-world testing. Commercial industrial initiatives exist but lack the transparency of peer-reviewed publications.

There is a need to review the literature on this interdisciplinary topic, integrate the field's findings with other related knowledge and explore how this can be applied to create evidence-based applications.

2.2 Blockchain technology theory

An author operating under the pseudonym Satoshi Nakamoto posted a paper *Bitcoin: A Peer-to-Peer Electronic Cash System* in 2008. [21] This paper used a combination of known technologies to describe what was to become Bitcoin [42], the first successful application of blockchain technology.

Blockchain technology is hard to define in one sentence. It may be more instructive to look at elements of this technology one by one before defining it. The descriptions below is based on a simplified public and permissionless[2] blockchain.

2.2.1 A peer-to-peer system

A peer-to-peer system is a type of distributed system. «A distributed system is a collection of autonomous computing elements that appears to its users as a single coherent system.» [43, p. 2] The Bittorrent protocol is one example of a peer-to-peer system. In a purely distributed peer-to-peer system there is no central command or single point of failure".

2.2.2 A decentralized ledger

In accounting the term *ledger* implies keeping two records. One for storing a list of all accounts and their credits and debits. [44] The other keeps track of all transactions during a time period and is used to update the accounts at the end of each time period. A bank or public office in charge of keeping a ledger is an example of a centralized ledger. In a blockchain, every node in the network keep a copy of all transactions that have occurred since the start of the ledger and updates the record every time a list (block) of transactions have occurred. Every node does so by communicating and agreeing with the other nodes and synchronizing its records.

2.2.3 An immutable and append only database

A blockchain that is designed like Bitcoin [42] or Ethereum [23] accepts new transactions that add to the record (or chain of blocks) but it is extremely costly to change the record in retrospect. Anyone can do a transaction and add to the blockchain. There is no administrator that can go back in the record and remove an item.

2.2.4 The blockchain data structure

Part of the reason why a blockchain is capable of being an immutable, append only, decentralized ledger is the data structure it uses. This data structure uses functions called cryptographic hash functions extensively. It is a one-way function that takes in data and outputs a fixed length string also called a hash code. This code can be seen as a 'fingerprint' of a dataset. The chance of finding a different dataset that produces the same hash code is negligible for practical purposes.

[2] 'Public and permissionless' is explained in chapter 2.2.11

2.2.4.1 Hash functions

Figure 2-2 shows the use of hash functions. These functions can be used in combinations.

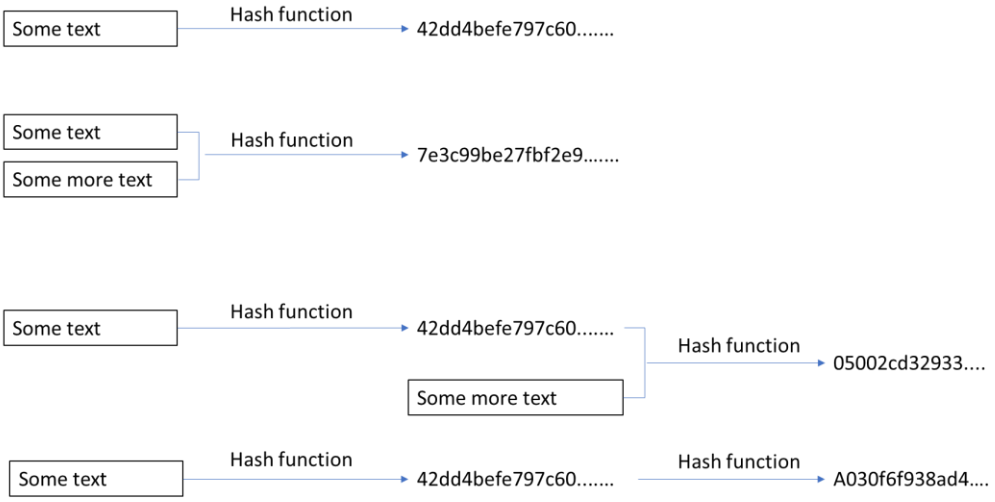

Figure 2-2 Combining hash functions

In figure 2-3 hash functions are used in a hierarchy that is referred to as a Merkle tree. [45]

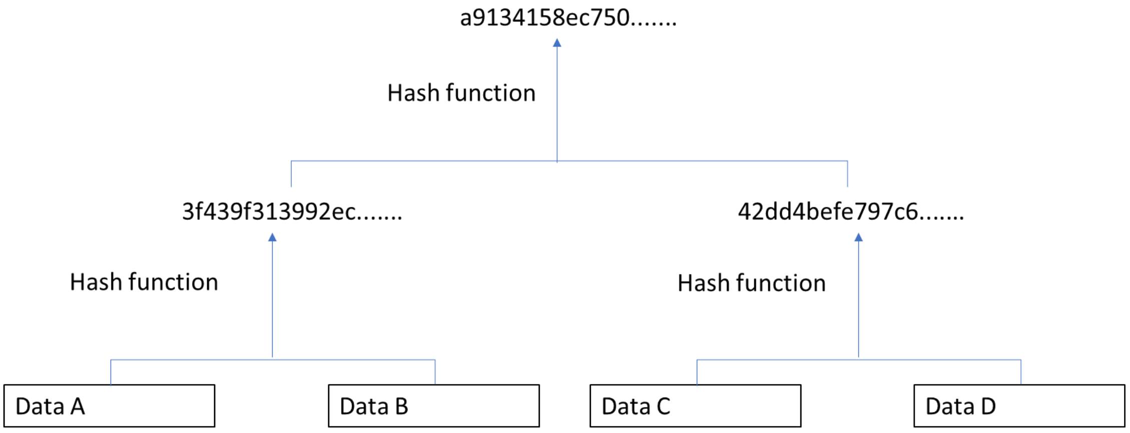

Figure 2-3 Merkle tree

Storing information in a Merkle tree has several advantages. Assuming someone would change the data in Data A. The combined hash of Data A and Data B would not match the hash one step up in the figure. The combined hash of Data C and Data D would still match. The combined hash of the middle layer would not match the root hash. This way one can repeat the hashing and quickly localize where the data has been changes.

Another advantage is that the root hash can be a reference (a hash pointer) to all the data in the tree. It is not necessary to check all data in every leaf to verify that all information is unchanged. If the root hash does not match, something has changes and one knows that the integrity of the tree has been compromised.

Data sets can be chained together by embedding the hash of the previous data set as shown in figure 2-4.

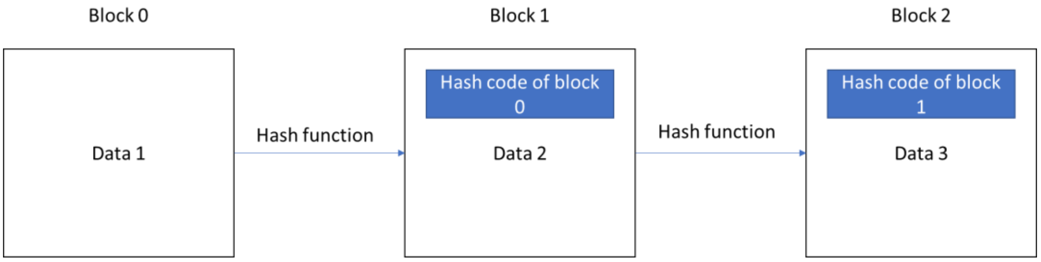

Figure 2-4 Linking blocks of data in a chain

Block 1 contains the hash code of everything from block 0 in addition to its own data (Data 2). Any change of content in each block or a change in the sequence of blocks would easily be detected because the hash values would not match. From block 1, each block contains a hash pointer to the previous block.

2.2.4.2 A simplified blockchain datastructure

It is possible to put together a simplified blockchain data structure by:

- Combining the data structures in figure 2-3 and figure 2-3
- Assuming that Data A, Data B and so on in figure 2-3 represents transactions
- Adding a timestamp in each block.

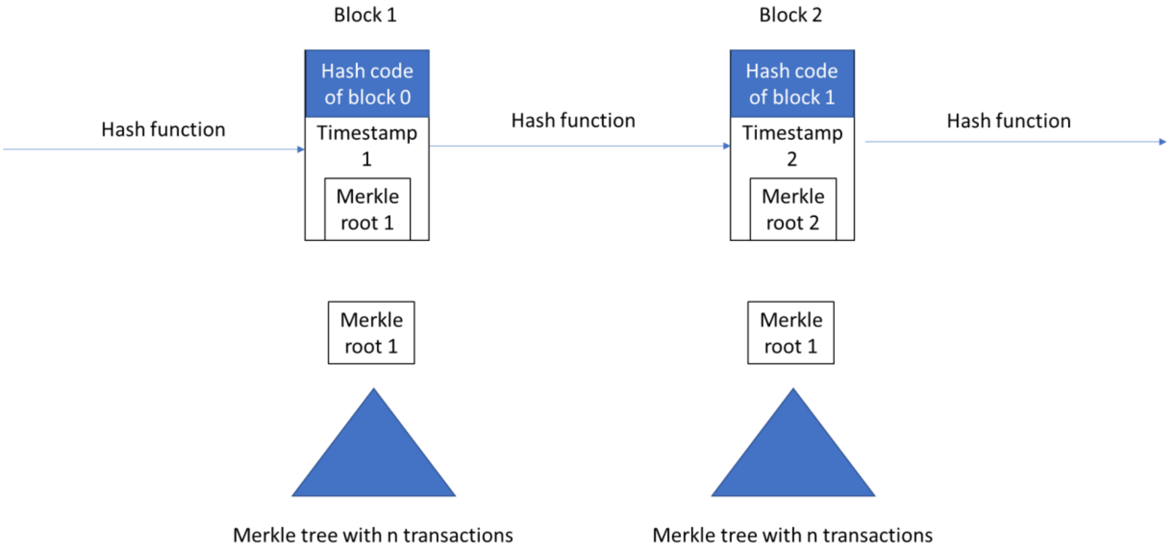

Figure 2-5 Simplified blockchain data structure

In figure 2-5 the base of the triangles represents a set of transactions. The Merkle root of the hierarchically stored transactions match the Merkle root inside the corresponding block. Any changes in the data structure will create a mismatch of hash values and can easily be detected.

2.2.5 Cryptography

2.2.5.1 Symmetric cryptography

Traditional (or symmetric) cryptography (see figure 2-6) required a secure channel for the exchange of a secret password. The sender could then use this password to encrypt a message, send it and the receiver could decrypt the message with the same secret password. A malicious bystander may intercept the message when travelling from sender to receiver, but would not be able to decrypt the message to read it. [46, p. 62] The problem is that the shared secret between sender and receiver must at some point be shared to begin with. This sharing may represent a security risk and be unpractical and slow.

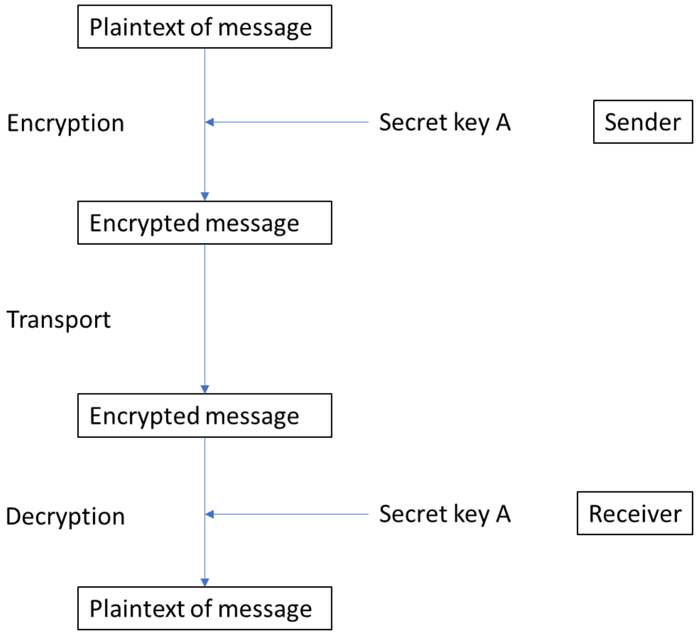

Figure 2-6 Symmetric cryptography

2.2.5.2 Public key cryptography

Public key cryptography is an «asymmetric form for cryptography in which the transmitter of a message and its recipient use different keys (codes), thereby eliminating the need for the sender to transmit the code and risk its interception.» [47] Asymmetric cryptography uses pairs of keys that are mathematically related. One key is called the public key and can be shared without any secrecy. The corresponding private key is kept secret by the owner. Assuming two parties A and B each with their pairs of keys. A has his private key AKprivate and AKpublic. B has her private key BKprivate and BKpublic. If A wants to send a secret message to B, he can find B's public key and use that to encrypt the message. Then use his own private key to encrypt the encrypted message. When B receives the encrypted message, she can use A's public key to decrypt the first layer. Then use her own private key to decrypt the message and read the resulting clear text message. There was no sharing of a secret, B knows that A (or someone who access A's private key) sent the message, she can read the message and any interceptor would not be able to read the message. This is illustrated in figure 2-7 below.

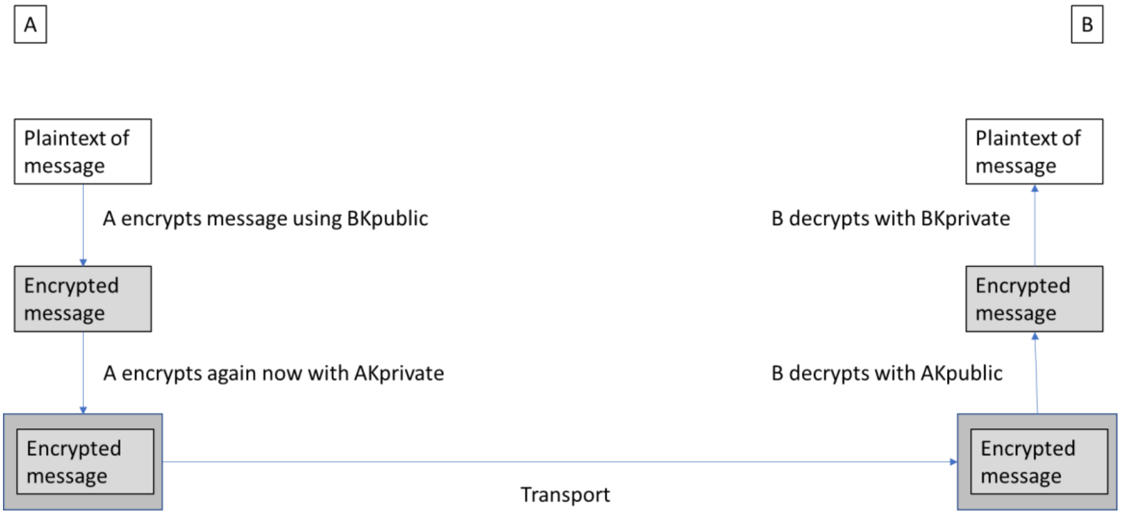

Figure 2-7 Asymmetric cryptography

2.2.6 Transactions

When transactions happen in a blockchain used as a ledger where tokens represent some value, there is a need to keep track of the identify if each account, how much value each account has, the sender, the receiver, how much value is transferred, the time the transaction happened and the sequence of the transactions. Real world blockchains will also include more information.

Public keys or a derivative of them function as 'account numbers'. In a blockchain context the owner of an account uses a digital signature to sign a transaction (like A in figure 2-8) and others can verify the transaction (like B in figure 2-8).

Digital signatures are generally used to authenticate messages without providing confidentiality also shown in figure 2-8. [46, p. 80].

In a distributed ledger there is no central authority that can verify the transactions of behalf of the users. Other participants in the network need to be able to read the transactions and verify that they comply with the protocol.

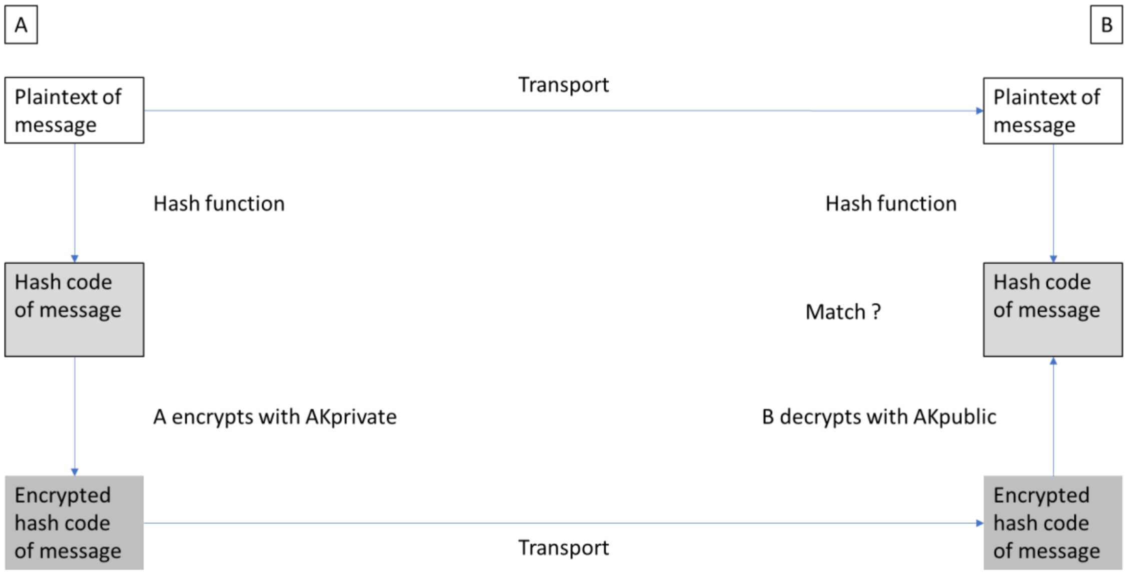

Figure 2-8 Digital signature

2.2.7 Mining

> «The activity of adding a new block to the blockchain-data-structure by solving a hash puzzle is also called mining or block mining» [48, p. 141]

When transactions are executed in a blockchain the transactions are communicated to the nodes in the network through a so-called gossip protocol and collected into a block. There is an ongoing competition to be the one (miner) that gets to do this and receive a reward that functions as an incentive for doing this work. The competition is based on solving a computationally demanding task. The first to solve this problem and communicate it to the network is the miner of that block. The difficulty level of the computationally demanding problem is also embedded in the block. This contributes to the immutability of the blockchain since anyone trying to reverse the transactions must repeat all the work at a cost that will deter attackers from trying.

2.2.8 Distributed consensus

> «Distributed consensus is the major underpinning of a blockchain. This enables a blockchain to present a single version of truth that is agreed upon by all parties without the requirement of a central authority» [49, p. 21]

When the nodes in the network are competing to add the new block of transactions to the chain and broadcasting the result to be the winner of that block's reward, there can be several different solutions at the same time. Assuming a worldwide network of nodes communicating through a gossip or 'best effort' protocol. Some nodes will accept one solution and start the race to mine the next block. Others have chosen another solution and do the same. How will this be decided when the chain splits into a Y-shape? This is also referred to as a fork [50]. Blockchains will let the nodes vote by their actions when they accept a version of the block and start building on top of that. The individual nodes bet on being right. Eventually one version will be the clear winner and the other nodes will follow based on their incentive to maximize their profit. Building blocks on top of a losing branch of the blockchain comes at the cost of solving computationally demanding tasks for no good.

2.2.9 Definitions of blockchain technology

After presenting elements of the blockchain technology two definitions will now make more sense:

> « Blockchain at its core is a peer-to-peer distributed ledger that is cryptographically secure, append-only, immutable (extremely hard to change), and updateable only via consensus or agreement among peers.» [49, p. 16]

> «The blockchain is a purely distributed peer-to-peer system of ledgers that utilizes a software unit that consist of an algorithm, which negotiates the informational content of ordered and connected blocks of data together with cryptographic and security technologies in order to achieve and maintain its integrity.» [48, p. 35]

The previous sections in chapter 2 have presented the elements in the first definition. [49]. The second definition [48] also emphasizes that an important aim of blockchain technology is to achieve and maintain integrity, that is, integrity in a distributed peer-to-peer-network.

2.2.10 Applications

When [21] presented blockchain technology, the aim was to apply it to the financial sector as digital cash. A digital currency that is independent of banks and governments. So far this has been a relative success. The value of all bitcoins are now approximately 168 billion USD. [22] The success of Bitcoin[3] illustrates some applicable use case principles of blockchain technology. It has a build in token that can be a value itself or represent something else. It manages ownership of tokens. Transactions transfer ownership from one account to another in a transparent and secure way. Any activity that needs to transfer ownership may find blockchain technology useful. Another principle is disintermediation. Used as a currency it removes the trusted third part. Transfer of ownership happens without any intermediaries and does not require the participants to trust each other. A system where trust is partly or completely lacking and where stakeholders need to collaborate may be also find this technology useful. Blockchain is distributed. This implies resilience from destruction of parts of the network. There is no 'off button' and consequently no single point of failure. This is useful for systems that need 100% up-time even when parts of the system are down.

Of interest for this thesis is the application in supply chains, and particularly supply chain security. This is a global system of many stakeholder that only trust each other to a certain degree and constantly buy and sell products on their way to the final customer. Cutting cost through intermediation is also a potential benefit. The immutability that blockchains offers creates an audit trail of what actually happened in cases of disputes in a supply chain network, providing non-repudiation.

[3] I am referring to Bitcoin Core. There is also Bitcoin Cash and Bitcoin SV(Satoshi Vision)

2.2.11 Different types of blockchains

In this thesis, blockchains will be classified based on the following definitions:

- «A public blockchain is a blockchain, in which there are no restrictions on reading blockchain data (which still may be encrypted) and submitting transactions for inclusion into the blockchain.»[51]
- «A private blockchain is a blockchain, in which direct access to blockchain data and submitting transactions is limited to a predefined list of entities.» [51]
- «A permissionless blockchain is a blockchain, in which there are no restrictions on identities of transaction processors (i.e., users that are eligible to create blocks of transactions).» [51]
- «A permissioned blockchain is a blockchain, in which transaction processing is performed by a predefined list of subjects with known identities. » [51]

These four definitions constitute two dimensions. Public vs. Private and Permissionless vs. Permissioned as shown in figure 2-9. The result is four types of blockchains. There may be variations and hybrids, but there will fundamentally be four prototypic blockchains with different features. The more 'permissioned' a blockchain is, the more restrictions there are on processing the transactions. The more 'private' a blockchain is, the more restrictions there are on reading the data on the chain and proposing transactions. As [48, p. 216] explains, the two dimensions are connected to read and write access to the blockchain and ultimately connected to the conflicts between transparency vs privacy and security vs. speed.

A private and permissioned blockchain is the most restrictive. A public and permissionless is the most liberal. Bitcoin is an example of a public and permissionless blockchain. Anyone can read the blockchain data and create transactions that may or may not be included in the blockchain. Anyone can process the transactions as miners. Depending of the use-case the different designs will be more or less fitting.

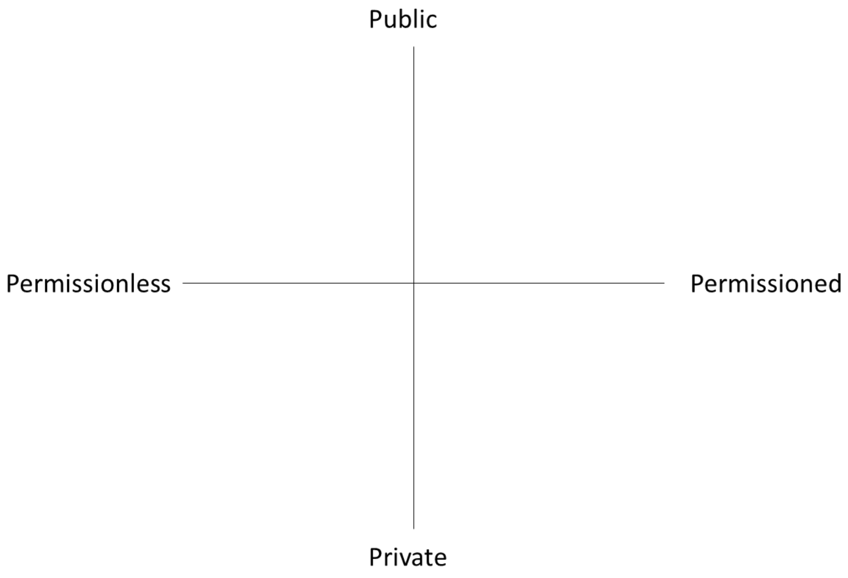

Figure 2-9 Categories of blockchains

2.2.12 Different consensus protocols

When miners are using their processing power to find the solution to the hash puzzle, work is done. This arrangement is called proof-of-work (PoW) and is referred to as a consensus protocol [50]. PoW is only one of many possible consensus protocols. As examples Bitcoin and Ethereum uses PoW, but Ethereum will probably transition to a proof-of-stake (PoS). EOS, a newer blockchain uses a variation of PoS called delegated proof of stake (DPoS), a variation of PoS. The choice of consensus protocol will affect the features of a blockchain and should be taken into consideration when building or choosing a blockchain technology for a particular use-case.

2.2.13 The CAP theorem

The CAP theorem states that there is a trade-off between consistency, availability and partition tolerance in an unreliable distributed system. [52] Since blockchain technology is a distributed system, the theorem will apply.

In a blockchain context consistency means that all nodes are synchronized so each have a copy of the blockchain. Availability means that the system is accessible and responds as required at all times. Partition tolerance means that the distributed system will continue to function even if parts of it is down. [49, p. 11].

Two mutually exclusive transactions in the blockchain can exist at the same time if one node in the network receives a transaction to send $1 from A to B and another node receives a transaction to send $1 from A to C when A only has $1 on the account. This illustrates the double spending problem. Unconfirmed transactions may be inconsistent, but eventually only one of the transactions will be confirmed and the blockchain will be consistent. [51]

Another formulation related to the CAP theorem in blockchains is The Scalability Trilemma, originally coined by one of Ethereum’s founders (Vitalik Buterin) that says that it is not possible to maximize decentralization, scalability, and security at the same time. Blockchains like Bitcoin and Ethereum have prioritized security and decentralization. As a consequence of this they have limited scalability. Other blockchains like Hyperledger Fabric have prioritized scalability measured in transactions per second and security. [53]

2.3 Supply chain management theory

2.3.1 Supply Chain

Massive numbers of products are manufactured and transported to customers every day. This system spans the globe in a complex network where the goods may change hands and owners many times before the end customer receives it. This is referred to as a supply chain. One of the simpler definitions of a supply chain is «... a chain of interconnected links that facilitates the movement of supplies. » [54, p. 3] Another definition is «... the network of all entities involved in producing and delivering a finished product to the final customer. » [55, p. 3]

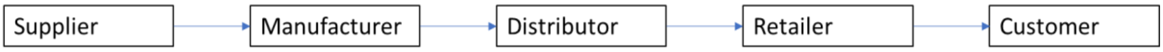

Figure 2-10 Supply chain, simple model

Figure 2-10 shows a model where one single supplier supplies raw materials to a manufacturer. This manufacturer transforms the raw materials into a product that is distributed to a retailer and sold to a customer.

In supply chain terminology there are two directions something can move. Downstream towards the customer or upstream towards the supplier (figure 2-11).

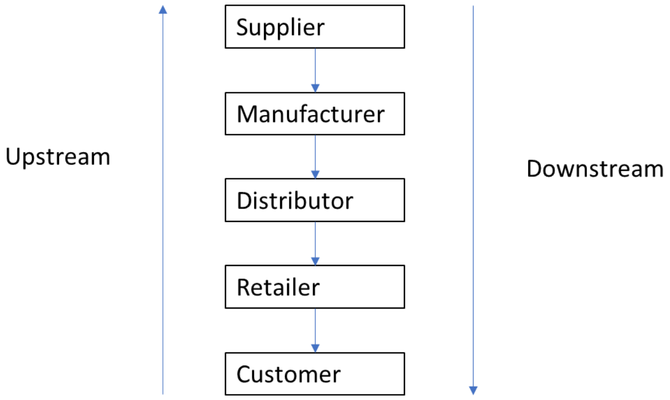

Figure 2-11 Directions in a supply chain

2.3.2 Supply Chain management

In real life, the process is much more complicated. This has led to an entire discipline focused on managing supply chains. Supply Chain Management (SCM) is «... the design and management of flows of products, information, and funds throughout the supply chain. » [55, p. 3]

Physical products will mainly move downstream towards customers but may move in the opposite directions in case of service, recalls, defect products or for other reasons. The same can be said of money. It mainly moves from the customer and upstream toward the suppliers, but money can also move towards the customer in case of a returned product. The information moves in both directions.

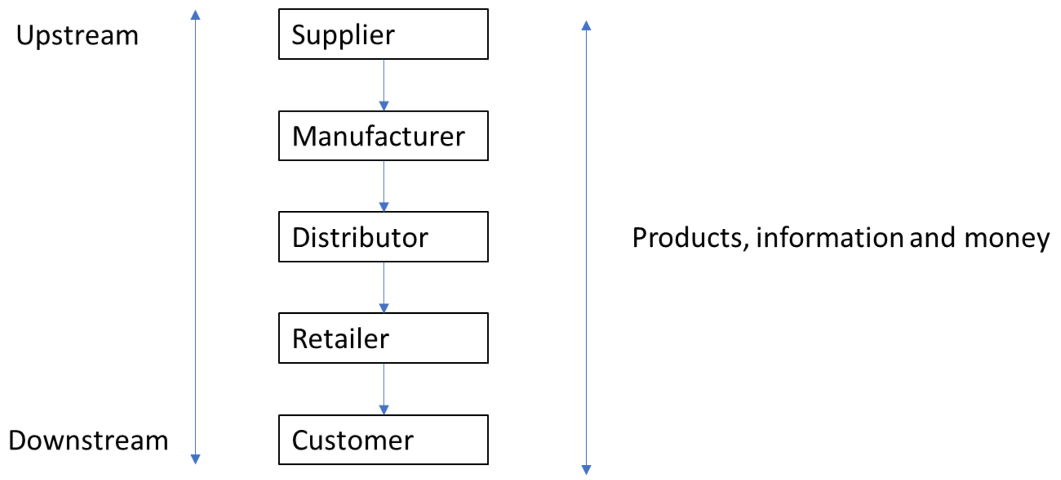

Figure 2-12 Movement of products, information and money

When there are many competing entities in a global market the supply chains become a complex network of participants that is challenging to monitor. A product may take a complex route from manufacturer to customer caused by marked forces. It may be profitable to repackage a product several times and transport it through several continents before it ends up at its destination.

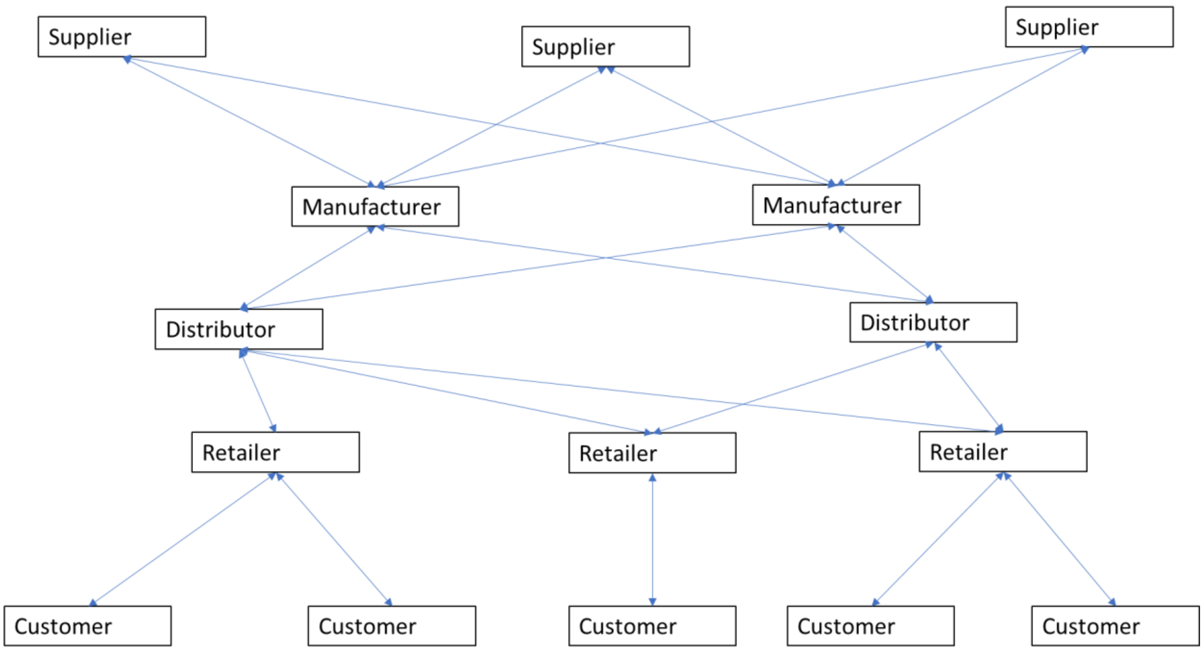

Figure 2-13 Supply chain as a complex network

Supply chains today rely heavily on information technology to coordinate all the information. The Internet, Enterprise Resource Planning (ERP) software, Global positioning systems (GPS), Radio frequency identification (RFID), Big data analytics and Internet of Things (IoT) are technologies that enables the supply chains to maintains its efficiency. [55, p. 19]. These technologies are also important for security reasons.

2.3.3 The Bullwhip Effect

In a complex supply chain, there are many actors that buy and sell at different points in the network. None of the actors have full access to the state of the entire network. Many actors may only 'see' one step upstream and one step downstream from where they are located. One consequence of this is an amplification of excess and shortage of products in the supply chain. This is known as The Bullwhip Effect. [56, p. 27]

The fundamental reason for this phenomenon is the lack of transparency in the supply chain. If all actors have access to everything at the same time, this problem would be possible to avoid.

2.3.4 Anti-counterfeit technology in the supply chain

According to [57] there are three main uses of anti-counterfeit technologies.

- Revealing that tampering has happened. Using tamper-resistent packing.
- Authenticating a product. Using for example a hologram.
- Tracking and tracing. That is, providing a pedigree of a product.
    - Tracking: «... knowing the specific physical location of a drug in the supply chain at any time.» [58]
    - Tracing: «The ability to know the previous form, packaging, location, duration and storage type..» [58]

There are three components to a system that tracks a product: tag, tracer and sensor. [59] The tag can be a sticker with a code that identifies the product. It can also be an RFID-tag. An example of a tracer can be a radioactive substance applied to the product. A sensor collects information about the environment (e.g. a temperature sensor).

2.4 The Pharmaceutical Industry

> « The discovery, development, and manufacture of drugs and medications (pharmaceuticals) by public and private organizations. » [60]

Humans have used plants, animals and minerals for thousands of years to manipulate illnesses, but modern use of pharmaceutical substances started in the eighteen hundreds based on a better understanding of chemistry and physiology. [60]

The industry is now considered a fundamental part of modern healthcare around the world.

Revenues of the worldwide pharmaceutical industry were larger than 1 Trillion USD in 2018. It is a global industry. Approximately half of the market is in North America. the European market is approximately one fifth of the total. The rest of the revenue is generated from around the word.[61] The largest company in the industry is Pfizer. It has a revenue of more than 50 billion USD and employs nearly 90 thousand people. [62]

It is assumed in this thesis that the supply chains of the pharmaceutical industry are not fundamentally different from other supply chains. The general considerations of supply chains and supply chain security will be applicable also for pharmaceutical supply chains. There are still some special considerations. The pharmaceutical industry is generally the subject of extensive regulations, more so that many other industries. Different legislation in different countries in an industry that is inherently global complicates the supply chain management further. The focus in this thesis is on the technological level and legal matters will not be discussed.

3 Research methods

The methods used to answer the research question are divided in two parts. The first part consists of reviewing the specific field the RQ addresses in order to draw conclusion regarding the research itself in the field. The second part consists of analysing the proposals in the field both from a blockchain-theory point of view and a supply chain management point of view and using the finding from research on other types of blockchain-based supply chains. The reason for this it to find inconsistencies in the proposals and see the opportunities the integration of theories, related research results and proposals may provide.

3.1 Reviewing the literature

3.1.1 Keywords and search structure

(TITLE-ABS-KEY (blockchain) AND TITLE-ABS-KEY (counterfeit OR false* OR falsified OR fake OR fraudulent OR substandard OR "low quality" OR bad OR "below standard" OR inadequate) AND TITLE-ABS-KEY (drug OR medicine OR pharma* OR medication))

In order to capture literature in this specific field, a combination of synonyms for 'blockchain', 'falsified', 'substandard' and 'pharmaceutical' were used in a Boolean search phrase for content in title, abstract or keywords.

3.1.2 Selecting search system and databases

The Scopus search system and corresponding databases were chosen.

A recent article [63] have pointed out some helpful advice when choosing search systems. They tested 28 search systems (34 databases) for systematic reviews using 27 test criteria to evaluate the capabilities of these system. The results were described in term of coverage, search queries, search results and search reproducibility. Sixteen of the databases were multidisciplinary.

17 of 28 search systems supported Boolean operators in the queries without any problems. Among the search systems that did not do well with Boolean operators were Google Scholar. Among the search systems that did well, even with long and complicated queries, were PubMed, Scopus and Web of Science. Google Scholar was one of the two search systems that failed to be completely reproducible.

Only 14 of the 28 search systems were found by the authors to be well-suited for systematic reviews. Among them were several multidisciplinary systems e.g. Scopus and Web of Science (Core Collection).

Others have studied the differences between the three major search systems [64], [65]. One of the conclusions the author of this thesis draws from these comparisons is that Google Scholar has a larger coverage and scope compared to the two other main search systems, especially regarding 'grey' or non-journal sources. With some reservations it can be seen as a superset of Web of Science and Scopus where the two latter will have a large degree of overlap.

Choosing search systems for the question in this paper is a matter of compromise. The topic covered is interdisciplinary in nature. This suggests using a multidisciplinary search system. Google Scholar has the bigger reach, but 'grey literature' is not desirable for this purpose. The problems with reproducibility and complex Boolean search are also factors that count against Google Scholar. Choosing between Web of Science and Scopus, that to a large degree overlap, may be difficult. Using both would be best, but this would require much more time. For these reasons Scopus is chosen as the only search system to cover the search in this thesis, partly because of the user-friendly interface and the ease at which one can generate visual statistics.

3.1.3 Inclusion and exclusion criteria

There was no time limit since the term 'blockchain' was included and would automatically limit the search to the first use of the term. Non-English literature would be excluded. Both traditional research papers and reviews would be included but treated separately. The quality and type of papers were not used to exclude or include, but if a paper turned out to be a non-scientific comment from a magazine, it would be excluded as a 'not-academic paper'. Unfortunately, some publications are not included in the subscriptions available for students at NTNU. In this case a publication would be excluded as 'no-access'.

Excluding non-English publications may introduce a bias, especially if a field has a significant portion of non-English publications. Including all languages would in theory be best but would require considerable resources for professional translation. Excluding papers behind a paywall not covered by NTNU could also potentially introduce bias.

The quality and type of papers may affect the result. Since the field is so small, only non-academic papers would be excluded based on type or quality. The Scopus search system puts restrictions on what papers can be in their databases. This is an indirect quality assessment and will exclude most 'grey' literature.

3.1.4 Procedure used to classify papers

- Read through the titles and abstracts. If title alone or title plus abstract makes it obvious that the paper is irrelevant, it is excluded and reason for exclusion is noted.
- Read through the full paper if possible.
    - If the paper was not accessible through the subscriptions from NTNU, it was excluded as 'no-access'.
    - If the paper was a non-English publication it was excluded as 'non-English'.
    - If the paper was not an academic paper it was excluded as 'not-academic paper'.
    - If the paper was not relevant to the topic, it was excluded as 'not-relevant'.
- The remaining papers was included by default and divided into non-reviews or reviews.

3.1.5 Selecting and describing content from individual papers or meta-information about the set of papers

The content of each included paper was summarized for overview. The volume of research as a function of time and region was described and visualised to illustrate the size of the research field. The use-cases in the proposals were briefly summarized. The proposals in the set of included papers were categorized as 'no proposal', 'theoretic proposal', 'proof-of-concept', 'prototype' and 'real-world testing'. This was done to map the maturity of the projects. Finally, the type of blockchain in the proposals were categorized if possible.

By this selection there would be enough data to give an assessment of the state of research in the field including possible gaps in research. Additionally, the data collected can be compared to general theory of blockchains, supply chain management and research results from related blockchain-supply chain fields.

3.1.6 Review as a research method

The idea of a literature review is sometimes associated exclusively with part of the preparation for research and not as a research method in itself. As [66] argues there are several advantages of using literature review as a research method: Providing overview in an interdisciplinary field where the research is fragmented is one example. Putting together results to find meta-level evidence is another.

3.2 Integrating the review results with related theories

The use-case description and types of blockchains described in the proposals were compared with theory on blockchain, SCM and research on blockchain and supply chains in general. The reason for this was to find gaps and inconsistencies in the proposals and possibly suggestions for improvements.

4 Results

4.1 Search strategy results

A search was conducted 22.03.2020. The results are shown in figure 4-1 below. There was only one review among the included papers.

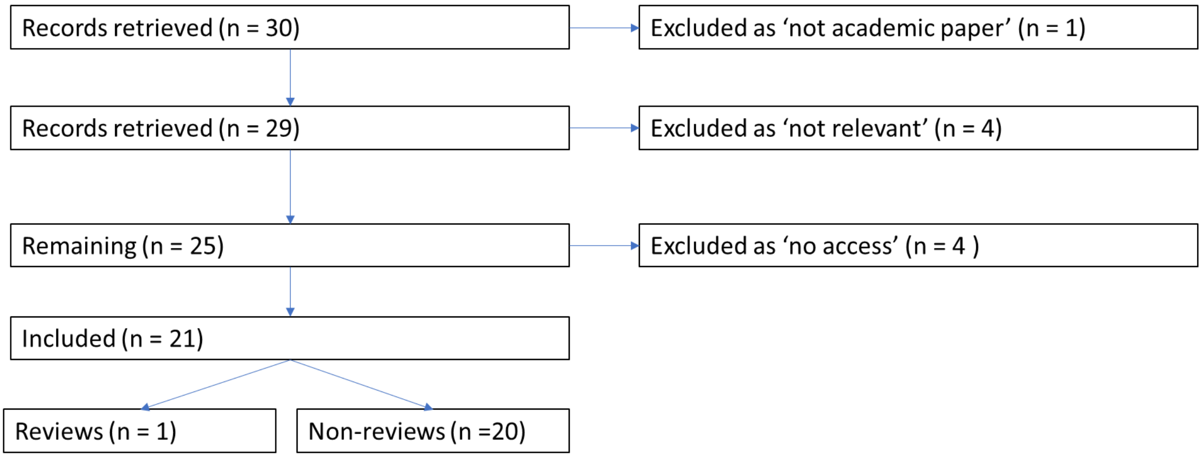
Records retrieved (n = 30)
Excluded as 'not academic paper' (n = 1)
Records retrieved (n = 29)
Excluded as 'not relevant' (n = 4)
Remaining (n = 25)
Excluded as 'no access' (n = 4)
Included (n = 21)
Reviews (n = 1)
Non-reviews (n =20)

Figure 4-1 Search inclusions and exclusions

4.2 Description of the data

4.2.1 Non-reviews

4.2.1.1 Overview of sources and short summaries

Se Appendix 1 for a list of included sources and short summaries of each included source (non-reviews).

4.2.1.2 Publications per year

There were 20 non-reviews included. As shown in figure 4-2 there is a clear increase in publications per year from 0 in 2017 to 11 in 2019.

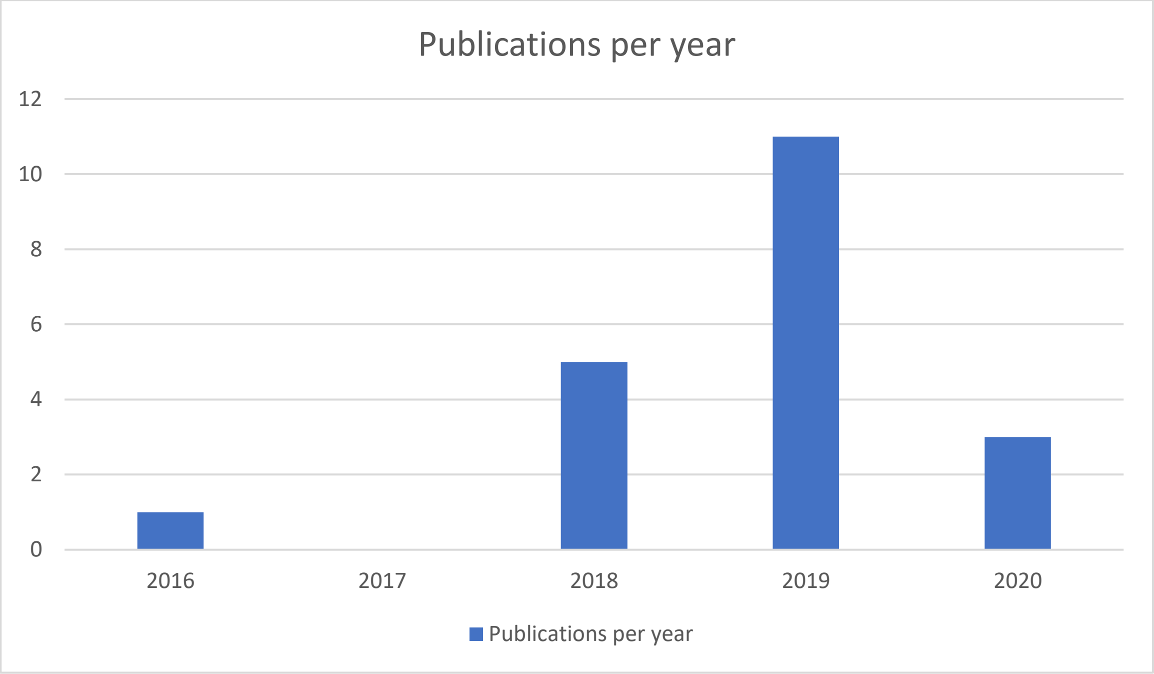

Figure 4-2 Publications per year

4.2.1.3 Publications by region

A significant minority of publications are Indian as shown in figure 4-3

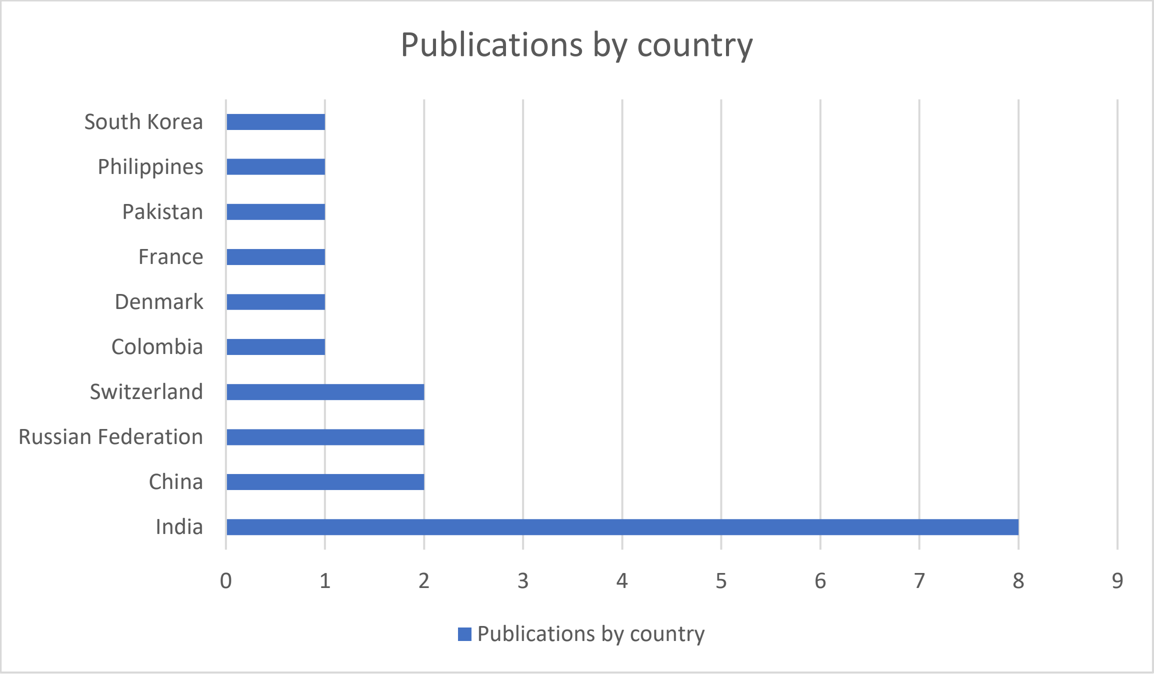

Figure 4-3 Publications by country

4.2.1.4 Use-cases in included sources

Table 1 Use-cases in sources

Publication	Simplified use-case description from sources
Sahoo et al., 2019 [67]	Simple general blockchain-supported supply chain system with focus on traceability and visibility.
Grest et al., 2019 [68]	This article takes an abstract meta-perspective on blockchain-based supply chain traceability.
Jamil et al., 2019 [69]	A blockchain-supported drug supply chain in a smart hospital.
Raj et al., 2019 [70]	A general blockchain-supported pharmaceutical supply chain
Anand et al., 2020 [71]	A general blockchain-supported pharmaceutical supply chain for tracking and tracing counterfeit drugs.
Chanson et al., 2019 [72]	The article proposes a design theory for sensor data protection systems with a focus on privacy for sensor data. Discussed use in pharmaceutical supply chain.
Azeem et al., 2020 [73]	A general blockchain-supported pharmaceutical supply chain with a focus of licensing/evaluation of manufacturers.
Sylim et al., 2018 [74]	A blockchain-supported pharmaco-surveillance blockchain system.
Mettler, 2016 [40]	No specific proposal
Bryatov & Borodinov, 2019 [75]	A general blockchain-supported pharmaceutical supply chain. Relational modelling.
Kumar et al., 2019 [76]	A general blockchain-supported pharmaceutical supply chain.
Nørfeldt et al., 2019 [77]	Supply and monitoring of personalized drug doses using blockchain technology.
Huang et al., 2018 [78]	A general blockchain-supported pharmaceutical supply chain.Traceability and regulation.
Botcha et al., 2019 [58]	Improved traceability in a pharmaceutical supply chain. Focus on edge devices and IoT using blockchains.
Tseng et al., 2018 [79]	A general blockchain-supported pharmaceutical supply chain. Focus on governance.
Pandey et al., 2020 [80]	A general blockchain-supported pharmaceutical supply chain. Focus on counterfeit detection and authentication of drug by user.

Plotnikov and Kuznetsova, 2018 [81]	A general discussion. No specific proposal.
Kumar and Tripathi, 2019 [82]	A general blockchain-supported pharmaceutical supply chain.
Archa et al., 2018 [83]	A general blockchain-supported pharmaceutical supply chain.
Molina et al.,2019 [84]	A general blockchain-supported pharmaceutical supply chain. Focus on traceability.

4.2.1.5 Maturity of proposals

Looking at the maturity and type of blockchain solution proposed there are some clear patterns as shown in table 2 ang figure 4-4.

Table 2 Maturity of proposals

Publication	**Theoretical proposal**	**Proof-of-concept**	**Prototype testing**	**Real world testing**
Sahoo et al., 2019 [67]	yes	no	no	no
Grest et al., 2019 [68]	yes	no	no	no
Jamil et al., [69]	yes	yes	no	no
Raj et al., 2019 [70]	yes	no	no	no
Anand et al., 2020 [71]	yes	no	no	no
Chanson et al., 2019 [72]	yes	yes	yes	no
Azeem et al., 2020 [73]	yes	no	no	no
Sylim et al., 2018 [74]	yes	no	no	no
Mettler, 2016 [40]	no	no	no	no
Bryatov & Borodinov, 2019 [75]	yes	no	no	no

Kumar et al., 2019 [76]	yes	yes	no	no
Nørfeldt et al., 2019 [77]	yes	yes	no	no
Huang et al., 2018 [78]	yes	no	no	no
Botcha et al., 2019 [58]	yes	no	no	no
Tseng et al., 2018 [79]	yes	no	no	no
Pandey et al., 2020 [80]	yes	yes	no	no
Plotnikov and Kuznetsova, 2018 [81]	no	no	no	no
Kumar and Tripathi, 2019 [82]	yes	no	no	no
Archa et al., 2018 [83]	yes	no	no	no
Molina et al.,2019 [84]	yes	no	no	no

There are no real-world implementations. Most proposals are of a theoretical or conceptual nature. The maturity is shown in figure 4-4.

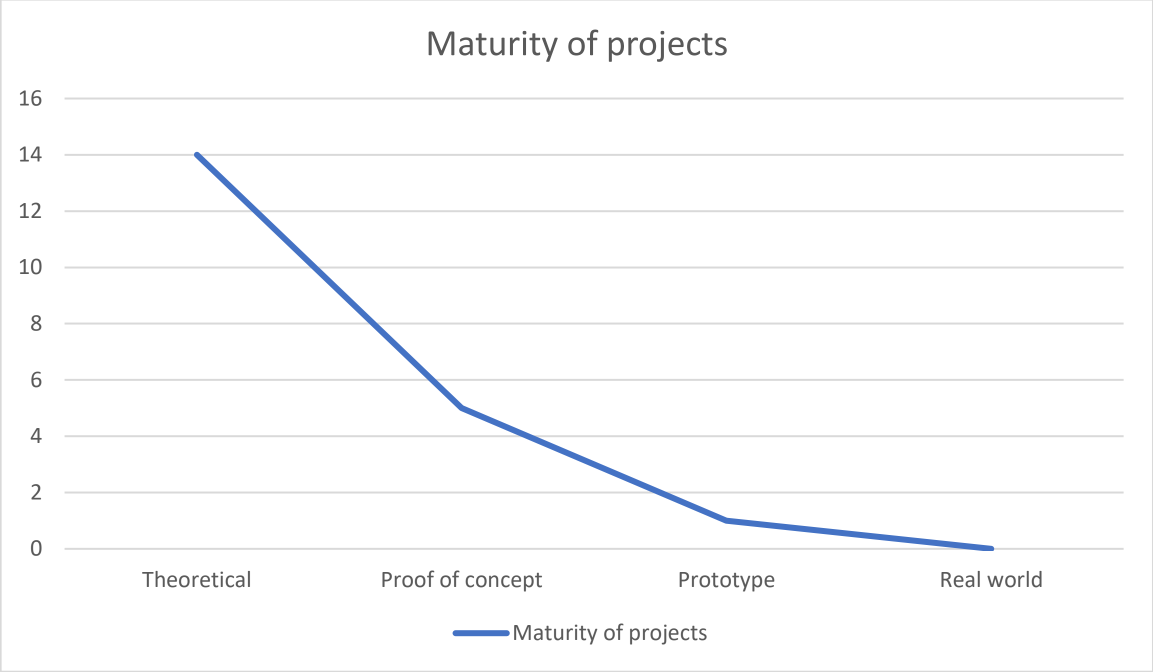

Figure 4-4 Maturity of projects

4.2.1.6 Types of blockchains in proposals

In table 3 the content of the sources has been analysed in order to categorize the proposals into the dimensions explained in chapter 2.2.11. Some of the sources did not have a specific proposal. In other sources it was partially unclear what features the blockchain-based solutions they described had. If a proposal had read access for all participants and all participants could propose transactions, then the value in the first column in table 3 was 'yes'. Otherwise the answer would be 'no' or 'unspecified'. If all users could be miners and verify transactions the answer in the second column would be 'yes'. Otherwise 'no' or unspecified.

All proposals in the set of sources assumed some kind of onboarding process. There would be vetting before an actor could join the network. This is unlike Bitcoin where anyone can join or leave without passing any tests.

Table 3 Categorizing proposals

Publication	**Public/private** **(Read access and right to propose new**	**Permissionless/ permissioned** **(All users can verify transactions**	**Comment**

	transactions for all users?)	**and add new blocks?)**	
Sahoo et al., 2019 [67]	Yes	Unspecified	Not enough information to classify the design proposal
Grest et al., 2019 [68]	Unspecified	Unspecified	
Jamil et al., 2019 [69]	No	No	Private and permissioned
Raj et al., 2019 [70]	No	No	Private and permissioned
Anand et al., 2020 [71]	Unspecified	Unspecified	The description is somewhat inconsistent.
Chanson et al., 2019 [72]	Unspecified	Unspecified	This paper was not focused on a particular proposal.
Azeem et al., 2020 [73]	Yes	No	Unclear who the miners can be. Public and permissioned
Sylim et al., 2018 [74]	Yes	No	Suggest a combination of Ethereum and Hyperledger.
Mettler, 2016 [40]	Unspecified	Unspecified	No specific proposal
Bryatov & Borodinov, 2019 [75]	No	No	Private and permissioned
Kumar et al., 2019 [76]	No	No	Private and permissioned
Nørfeldt et al., 2019 [77]	Unspecified	Unspecified	
Huang et al., 2018 [78]	No	No	Private and permissioned
Botcha et al., 2019 [58]	Unspecified	Unspecified	
Tseng et al., 2018 [79]	Yes	No	Public and permissioned
Pandey et al., 2020 [80]	No	No	Private and permissioned
Plotnikov and	Unspecified	Unspecified	No detailed proposal

Kuznetsova, 2018 [81]			
Kumar and Tripathi, 2019 [82]	Yes	Unspecified	
Archa et al., 2018 [83]	Unclear	Yes	
Molina et al.,2019 [84]	No	No	Private and permissioned.

An illustration of the table 3 can be seen in figure 4-5.

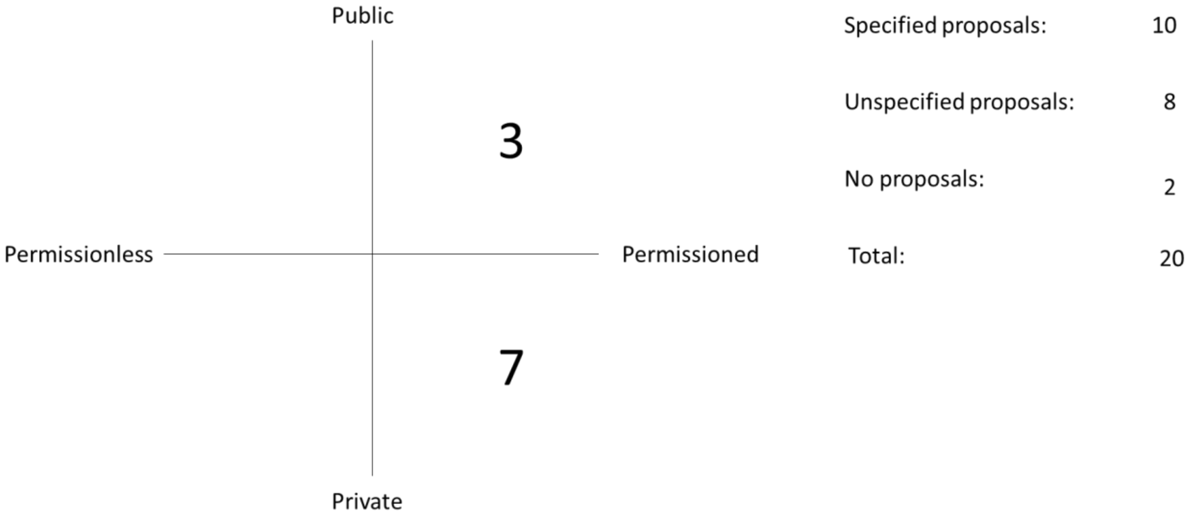

Figure 4-5 Types of blockchain

4.2.2 Review

There was only one included review [41]. This review from 2017 took a general approach on existing and emerging digital technologies used to combat falsified pharmaceuticals. The review identified 5 categories of digital technologies for combating FSP in the supply chain. One of the categories was blockchain technology. This was not a review that focused exclusively on blockchain technology. They identified 4 main uses of this technology (tracking/tracing, transparency for increased detection, integrating anticounterfeit devices for detection and authentication and enhanced information sharing across databases).

5 Discussion

5.1 Recap of the research question

The research question was presented in chapter 1.6 and is repeated here:

RQ: What research has been done on the topic of using blockchain technology to mitigate FSP in the supply chains? Secondarily, how can the results of this research, together with theory and research from allied fields, inform us about applying this technology for the specific purpose of combating FSP?

In the following, the results from chapter 4 used to review the field is discussed first. Then some additional topics are discussed that will hopefully be helpful for developers.

5.2 Volume of included papers

Searching for relevant literature, a small number of papers resulted from the search (n=30). Of these only 20 were included based on the inclusion/exclusion criteria. At first sight it may appear as this is a very small research field. But blockchain technology has only existed for approximately a decade. That would reduce the time available for publications. The more generalized blockchain-technology that allows applications outside of cryptocurrencies through smart contracts have only existed in half that time. As an example, Ethereum went live in 2015. [23] This was the first smart-contract blockchain that allows Turing complete programmable applications[4]. In addition to this, the field of focus is a small part of applying blockchain technology to supply chain problems. Based on the above, it is less surprising that the research field is small. Another factor is the search itself. The use of keywords and databases may have excluded some sources. A more open set of key words would have resulted in more potential sources, but it is unclear how many of the potentially included sources that were actually lost. Using both Scopus and Web Of Science may have caught some additional sources even if their scope in mostly overlapping. Google Scholar has the broadest scope but includes a lot of 'grey' literature that was not the focus in this study. In addition, Google Scholar also has issues regarding handling complex Boolean search strings and reproducibility.

5.3 Publications per year

Unsurprisingly, there was no publication prior to 2015. The idea of applying blockchain technology to supply chains was quite new at the time. Blockchain technology was associated with financial applications like storing value and doing payments. The rapid increase in the number of publications correlate with the media attention and the price of cryptocurrencies. The general attention on this type of technology and possibly the opportunity for funding of research may partly explain it. It is yet to be seen if research on blockchain technology will continue to rise despite the recent decline in media

[4] Bitcoin has a simple script language that is (intentionally) not Turing complete. In Ethereum smart contract programming with Solidity, there is Turing completeness, but the presence of 'gas' prevents certain types of programs and some argue that this makes smart contract programming not Turing complete.

attention and prices. Another factor could be more attention towards the problem of FSP in the supply chains and an increased search for alternative technological solutions.

5.4 Origin of publications

The country of origin of the included non-review papers were dominated by India and no non-review papers had an origin in the US. This could be a coincidence since the number of papers were small. There might be an active research group in India that has focused on this particular problem. Another possible explanation may be that the presence of FSP seem to be more prevalent in India and other non-western countries compared to the US. The topic may be more relevant for people in India and would draw more attention from researchers there. The exclusion of non-English papers was not a factor.

5.5 The use-cases focused on by the researchers

Of the 20 included papers, 14 of them focused on similar scenarios: A simple general pharmaceutical supply chain and different perspectives on how blockchain technology could contribute to solve security related problems to combat FSP in the supply chain. This is also the core of the topic for this thesis. There were variations in detail and specific solutions, but many similarities. A minority of the papers had a different approach. [68] had a meta focus of traceability in blockchain supported supply chains. [72] focused on IoT sensor data protection in several contexts, also blockchain-based supply and used a pharmaceutical supply chain as an example at the end or the article. [58] proposed a design for using IoT edge devices as a cloud based back-end for pharmaceutical supply chains. [77] proposed a solutions for a specific use case for safety and personalized dosing of medication. [40] and [81] did not provide a proposal, but a more general discussion.

The 14 relatively generic proposals did not elaborate much on general supply chain management theory or experience from using blockchain technology in related supply chains in their articles, although this could arguably be a relevant part of their proposals. An example is [82] that propose a blockchain based secure infrastructure for a medical chain to improve traceability of counterfeit medicine. The authors provide a simple figure of the supply chain showing the types of participants in the chain. The 14 proposals that addressed the core problem would typically take a 'high-level' approach to the problem of FSP and use simple models.

The generic, high-level approach that seem to be the trend may illustrate the fact that the field is still new and immature like blockchain technology is. The interdisciplinary nature of the field may also represent challenges. Not many are experts on general computer science, blockchain technology, supply chain management and the problem of FSP. These different fields use different models and terminology. There are many 'moving parts' and the integration of models across these disciplines would be demanding.

5.6 Maturity of the projects

Looking at the maturity of the projects in the proposals, it is a pattern that most proposals are of a theoretical or conceptual nature. The more mature, the less likely it is to find examples of research in the field (Figure 4-4). Among the included papers, no paper had developed anything that was tested in the real world. Looking at reviews from other types of blockchain-based supply chains, a similar phenomenon exists. In [31], a review from 2019 on blockchain applications in the agri-food supply chain, the authors found only two real world case studies excluding commercial projects. One that implemented a blockchain business network for agricultural exports in Brazil and another that focused on traceability of wood from standing trees to final user. A similar conclusion was drawn by [36] when reviewing blockchain technology in the transport sector. They found that most scientific papers focused on potential applications and there were very few real implementations. Wang et al [27] reviewed the general field of blockchain technology in supply chains in 2018/2019. They found that the general state of research publications was at the sense-making and exploration stage and that there is very limited evidence of the real impact of this new technology on the supply chains.

What was seen in the use-cases, a hight-level generic approach with simple theoretical models may be connected to what is seen in the maturity pattern. There is a distance to the real and tangible world illustrating a field that is new and exploratory.

5.7 Types of blockchains chosen

In 2.2.11 four definitions for classifying blockchains were defined. The included proposals have, to the extent possible, been classified accordingly in table 3. One observation is that some of the proposals were unclear as to what type of blockchain design they had in mind. It was difficult to find information in the papers what would allow a classification. As discussed previously regarding maturity and use-case, the field is new and many of the proposals are of a conceptual nature.

Those proposals that contained enough information to allow classification were all more or less permissioned. Permissioned means that only a predefined list of subjects with known identities can process the transactions. That is, verify transactions or be miners. Almost all the proposals assumed some kind of onboarding for participants in the supply chain. Typically, regulators like government agencies would have a special status in the network. Manufacturers and other participants would need to be approved in some way, for example through a certification process. As mentioned in chapter 2.2.11 and explained in [48, p. 216], choosing between permissionless vs. permissioned is a choice between security and speed. When the proposals describe a permissioned blockchain they are effectively choosing speed over security. To compensate for this, they invest trust in some entities that get to decide who will have read and write access to the blockchain and who will not. Someone also made the rules that decides the read and write access. This introduce an element of centrality in the distributed system and assume that the users have a degree of trust in each other. If key actors with more influence that others were corrupted, this would represent a serious security vulnerability. The majority (7/10) of the specified proposals fell down on the private side of the private-public dimension. Private blockchains put restrictions on the users' right to read transactions and propose transactions (that may or may not be included in the blockchain). Choosing between public and private is a choice between transparency and privacy. As explained in [48, p. 214] the transparency makes it possible for all participants to audit the transactions and clarify ownership. This stands in contrast to privacy where the transaction data details are hidden from the public.

The most common choice among the proposals were private, permissioned blockchains. Speed and privacy over security and transparency.

These choices should be viewed in light of the use-case descriptions. That it, the environment, and problem focus. The generic pharmaceutical blockchain-based supply chains in most of the proposals assumed an environment of partial trust. Not a completely trust less environment with an unknown number of nodes. The participants needed to be vetted or certified to access the network. That means they would to some degree be trusted if they passed the onboarding process. There was also the assumption of a centralized power that would regulate the marked and be trusted by default. Based on this, a private, permissioned blockchain is a reasonable choice.

One problem is the nature of the pharmaceutical industry as described in chapter 2.4. It is a large, global industry with a complex supply chain including a large number of participants that do not necessarily trust each other. The pharmaceutical industry is strongly regulated, but there are different laws and regulations for each region of the world. This would imply a network of blockchains with different arrangements for each region that are capable of a high degree of interoperability. 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." [85] There exist some technologies that are addressing the problem of interoperability. The Cosmos Network [86] and Polkadot [87] are two examples of projects working on this problem.

5.8 Additional topics for discussion

5.8.1 What can blockchain technology offer pharmaceutical supply chain security?

Wang et al. [27] considered in their review that the value of blockchain technologies for supply chains was in visibility, traceability, digitalization, disintermediation, data security and smart contracts. Some of the features they listed are important both for security and non-security reasons at the same time. Visibility, that all actors see the same truth at the same time, will make a supply chain more effective. As explained in chapter 2.3.3, a troublesome phenomenon in supply chains is The Bullwhip Effect. The reason behind this phenomenon was limited visibility for the actors in the supply chain. Using blockchains and choosing a design where all parties can read all the data in the blockchain will reduce or eliminate The Bullwhip Effect. This would make the supply chain more efficient. At the same time, transparency in a public permisisonless blockchain will be a security enhancement since all parties can verify transactions and detect any errors. Traceability, «The ability to know the previous form, packaging, location, duration and storage type…» [58], satisfies a customer's need for knowing the history of the product being purchased. This adds value to the product. At the same time, it is an important part of securing the supply chain against FSP. A similar argument can be made for disintermediation. Removing unnecessary middlemen can be cost effective. At the same time, it may reduce risk in the supply chain. Fewer links from manufacturer to customer equates to less chance for a counterfeiter to inject falsified pharmaceuticals into the supply chain. The same can be said about the quality risk of pharmaceuticals. The more stops on the journey from manufacturer to customer, the more risk of delays where the storage environment and physical handling may affect the quality of the products.

Digitalization or «the process through which the physical products and services people buy become dependent on virtual products and services.» [56, p. 208] can also have a dual role. In general, it can add value to the customer. The digital services, if useful, give something to the customer that may increase user satisfaction. At the same time, a digital service may also be an app that helps the customer authenticate the product and this way mitigate falsifications.

The relative immutability of records is one of the most important advantages of blockchain technology if immutability is vital for a particular use case. In a purely distributed blockchain this can prevent attacks that aim to change the history of transactions. An example would be corruption. In a centralized system where someone has the power to change records in a database, there is a possibility for corruption. In a centralized pharmaceutical supply chain, an actor may change the record and inject falsified or substandard products.

The partition tolerance is another advantage a distributed system can offer. For many applications 100% uptime can be essential. A blockchain-based supply chain will be able to continue to function even if parts of the network fails. There is no single point of failure. If the information system of a traditional supply chain fails, a backup plan will typically be used. The phase where stakeholders need to improvise will represent an opportunity to introduce falsified or low-quality products.

5.8.2 Limitations

5.8.2.1 Consensus mechanisms

As mentioned in chapter 2.2.8 the blockchain reaches a distributed consensus where the nodes agree on a single truth without a central authority. In order to come to this agreement in a public permissionless blockchain like Bitcoin, mining is done. The activity of mining includes adding a block by solving a hash puzzle in competition with other miners. Bitcoin uses proof of work (PoW) as the consensus mechanism. Different blockchain designs used different consensus mechanisms and this has consequences for the performance of the network. This brings the question of what mechanism is the most appropriate for a pharmaceutical supply chain?

Vukovic [88] explored different consensus mechanisms by contrasting the two main families of mechanisms, PoW and BFT (Byzantine Fault Tolerance). As he pointed out the PoW blockchains show good scalability in term of number of nodes, but poor performance in terms of transactions per second. On the other hand, BFT blockchains can do many transactions for a small number of nodes in the network. These two families of mechanisms (standard BFT and standard PoW) represents opposites in terms of scalability. [88, Fig. 1] Another relevant point from this paper is the identity management requirements for these two contrasting blockchains. In BFT, every node needs to know of every other node in the network to reach consensus. This is clearly less flexible than PoW in Bitcoin but may be suitable for some application. In all the proposals described in chapter 4, there was the assumption that participants in the network had to be known and vetted.

If forced to choose between the two standard mechanisms and given the most likely legal limitations that would require only vetted and known participants, it is best to choose the BFT mechanism because of increased performance in term of transactions per second. But the poor performance in term of number of nodes would be unacceptable for a global pharmaceutical supply chain consisting of a large number of participants.

One of the included sources in the main search from chapter 4 [74] claims that distributed proof of stake (DPoS) or practical byzantine fault tolerance (PBFT) fits the pharmaceutical supply chain environment best. They argued that these two algorithms eliminate the need for third-party miners that would compete for resources (power and currency) and that they are better for private consortium (permissioned) networks.

PBFT is a variation and optimization of BFT. Hyperledger Fabric is one of the technologies that are using this mechanism. According to [89], PBFT does not have the waiting time for the finality of a transaction. Unlike Bitcoin where there is a waiting time for the next blocks to finish before the transactions is considered final. It still shares the problem with BFT where performance in terms of transactions per second is weakened as the number of nodes becomes larger. Another potential problem with PBFT is the large number of IoT devices in a IoT-blockchain integrated supply chain solution. [38]

PoS is a consensus mechanism that requires the participants to prove possession of a certain amount of the cryptocurrency and lock it down in order to create new blocks. [90] The DPoS mechanism is a variation of PoS and was first discussed by Daniel Larimer. [91] In DPoS the participants in the network vote for a set of delegates that sign the transactions. The 'voting by proxy' introduces an element of centrality, but anyone can potentially become a delegate. The DPoS is used in EOS, a recent blockchain. [92]

According to [90] DPoS consensus algorithm all have good non-repudiation, a high degree of censorship resistance and a good resistance against denial of service (DoS) attacks and Sybil[5] attacks. In addition, a high throughput, high scalability, and a low latency.

There are many other consensus mechanisms proposed, including combinations of several consensus mechanisms. As far as the author understands, there are no obvious best fit for a security focused pharmaceutical supply chain.

5.8.2.2 The Scalability Trilemma

The Scalability Trilemma claims that you cannot maximize decentralisation, security, and scalability at the same time. Some blockchain technologies are trying to find ways to partly compensate for this. Using Ethereum as an example, its design has prioritized security and decentralization at the cost of scalability. As of now Ethereum runs at approximately 10 transactions per second. [93] A centralized system would easily be able to process a lot more transactions per second. Ethereum is planning to replace the consensus mechanism with PoS and introduce sharding (partitioning the blockchain into smaller blockchains that can run in parallel). This has not yet been implemented, but is expected to improve scalability. [94]

5.8.2.3 Privacy

The conflict between privacy and transparency in a public permissionless blockchain is a limitation that creates a challenge in applications where privacy is important to the stakeholders. A typical example would be health related applications like electronic health records. In a pharmaceutical supply chain, the stakeholders may not want to share information when competing. The end user of pharmaceuticals would also want to keep information about medication away from other than the health personnel directly involved in their treatment.

5.8.2.4 Limited flexibility

Blockchain technology also have a limited flexibility compared to centralized information systems. Stakeholders that have committed to a blockchain-based supply chain, may find

[5] The attackers would create a large number of fake identities and gain an unfair influence.

that the environment they operate in is changing and will not be able to adapt to those changes as rapidly as their competitors using non-blockchain technology.

5.8.2.5 Cost

The robust security features of a blockchain-based system come at a cost. The computational cost of PoW is one example. The redundant storage of transaction data in every node in the network is another. In a competitive industry like pharmaceutical supply chains there may be small margins of profit and a reluctance to commit to a more expensive system.

5.8.2.6 Practical development limitations

The most used suite of technology in the proposals were Hyperledger. Or more precisely Hyperledger Fabric. The second most used technology was Ethereum. Ideally developers start with the problem and then choose the technology that fits the problem the best. Unfortunately, this may not be possible in the blockchain space. Compared to more mature fields, there is less tools to choose from, less support and a steep learning curve. Implementing a prototype for a pharmaceutical supply chain using the Ethereum technologies would require a general understanding of blockchain technology, proficiency in programming smart contracts using one of the languages available (Solidity is the de facto standard), extensive testing in a test network and finally careful auditing of contracts before deploying it on the main network. The immutability features of the main network would severely reduce the options for updates and changes after the fact. All this is quite demanding and would come on top of a larger system where regular web development also plays an important part.

5.8.3 Do you need a blockchain?

A developer of a pharmaceutical supply chain design for enhanced protection against FSP would first have to evaluate if blockchain technology is a good fit or not. To answer this question a few researchers have developed general frameworks to help in that regard. Lo et al. [95] made a framework consisting of 7 criteria in 2017. They also provided use-cases where they went through the 7 criteria and concluded with blockchain or database. The supply chain and identity management use cases were deemed suitable for blockchains. Electronic health records and the stock market was deemed not suitable.

Looking closer at the 7 criteria with the main topic of this thesis in mind, can be helpful for someone developing a proposal.

The first criterion is whether the system requires multiparty involvement. This is clearly the case in a pharmaceutical supply chain. It is a large global industry where products may change hands many times on its journey.

The second criterion is whether a trusted authority is required and if the trusted authority can be decentralized. All the proposals in the included papers had a trusted authority with a special power, typically a government regulator. Even in a global network of blockchain-based supply chains, there would probably be trusted authorities in the sub-networks that had the power to certify participants. The question is whether such authorities can be decentralized. A participant in the network may get a certificate as a pharmaceutical manufacturer somewhere else and present proof of this to peers, but that would only move the trust somewhere else.

The third criterion is whether the operations need to be centralized. In the pharmaceutical supply chain, the operations do not have to be centralized. A large number of independent organizations are involved in a distributed way from 'hook to fork'.

The fourth criterion is transparency and confidentiality. In a private permissioned blockchain read access can be regulated. In a public, permissionless chain the participants can read all the transactions. Competitors would be reluctant to share some of their data to each other. On the other side there are advantages in supply chain efficiently by having a large degree of transparency. At some point in the supply chain pharmaceuticals would be sold to the end user and there would be a need for privacy from other participants like manufacturers and others. Only the pharmacy and other health personnel involved in the treatment of an individual should be able to read who uses the drugs.

The fifth and sixth criterion is integrity in the transaction history and immutability. This is desirable for several reasons. It would be very costly to go back and change transactions. The pharmaceuticals could be tracked with confidence. From an anti-counterfeit point of view, it would be worth the extra cost in most cases. It would also provide non-repudiation in cases of conflict between participants.

The last and seventh criteria is performance. In a global pharmaceutical supply chain, many transactions would take place every minute. How many per second is unknown. It would depend on many factors, included the type of blockchain used. As the authors in [95] point out, parts of the existing supply chains today are based on paper documentation. In this perspective high performance is not required. On the other hand Visa claims to be able to handle 65 thousand transactions per second. [96] Other sources claim this is wrong and that is handles approximately 1700 transactions per second. [97]

Scriber [98] argues for the use of 5 main criteria to help decide if a system is a good fit for blockchain technology. His criteria are partly overlapping with Lo et al.

The first criterion is the requirement of immutability. Immutability comes at a cost and the importance of this needs to be significant in order to choose a blockchain solution. From a security point of view immutability is a clear advantage and may be worth it in building a pharmaceutical supply chain.

The author further argues that all participants should agree to the importance of viewing and validating the transactions. That is, read the blockchain and verify transactions. The need for transparency and distributed trust can be met by a blockchain.

The third criterion is based on the fitness to a set of diverse participants. If everyone knows and trust each other blockchain technology would not be necessary. In a global pharmaceutical supply chain, there would be a diversity of actors that do not have a default trust in each other.

The fourth criterion focus on the incentive to support the blockchain over time. Regarding the heavily regulated pharmaceutical industry there would be an incentive if regulatory authorities decides that everyone must use it. Some actors would still find it in their interest for other reasons. Pharmaceutical companies would find it in their interest if blockchain technology protects their brand and products against falsification. Cost reductions through disintermediation would also be an incentive. In a blockchain based pharmaceutical supply chain there would also be less dispute when deciding who is responsible for damages on products. It would be easier to locate where something went wrong and provide non-repudiation.

The last criterion is efficiency or whether there are enough participants and complexity to continue supporting the technology.

Going through these frameworks forces developers to consider relevant factors early in the development cycle.

5.9 What could have been done differently?

A wider search of the literature in the relevant research field may have resulted in a richer set of sources for reviewing the field.

A more thorough analysis of the models and experiences in the supply chain management field could have resulted in findings that could have been useful for integration with blockchain theory.

There are several industry projects exploring security focused blockchain-based pharmaceutical supply chains. Case studies involving these projects would probably have been informative.

A better focus on IoT-blockchain integration and sensor-to-blockchain security would have given more suggestions for developers in choosing designs. Consensus mechanisms based on DAG (directed acyclic graph) as used in the IOTA blockchain could have been discussed.

6 Conclusions

Although the prevalence of FSP in the supply chain is uncertain, it represents a significant threat to patients in most regions the world. Introducing new technology in supply chain security may be one factor that can improve the situation.

The research field of using blockchain technology to combat FSP is small but increasing in volume. The Western world may be underrepresented in the research effort in this field.

Most research in the field are still of a theoretical or conceptual nature and the proposals lack maturity with very little real-world implementations. This is also the case in related research fields where applying blockchain technology in supply chains are in focus.

There seem to be too little emphasis on the experience and models from supply chain management when making proposals on using blockchain technology to combat FSP.

Researchers in the field choose private and permissioned blockchains when designing solutions choosing speed and privacy over security and transparency.

The nature of the global pharmaceutical industry suggests further research into interoperability between different blockchains. A system of interoperable pharmaceutical blockchains each adapted to the local environment could be an interesting research topic.

Considering the most likely environment for a blockchain-based pharmaceutical supply chain, a consensus mechanism from the BFT family would probably be a better fit than a mechanism from the PoW family.

If designing a security focused blockchain-based pharmaceutical supply chain, a careful consideration of the characteristics of different consensus mechanisms is advantageous.

Developers planning to build a blockchain-based pharmaceutical supply chain will find it useful to use frameworks with listed criteria like in [95] and [98] as a starting point to evaluate if blockchain technology is the best option.

Bibliography

[1] WHO, *WHO Global Surveillance and Monitoring System for substandard and falsified medical products*. WHO, 2017.

[2] WHO, "A study on the public health and socioeconomic impact of substandard and falsified medical products," 2017.

[3] T. K. Mackey, R. Cuomo, C. Guerra, and B. A. Liang, "After counterfeit Avastin® - What have we learned and what can be done?," *Nat. Rev. Clin. Oncol.*, vol. 12, no. 5, pp. 302–308, 2015, doi: 10.1038/nrclinonc.2015.35.

[4] "Roche." [Online]. Available: www.roche.com. [Accessed: 04-May-2020].

[5] "Felleskatalogen Avastin." [Online]. Available: https://www.felleskatalogen.no/medisin/avastin-roche-546596. [Accessed: 04-May-2020].

[6] Z. P. Qureshi *et al.*, "Caveat Oncologist: Clinical Findings and Consequences of Distributing Counterfeit Erythropoietin in the United States," *J. Oncol. Pract.*, vol. 8, no. 2, pp. 84–90, 2012, doi: 10.1200/jop.2011.000325.

[7] L. Peña–Acevedo, A. F. Zuluaga, and A. Aristizabal–Solis, "A counterfeit multivitamin product inducing severe bleeding disorders in humans," *Clin. Toxicol.*, vol. 0, no. 0, pp. 1–3, 2020, doi: 10.1080/15563650.2019.1703999.

[8] A. Petersen, N. Held, and L. Heide, "Surveillance for falsified and substandard medicines in Africa and Asia by local organizations using the low-cost GPHF Minilab," pp. 1–22, 2017, doi: https:/doi.org/10.1371/journal.pone.0184165.

[9] F. Khuluza, "In-vitro evaluation of the quality of paracetamol and co-trimoxazole tablets used in Malawi based on pharmacopoeial standards," *Malawi Med. J.*, vol. 26, no. 2, pp. 38–41, 2014.

[10] I. Chikowe, D. Osei-Safo, J. J. E. K. Harrison, D. Y. Konadu, and I. Addae-Mensah, "Post-marketing surveillance of anti-malarial medicines used in Malawi," *Malar. J.*, vol. 14, no. 1, pp. 1–11, 2015, doi: 10.1186/s12936-015-0637-z.

[11] M. Tivura *et al.*, "Quality of Artemisinin-based Combination Therapy for malaria found in Ghanaian markets and public health implications of their use," *BMC Pharmacol. Toxicol.*, vol. 17, no. 1, pp. 1–10, 2016, doi: 10.1186/s40360-016-0089-2.

[12] M. El-Duah and K. Ofori-Kwakye, "Substandard artemisinin-based antimalarial medicines in licensed retail pharmaceutical outlets in Ghana," *J. Vector Borne Dis.*, vol. 49, no. 3, pp. 131–139, 2012.

[13] D. Nabirova *et al.*, "Assessment of the quality of anti-tuberculosis medicines in Almaty, Kazakhstan, 2014," *Int. J. Tuberc. Lung Dis.*, vol. 21, no. 10, pp. 1161–1168, 2017, doi: 10.5588/ijtld.17.0074.

[14] A. N. Khan, R. K. Khar, and M. Udayabanu, "Pilot study of quality of diclofenac generic products using validated in-house method: Indian drug regulatory concern," *J. Appl. Pharm. Sci.*, vol. 5, no. 12, pp. 147–153, 2015, doi: 10.7324/JAPS.2015.501226.

[15] E. Medina, E. Bel, and J. M. Suñé, "Counterfeit medicines in Peru: A retrospective review (1997-2014)," *BMJ Open*, vol. 6, no. 4, 2016, doi: 10.1136/bmjopen-2015-

010387.

[16] A. T. Mori, E. Meena, and E. A. Kaale, "Economic cost of substandard and falsified human medicines and cosmetics with banned ingredients in Tanzania from 2005 to 2015: A retrospective review of data from the regulatory authority," *BMJ Open*, vol. 8, no. 6, pp. 1–7, 2018, doi: 10.1136/bmjopen-2018-021825.

[17] J. Chiang, F. A. Yafi, P. J. Dorsey, and W. J. G. Hellstrom, "The dangers of sexual enhancement supplements and counterfeit drugs to 'treat' erectile dysfunction," *Transl. Androl. Urol.*, vol. 6, no. 1, pp. 12–19, 2017, doi: 10.21037/tau.2016.10.04.

[18] M. S. Rahman *et al.*, "The health consequences of falsified medicines- A study of the published literature," *Trop. Med. Int. Heal.*, vol. 23, no. 12, pp. 1294–1303, 2018, doi: 10.1111/tmi.13161.

[19] T. Kelesidis and M. E. Falagas, "Substandard/counterfeit antimicrobial drugs," *Clin. Microbiol. Rev.*, vol. 28, no. 2, pp. 443–464, 2015, doi: 10.1128/CMR.00072-14.

[20] A. Koczwara and J. Dressman, "Poor-Quality and Counterfeit Drugs: A Systematic Assessment of Prevalence and Risks Based on Data Published From 2007 to 2016," *J. Pharm. Sci.*, vol. 106, no. 10, pp. 2921–2929, 2017, doi: 10.1016/j.xphs.2017.05.018.

[21] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. [Online]. Available: https://bitcoin.org/en/bitcoin-paper. [Accessed: 22-Apr-2020].

[22] "Coinmarketcap." [Online]. Available: coinmarketcap.com. [Accessed: 30-Apr-2020].

[23] Ethereum, "Ethereum Hompage." [Online]. Available: ethereum.org. [Accessed: 24-Apr-2020].

[24] "Hyperledger," *The Linux Foundation*. [Online]. Available: https://www.hyperledger.org/. [Accessed: 06-May-2020].

[25] M. M. Queiroz, R. Telles, and S. H. Bonilla, "Blockchain and supply chain management integration: a systematic review of the literature," *Supply Chain Manag.*, vol. 25, no. 2, pp. 241–254, 2019, doi: 10.1108/SCM-03-2018-0143.

[26] M. L. Di Silvestre *et al.*, "Blockchain for power systems: Current trends and future applications," *Renew. Sustain. Energy Rev.*, vol. 119, no. January 2019, 2020, doi: 10.1016/j.rser.2019.109585.

[27] Y. Wang, J. H. Han, and P. Beynon-Davies, "Understanding blockchain technology for future supply chains: a systematic literature review and research agenda," *Supply Chain Manag.*, vol. 24, no. 1, pp. 62–84, 2019, doi: 10.1108/SCM-03-2018-0148.

[28] F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues," *Telemat. Informatics*, vol. 36, no. November 2018, pp. 55–81, 2019, doi: 10.1016/j.tele.2018.11.006.

[29] S. Makridakis and K. Christodoulou, "Blockchain : Current Challenges and Future Prospects / Applications," *Futur. Internet*, pp. 1–16, 2019.

[30] A. Gurtu and J. Johny, "Potential of blockchain technology in supply chain management: a literature review," *Int. J. Phys. Distrib. Logist. Manag.*, vol. 49, no. 9, pp. 881–900, 2019, doi: 10.1108/IJPDLM-11-2018-0371.

[31] F. Antonucci, S. Figorilli, C. Costa, F. Pallottino, L. Raso, and P. Menesatti, "A review on blockchain applications in the agri-food sector," *J. Sci. Food Agric.*, vol.

99, no. 14, pp. 6129–6138, 2019, doi: 10.1002/jsfa.9912.

[32] H. Feng, X. Wang, Y. Duan, J. Zhang, and X. Zhang, "Applying blockchain technology to improve agri-food traceability: A review of development methods, benefits and challenges," *J. Clean. Prod.*, vol. 260, p. 121031, 2020, doi: 10.1016/j.jclepro.2020.121031.

[33] K. Gopi, D. Mazumder, J. Sammut, and N. Saintilan, "Determining the provenance and authenticity of seafood: A review of current methodologies," *Trends Food Sci. Technol.*, vol. 91, no. June, pp. 294–304, 2019, doi: 10.1016/j.tifs.2019.07.010.

[34] J. F. Galvez, J. C. Mejuto, and J. Simal-Gandara, "Future challenges on the use of blockchain for food traceability analysis," *TrAC - Trends Anal. Chem.*, vol. 107, pp. 222–232, 2018, doi: 10.1016/j.trac.2018.08.011.

[35] J. Astill *et al.*, "Transparency in food supply chains: A review of enabling technology solutions," *Trends Food Sci. Technol.*, vol. 91, no. July, pp. 240–247, 2019, doi: 10.1016/j.tifs.2019.07.024.

[36] V. Astarita, V. P. Giofrè, G. Mirabelli, and V. Solina, "A Review of Blockchain-Based Systems in Transportation," *Inf.*, vol. 11, no. 1, pp. 1–24, 2020, doi: 10.3390/info11010021.

[37] E. Tijan, S. Aksentijević, K. Ivanić, and M. Jardas, "Blockchain technology implementation in logistics," *Sustain.*, vol. 11, no. 4, 2019, doi: 10.3390/su11041185.

[38] L. Lao, Z. Li, S. Hou, B. Xiao, S. Guo, and Y. Yang, "A survey of IoT applications in blockchain systems: Architecture, consensus, and traffic modeling," *ACM Comput. Surv.*, vol. 53, no. 1, 2020, doi: 10.1145/3372136.

[39] J. Sengupta, S. Ruj, and S. Das Bit, "A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT," *J. Netw. Comput. Appl.*, vol. 149, no. September 2019, p. 102481, 2020, doi: 10.1016/j.jnca.2019.102481.

[40] M. Mettler, "Blockchain technology in healthcare: The revolution starts here," *2016 IEEE 18th Int. Conf. e-Health Networking, Appl. Serv. Heal. 2016*, pp. 1–3, 2016, doi: 10.1109/HealthCom.2016.7749510.

[41] T. K. Mackey and G. Nayyar, "A review of existing and emerging digital technologies to combat the global trade in fake medicines," *Expert Opin. Drug Saf.*, vol. 16, no. 5, pp. 587–602, 2017, doi: 10.1080/14740338.2017.1313227.

[42] Bitcoin Project, "bitcoin.org." [Online]. Available: bitcoin.org. [Accessed: 24-Apr-2020].

[43] M. Van Steen and A. S. Tananbaum, *Distributed Systems 3rd. Ed*, 3rd. Maarten van Steen, 2018.

[44] The Editors of Encyclopaedia Britannica, "Bookkeeping," *Encyclopædia Britannica*. 2002.

[45] R. C. Merkle, "A digital signature based on a conventional encryption function," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence*, 1988, doi: 10.1007/3-540-48184-2_32.

[46] W. Stallings and L. Brown, *Computer Security Principles and Practice*, 3rd ed. Pearson Education Limited, 2015.

[47] G. J. Simmons, "Public-key cryptography," *Encyclopædia Britannica Inc.*, 2020. [Online]. Available: https://www.britannica.com/topic/public-key-cryptography. [Accessed: 23-Apr-2020].

[48] D. Drescher, *Blockchain Basics: A Non-Technical Introduction in 25 Steps*, 1st ed. Frankfurt am Main: Apress, 2017.

[49] I. Bashir, *Mastering Blockchain*, 1st ed. Birmingham - Mumbai: Packt Publishing Ltd., 2017.

[50] S. Bano *et al.*, "Consensus in the Age of Blockchains," 2017.

[51] T. B. Group, "Public versus Private Blockchains," 2015. [Online]. Available: https://bitfury.com/content/downloads/public-vs-private-pt1-1.pdf. [Accessed: 19-May-2020].

[52] S. Gilbert and N. Lynch, "Perspectives on the CAP Theorem," *Computer (Long. Beach. Calif).*, vol. 45, no. 2, pp. 30–36, 2012, doi: 10.1109/mc.2011.389.

[53] S. van Laar, "A shortcoming of blockchain: the scalability trilemma," 2019. .

[54] A. G. Arway, *Supply Chain Security: A Comprehensive Approach*, 1st ed. CRC Press, 2013.

[55] N. R. Sanders, "Supply Chain Management A Global Perspective," 2.ed, Ed. Wiley, 2018.

[56] D. Stanton, *Supply Chain Management for Dummies*, Kindle Edi. Wiley, 2018.

[57] D. Bansal, S. Malla, K. Gudala, and P. Tiwari, "Anti-counterfeit technologies: A pharmaceutical industry perspective," *Sci. Pharm.*, vol. 81, no. 1, pp. 1–13, 2013, doi: 10.3797/scipharm.1202-03.

[58] K. M. Botcha, V. V. Chakravarthy, and A. Anurag, "Enhancing traceability in pharmaceutical supply chain using internet of things (iot) and blockchain," *Proc. - 2019 IEEE Int. Conf. Intell. Syst. Green Technol. ICISGT 2019*, pp. 45–48, 2019, doi: 10.1109/ICISGT44072.2019.00025.

[59] R. Azzi, R. K. Chamoun, and M. Sokhn, "The power of a blockchain-based supply chain," *Comput. Ind. Eng.*, vol. 135, no. May, pp. 582–592, 2019, doi: 10.1016/j.cie.2019.06.042.

[60] J. W. Dailey, "Pharmaceutical industry," *Encyclopædia Britannica*, 2018. [Online]. Available: https://www.britannica.com/technology/pharmaceutical-industry/Obstacles-in-drug-development. [Accessed: 20-Mar-2020].

[61] M. Mikulic, "Global pharmaceutical sales from 2017 to 2019, by region (in billons U.S. dollars)," *Statista*, 2020. [Online]. Available: https://www.statista.com/statistics/272181/world-pharmaceutical-sales-by-region/. [Accessed: 29-Apr-2020].

[62] M. Mikulic, "Pfizer - Statistics & Facts," *Statista*, 2020. [Online]. Available: https://www.statista.com/topics/1394/pfizer/. [Accessed: 29-Apr-2020].

[63] M. Gusenbauer and N. R. Haddaway, "Which academic search systems are suitable for systematic reviews or meta-analyses? Evaluating retrieval qualities of Google Scholar, PubMed, and 26 other resources," *Res. Synth. Methods*, no. September 2019, 2019, doi: 10.1002/jrsm.1378.

[64] A. W. Harzing and S. Alakangas, "Google Scholar, Scopus and the Web of Science: a longitudinal and cross-disciplinary comparison," *Scientometrics*, vol. 106, no. 2, pp. 787–804, 2016, doi: 10.1007/s11192-015-1798-9.

[65] A. Martín-Martín, E. Orduna-Malea, M. Thelwall, and E. Delgado López-Cózar, "Google Scholar, Web of Science, and Scopus: A systematic comparison of citations in 252 subject categories," *J. Informetr.*, vol. 12, no. 4, pp. 1160–1177, 2018, doi: 10.1016/j.joi.2018.09.002.

[66] H. Snyder, "Literature review as a research methodology: An overview and guidelines," *J. Bus. Res.*, vol. 104, no. March, pp. 333–339, 2019, doi: 10.1016/j.jbusres.2019.07.039.

[67] M. Sahoo, S. S. Singhar, B. Nayak, and B. K. Mohanta, "A Blockchain Based Framework Secured by ECDSA to Curb Drug Counterfeiting," *2019 10th Int. Conf. Comput. Commun. Netw. Technol. ICCCNT 2019*, pp. 1–6, 2019, doi: 10.1109/ICCCNT45670.2019.8944772.

[68] M. Grest, M. Lauras, A. Montarnal, A. Sarazin, and G. Bousseau, "A Meta Model for a Blockchain-based Supply Chain Traceability," *2019 Int. Conf. Ind. Eng. Syst. Manag.*, pp. 1–6, 2019.

[69] F. Jamil, L. Hang, K. H. Kim, and D. H. Kim, "A novel medical blockchain model for drug supply chain integrity management in a smart hospital," *Electron.*, vol. 8, no. 5, pp. 1–32, 2019, doi: 10.3390/electronics8050505.

[70] R. Raj, N. Rai, and S. Agarwal, "Anticounterfeiting in Pharmaceutical Supply Chain by establishing Proof of Ownership," *IEEE Reg. 10 Annu. Int. Conf. Proceedings/TENCON*, vol. 2019-Octob, pp. 1572–1577, 2019, doi: 10.1109/TENCON.2019.8929271.

[71] R. Anand, K. Niyas, S. Gupta, and S. Revathy, *Anti-counterfeit on medicine detection using blockchain technology*, vol. 89. Springer Singapore, 2020.

[72] M. Chanson, A. Bogner, D. Bilgeri, E. Fleisch, and F. Wortmann, "Blockchain for the IoT: Privacy-preserving protection of sensor data," *J. Assoc. Inf. Syst.*, vol. 20, no. 9, pp. 1271–1307, 2019, doi: 10.17705/1jais.00567.

[73] M. et al Azeem, *Blockchain Based Decentralized Authentication and Lincensing Process of Medicine*, vol. 1. Springer International Publishing, 2020.

[74] P. Sylim, F. Liu, A. Marcelo, and P. Fontelo, "Blockchain technology for detecting falsified and substandard drugs in distribution: Pharmaceutical supply chain intervention," *J. Med. Internet Res.*, vol. 20, no. 9, pp. 1–12, 2018, doi: 10.2196/10163.

[75] S. R. Bryatov and A. A. Borodinov, "Blockchain technology in the pharmaceutical supply chain: Researching a business model based on Hyperledger Fabric," *CEUR Workshop Proc.*, vol. 2416, pp. 134–140, 2019, doi: 10.18287/1613-0073-2019-2416-134-140.

[76] A. Kumar, D. Choudhary, M. S. Raju, D. K. Chaudhary, and R. K. Sagar, "Combating counterfeit drugs: A quantitative analysis on cracking down the fake drug industry by using blockchain technology," *Proc. 9th Int. Conf. Cloud Comput. Data Sci. Eng. Conflu. 2019*, pp. 174–178, 2019, doi: 10.1109/CONFLUENCE.2019.8776891.

[77] L. Nørfeldt, J. Bøtker, M. Edinger, N. Genina, and J. Rantanen, "Cryptopharmaceuticals: Increasing the Safety of Medication by a Blockchain of Pharmaceutical Products," *J. Pharm. Sci.*, vol. 108, no. 9, pp. 2838–2841, 2019, doi: 10.1016/j.xphs.2019.04.025.

[78] Y. Huang, J. Wu, and C. Long, "Drudgeledger: A Practical Blockchain System for Drug Traceability and Regulation," in *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 2018, pp. 1349–1354, doi: 10.1109/Cybermatics.

[79] J. H. Tseng, Y. C. Liao, B. Chong, and S. W. Liao, "Governance on the drug supply chain via gcoin blockchain," *Int. J. Environ. Res. Public Health*, vol. 15, no. 6, 2018, doi: 10.3390/ijerph15061055.

[80] P. Pandey and R. Litoriya, "Securing E-health Networks from Counterfeit Medicine Penetration Using Blockchain," *Wirel. Pers. Commun.*, no. 0123456789, 2020, doi: 10.1007/s11277-020-07041-7.

[81] V. Plotnikov and V. Kuznetsova, "The Prospects for the Use of Digital Technology 'blockchain' in the Pharmaceutical Market," *MATEC Web Conf.*, vol. 193, pp. 1–6, 2018, doi: 10.1051/matecconf/201819302029.

[82] R. Kumar and R. Tripathi, "Traceability of counterfeit medicine supply chain through Blockchain," *2019 11th Int. Conf. Commun. Syst. Networks, COMSNETS 2019*, vol. 2061, no. 1, pp. 568–570, 2019, doi: 10.1109/COMSNETS.2019.8711418.

[83] Archa, B. Alangot, and K. Achuthan, "Trace and track: Enhanced pharma supply chain infrastructure to prevent fraud," *Lect. Notes Inst. Comput. Sci. Soc. Telecommun. Eng. LNICST*, vol. 218, no. 1, pp. 189–195, 2018, doi: 10.1007/978-3-319-73423-1_17.

[84] J. C. Molina, D. T. Delgado, and G. Tarazona, *Using Blockchain for Traceability in the Drug Suppy Chain*, vol. 1. Springer International Publishing, 2019.

[85] E. Muzzy and M. Anderson, "Avoiding Blockchain Balkanization," *Consensys*. [Online]. Available: https://consensys.net/research/avoiding-blockchain-balkanization/. [Accessed: 21-May-2020].

[86] "The Cosmos Network." [Online]. Available: https://cosmos.network/. [Accessed: 21-May-2020].

[87] "The Polkadot Network." [Online]. Available: https://polkadot.network/. [Accessed: 21-May-2020].

[88] M. Vukolić, T. Quest, B. Fabric, and P. Bft, "The Quest for Scalable Blockchain Fabric : Proof-of-Work vs . BFT Replication Marko Vukolić To cite this version : HAL Id : hal-01445797 The Quest for Scalable Blockchain Fabric :," 比较类论文, 2017.

[89] "Crushcrypto." [Online]. Available: https://crushcrypto.com/what-is-practical-byzantine-fault-tolerance/. [Accessed: 23-May-2020].

[90] S. Ferdous, M. Jabed, M. Chowdhury, M. A. Hoque, and A. Colman, "Blockchain Consensus Algorithms : A Survey," pp. 1–39.

[91] S. Fabian and L. Daniel, "BITSHARES 2.0: GENERAL OVERVIEW," 2017. [Online]. Available: https://cryptorating.eu/whitepapers/BitShares/bitshares-general.pdf. [Accessed: 23-May-2020].

[92] EOS, "EOS." [Online]. Available: eos.io. [Accessed: 24-Apr-2020].

[93] "Ethereum. Transactions per second." [Online]. Available: https://blockchair.com/ethereum/charts/transactions-per-second?interval=1m. [Accessed: 21-May-2020].

[94] "Ethereum 2.0." [Online]. Available: https://consensys.net/blog/blockchain-explained/what-is-ethereum-2/. [Accessed: 21-May-2020].

[95] S. K. Lo, X. Xu, Y. K. Chiam, and Q. Lu, "Evaluating Suitability of Applying Blockchain," *Proc. IEEE Int. Conf. Eng. Complex Comput. Syst. ICECCS*, vol. 2017-Novem, pp. 158–161, 2018, doi: 10.1109/ICECCS.2017.26.

[96] "VISA." [Online]. Available: https://usa.visa.com/dam/VCOM/download/corporate/media/visanet-technology/aboutvisafactsheet.pdf. [Accessed: 21-May-2020].

[97] "News Bitcoin." [Online]. Available: https://news.bitcoin.com/no-visa-doesnt-handle-24000-tps-and-neither-does-your-pet-blockchain/. [Accessed: 21-May-2020].

[98] B. A. Scriber, "A Framework for Determining Blockchain Applicability," IEEE Software, pp. 70–77, 2018.

NTNU

Norwegian University of
Science and Technology