University of Zurich[UZH]

MASTER THESIS – Communication Systems Group, Prof. Dr. Burkhard Stiller

Reducing Counterfeit Products with Blockchains

Sacha Uhlmann
Zürich, Switzerland
09-608-076

Supervisor: Dr. Thomas Bocek, Andri Lareida
Date of Submission: 15.01.2017

University of Zurich
Department of Informatics (IFI)
Binzmühlestrasse 14, CH-8050 Zurich, Switzerland

ifi

Master Thesis
Communication Systems Group (CSG)
Department of Informatics (IFI)
University of Zurich
Binzmühlestrasse 14, CH-8050 Zurich, Switzerland
URL: http://www.csg.uzh.ch/

Zusammenfassung

Fälschungen führen zu grossen finanziellen Verlusten, nicht nur für Produzenten, sondern auch für das Gemeinwohl durch Steuerausfälle. Im Falle von pharmazeutischen Produkten können die Konsequenzen schwerwiegender und nicht nur finanziell sein: Gefälschte Produkte können keine oder falsche aktive Inhaltsstoffe beinhalten und deshalb von wirkungslos bis schädlich sein. Speziell aus Entwicklungsländern wird von tödlichen Folgen durch gefälschte Pharmazeutika berichtet.

Blockchain-Technologien entwickelten sich über die letzten Jahre. Der meist entwickelte und verwendete Anwendungsfall beinhaltet finanzielle Transaktionen. Jedoch hat die Blockchain-Technologie das Potential andere Märkte zu revolutionieren. Sie ermöglicht ohne Mittelspersonen oder -institutionen effizient zu operieren, erlaubt schnellere Transaktionen und grössere Transparenz.

Diese Arbeit erforscht die Möglichkeit, Fälschungen mit Hilfe der Blockchain-Technologie zu reduzieren. Sie wird in Zusammenarbeit mit modum.io AG ausgeführt. modum.io ist eine Startup-Firma, welche sich auf die Temperaturüberwachung von pharmazeutischen Produkten mit Blockchain-Technologie spezialisiert hat.

Diese Arbeit liefert eine Übersicht über Produkte und Firmen auf dem Gebiet der Bekämpfung von Fälschungen. Verschiedene Blockchain-Technologien und welche ihrer Charakteristiken besonders interessant sind für den Einsatz von Fälschungssicherheit werden vorgestellt.

Drei verschiedene Konzepte werden entwickelt und ein Konzept, die Erweiterung des existierenden modum.io System, wird weiterverfolgt. Es zeigt sich, dass die Reduzierung von Fälschungen nicht ausschliesslich mit technologischen Mitteln erreicht werden kann. Konsumenten sensibilisieren, Fälscher mit rechtlichen Schritten bekämpfen, ein gutes Warnsystem und manipulationssichere Verpackungen verwenden, sind alles wichtige Aspekte. Diese Faktoren kombiniert mit Blockchain-Technologien erlauben einen effizienten und ganzheitlichen Ansatz zur Bekämpfung von Fälschungen.

Abstract

Counterfeits result in major financial losses, not only to manufacturers, but they also reduce the general welfare due to missed tax revenue. In case of pharmaceutical products, the implications are more severe than monetary: counterfeit products might not contain the right active ingredients and therefore be useless to harmful. Especially in developing countries, fatal consequences of counterfeited pharmaceuticals are reported.

Blockchain technologies have emerged over the last years. While the most explored use case is financial transactions, it has the potential to disrupt other markets. Blockchains remove the need for trusted intermediaries, can facilitate faster transactions and add more transparency.

This thesis explores the possibility to reduce counterfeit using blockchain technology. It is conducted in cooperation with modum.io AG. modum.io is a startup which uses blockchain technology to ensure that pharmaceuticals are transported within the allowed temperature range.

This thesis provides an overview of different solutions in the anti-counterfeit area, different blockchain technologies and what characteristics make blockchains especially interesting for the use case.

Three different concepts are developed and one concept, the expansion of an existing system, is pursued further. It is shown, that reducing counterfeits cannot be achieved by using technological means only. Increasing awareness, fighting counterfeiters on a legal level, a good alert system, and having tamper-proof packaging are all important aspects. These factors combined with blockchain technology can lead to an efficient and holistic approach to reduce counterfeiting.

Acknowledgments

I want to thank Prof. Dr. Burkhard Stiller and all of the Communication System Research Group for providing the opportunity to write this thesis. Thanks to Andri Lareida for co-supervising this thesis.

Special thanks to my supervisor Thomas Bocek, for all the inputs, the discussions and expertise shared with me.

I also want to thank the whole team of modum.io, especially Andreas Keller and Tim Strasser for sharing all their technical expertise with me and Malik El Bay for the inspiration and motivation.

I also want to thank all the other people that I met during the six months of working on this thesis for all the insights and inspirational discussions. Without this, I would not have been able to complete this thesis.

Contents

Chapter 1

Introduction

Trust is a central element in all transactions. No matter if sending money or exchanging goods, it becomes difficult if there is no trust between the entities involved. It becomes even more difficult, as with many transactions, third parties are involved, such as banks. Often, not only one third-party is involved in a transaction, but multiple. An international money transfer does not only include the bank of the sender, the bank of the receiver, but also multiple intermediary entities such as clearing houses. The entities involved in the transaction do not only have to trust each other, but also the third parties. Removing these third parties can decrease transaction cost, facilitate faster transactions and add more transparency.

Bitcoin has successfully shown that removing such third-parties is possible. The cryptocurrency permits direct sending coins to a transaction partner, without the need to use banks and clearing houses. The assets are directly transferred from one account to another. There are no intermediaries and thereby no need to trust third parties. In addition, the question if a transaction is valid is not answered by an institution, but by algorithms used. Therefore, it completely removes the need to trust any third party.

The technology behind Bitcoin, the blockchain, can however not only be used for financial transactions and crypto currencies in general. The technology has potential to "redefine the digital economy" [93], because it allows immutable transactions, which can be checked at all times from everyone. This is because the information is publicly available and distributed globally. It is "chronologically updated and cryptographically sealed" [31]. The full range of applicable use cases for this technology has to be seen, but tracking ownership and history of a product is surely one of them [47]. This thesis explores the possibility to reduce counterfeit using blockchain technology.

1.1 Motivation

The OECD estimates that the international trade volume of counterfeited products was up to $200 billion in 2005 [74]. This does not include counterfeit products which were sold in the same country as produced nor Internet piracy. The number is alarming, as

this does not only lead to lost revenue for manufacturers, but also tax losses and thereby a reduction of general welfare. Typical products being counterfeited do not only include high-value luxury goods such as designer clothing, footwear, watches and jewelery, but a wide range of more common products. The list can be expanded to consumer electronics, other electrical components, food, drinks, tobacco, agricultural products, toiletry products and pharmaceuticals. In case of pharmaceutical products, the implications are more severe than monetary: counterfeit products might not contain the right active ingredients and therefore can be useless to harmful. Especially in developing countries, people are dying after being treated with fake medicine [3]. Fake pharmaceuticals are however not only a threat in developing countries, according to the World Health Organization (WHO) over 34 million counterfeited pills were seized in two months in 2009 [101].

Considering the potentially fatal and financial consequences, it is not surprising that global efforts to reduce counterfeit are in place. However, there is no evidence that the number was reduced in the last few years. Blockchain technologies are considered trustless, immutable and globally distributed. The question arises, how this technology can be used in the fight against piracy, what characteristics are helpful and how a potential solution can be implemented

1.2 Description and Context of Work

This thesis is conducted in cooperation with modum.io AG. modum.io is a startup which uses blockchain technology to ensure that pharmaceuticals are transported within the allowed temperature range. It was founded in 2016, following a regulation change in the EU which also affects Switzerland. It states that all prescription medicines have to be temperature monitored. This collaboration with modum.io helped with blockchain and market expertise, but also pushed the thesis into a pharmaceutical direction. While the considered approaches can be applicable in different sectors, it was important that the solution can also be applied in a pharmaceutical context. As modum.io was participating in the start-up accelerator "Kickstart Accelerator"[1] during this thesis, plenty of work was performed which was not directly related to this thesis, such as improving the existing system, helping with finding and fixing bugs as well as other issues.

The work conducted is multilateral. First of all, an overview of existing solutions in the anti-counterfeit space is provided. Different blockchain implementations are considered and it is evaluated if they are useful for reducing counterfeit. The main challenge with blockchain technologies as of the time of writing this thesis is not the lack of different approaches, but the maturity of products. In a second step, regulation changes to reduce counterfeit pharmaceuticals in the European market as well as the United States are considered and discussed. The question if a legal compliant system can be built and if there is a possibility to bring it to market is answered. As the subject of this thesis is broader than just considering the chances introduced by upcoming legal changes, different approaches are developed which help with reducing counterfeit in different segments. Finally, one of these approaches is pursued in more depth and evaluated, both in regards of impact to the existing system and if it can ultimately reduce counterfeits.

[1] `http://kickstart-accelerator.com/`

1.3 Thesis Outline

This thesis is structured as follows: Chapter 2 introduces the related work on the subject. This includes anti-counterfeit systems which are based on blockchain and other technologies. Different blockchain implementations are analyzed and evaluated in regard of a potential solution in Chapter 3. In Chapter 4, recent legislation changes in the pharmaceutical sector are discussed, which open potential markets for solutions. One of the considered solutions is based on the legislation changes, others systems are considered as well. These potential solutions, as well as who could benefit from them and the impact on potential implementations are discussed in Chapter 5. It also contains the reasoning and final decision which system to push forward. In Chapter 6, the chosen approach and the needed changes to the existing system are introduced in more depth. Chapter 7 evaluates the impact of these changes, how they can help to reduce counterfeits and the role of the blockchain. This thesis concludes with Chapter 8, including the key findings, an overview of achievements and potential future work.

Chapter 2

Related Work

Several anti-counterfeit solutions already exist. In this section, general approaches are first introduced, to then discuss products which are available in the market. Due to the context of this thesis, the focuses is on approaches and solutions which either use blockchain technology, focus on pharmaceuticals, or do both.

2.1 General Approaches to Reduce Counterfeit

Anti-counterfeiting solutions should protect organizations from financial and reputation losses, and, especially in the case of pharmaceutical products, customer safety. [59] argues that good anti-counterfeiting techniques should generally be simple to apply, but difficult to imitate and have four main features: They should be difficult to duplicate, it should be possible to identify them without special equipment, it should be difficult to re-use them, and it should be visible if they where tampered with.

From a product perspective, there are three general technologies to reduce counterfeits [59]:

Overt:
Overt technologies include all packaging technologies which are visible in the product itself. This includes holograms, color shifting inks, security threads, water marks etc. The advantage of overt technologies is that they can be checked by the end-consumer.

Covert:
Covert technologies are also applied on the product itself, but are not identifiable without special equipment. This includes UV, bi-fluorescent and pen-reactive ink, as well as digital watermarks and hidden printed messages. Covert technologies help to identify counterfeits in the supply-chain and are especially efficient combined with overt technologies.

Track and trace:
The final category is track and trace. This includes Radio Frequency Identification (RFID) tags, Electronic Product Codes (EPCs) and barcodes. Track and trace technologies allow for simpler tracing of products, thereby enabling the reduction of counterfeits, as the history of a product is available. The tag or barcode is included by the manufacturer. Distributors scan the identification, enabling them to check the authenticity of the product and update the status. Finally, retailers can also scan the product, to check the history and authenticity of the product. This approach does not only tackle the counterfeit problem, but also enables track and trace through the whole product lifecycle.

Protecting the production is, however, not enough to decrease counterfeiting. [5, 32] have identified further factors to reduce counterfeits:

Budgeting to monitor, deter, and remove counterfeits [5]:
Companies need to ensure that they have the legal protection and registrations in place to be protected against counterfeits, this includes trademarks, copyrights, design patents etc. With this in place, it can still be costly to actively fight against counterfeits. Especially luxury goods companies spend millions to actively fight counterfeits and work together with private investigators. Having a budget for acting upon counterfeits is therefore important.

Controlling outsource suppliers [5]:
Many companies use outsourced suppliers. This opens the risk that the outsourced supplier will not only produce legitimate products, but also counterfeits, with having access to all the original assets. Outsourcers should be carefully evaluated and monitored. Another option is to not outsource the whole product to one company, but split the product manufacturing to multiple companies, or keep part of the production in-house. This ensures, that no single external company has all the assets to create counterfeited products. If must also be ensured, that upon contract termination, all assets are returned to the outsourcing company.

Developing early warning signals of counterfeiting [5]:
Counterfeits are often not discovered for a significant time. This leads to issues, as the longer counterfeits have been available, the more they can spread and finding the source becomes more difficult. Organizations therefore should have warning signals in place to identify counterfeits.

Increase Awareness [32]:
Approaches which help to identify counterfeits do not help, if there is no awareness of the issue with counterfeits. Especially critical for pharmaceuticals, the public must be aware of the risk of counterfeited products.

Legal actions to reduce counterfeits [5]:
If counterfeiters or sellers of counterfeits are identified, it is important for the genuine manufacturer to take legal actions. The operations must be shut down and the counterfeited products seized.

Reducing gray market activity [5]:

Counterfeits often enter the market from unauthorized resellers. It is estimated, that pharmaceuticals can go through 20-30 countries before being sold. At every step, there is the risk that counterfeits are introduced.

Reducing gray market activity is however not trivial. It requires distributors and customers to be aware of the gray market risks and not participate in them.

Support of the analytics [32]:

If a product is suspected to be a counterfeit, it should be analyzed as soon as possible. This typically starts with a visual inspection of the packaging, the packaging content (such as leaflets) and the medicine itself. If the product turns out to be counterfeited, the risk should be evaluated and patients informed. Furthermore, law agencies should take the requisite steps to identify were the counterfeit has come from and act upon it. This fights counterfeit by increasing awareness and by fighting criminal organizations introducing counterfeits.

2.2 Blockchain Based Anti-Counterfeit Solutions

Even though blockchain is still a rather new technology, there are already multiple organizations which are using the technology. Even multiple solutions in the anti-counterfeit space exist, which are introduced in this section.

Blockverify

Blockverify is an anti-counterfeit blockchain solution. It is developed by Venture Proxy Ltd., an organization founded in 2014 and based in London, UK [10].

Blockverify offers global solutions to identify counterfeits, using blockchain technology to prevent duplicates and allows companies themselves to create products and monitor supply chains [7]. They target luxury items, diamonds, electronics as well as the pharmaceutical market.

The process they use is simple [7]. Each product which is tracked by Blockverify has an Blockverify tag and is tracked along the supply chain. It is up to the customer to define how transparent the supply chain is. Retailers can check that received goods are genuine. Once a product is sold, the consumer can also verify if it is authentic and activate the ownership of the product. As the transactions are stored in the blockchain, it cannot be corrupted, even by the manufacturers themselves. Blockverify can provide “verified history” of each product in its system.

They use the Bitcoin and a private blockchain to store the information. The combination of both allows them to ensure that only they control which information is publicly available, and which can only be accessed by them. [50]. According to an bitcoinist.com article, they have run a pilot program with an UK subsidiary of a Swiss pharmaceutical company [12].

Chronicled

Chronicled Inc. is a San Francisco based organization founded in 2014. They received fundings of $1.4m and $3.4m in 2015 respectively 2016 [24, 80]. They are working on solutions to link physical goods to the blockchain [26]. They started with a the goal to eliminate counterfeit sneakers [81, 27], but broadened their target-market significantly.

Their initial use case of sneakers was simple: Using smart tags and the Chronicled App, users can claim their sneakers, check if their are authentic and keep track of their collection using the App [27]. They generalized this approach by autumn 2016 and offer services for all sorts of products. Example use cases include furniture showrooms, art, wine and sneakers.

Chronicled offers "identity inlays and tamper-evident cryptographic seals" , which allow to link physical goods with the blockchain [26]. They offer both BLE and NFC cryptographic chips, which sign all transactions, before they are stored in a public blockchain. Manufacturers can include the microchips during the production process or at a later stage and use the Chronicled App to register the product in the Blockchain. Consumers can then use the Chronicled App to check the authenticity of a product. Their offer does not only include the cryptographic chips, but also subscription based access to there platform and App [26].

In August 2016 Chronicled has also launched an "Open Registry for the Internet of Everything" [25]. This Ethereum based platform service is publicly accessible and aims "to make private IoT registries interoperable" [48]. While the Open Registry uses Ethereum, Chronicled consider themselves as "blockchain agnostic", currently supporting Ethereum but with plans to support others such as Bitcoin, Z Cash, Hyperledger, and Symbiont [26].

Everledger

Everledger is a London based startup with the goal to combat fraud [60]. They describe themselves as a "fraud description system, overlaying big data from closed sources" [38]. Unlike the previous discussed providers, Everledger has a strong focus on insurance fraud and does not only target owners of products, but also insurance companies, claimants and law enforcement. It currently focuses on diamonds. Diamonds have the advantage, that they there is no need to add additional tags to a diamond to identify it, as they can be uniquely identified by 40 different data points [19].

To ensure data authenticity and still allow for complex smart contracts, Everledger combines private blockchains with public blockchains. They use the Eris stack as private blockchain and Bitcoins blockchain for ensuring immutability of the transaction history. They also have plans for supporting the Ethereum blockchain, once it "moves out of the test phase" [39].

Provenance

Provenance, developed by Project Provenance Ltd., is another blockchain solution which allows to track the origin of a product. Provenance is not marketed as an anti-counterfeit solution, but rather focus on traceability and transparency of products [75]. Their solution enables tracing the history of a product, starting with the production and including all steps in the supply chain [77]. All information is stored on a public blockchain, and therefore not mutable. While their main selling point is added value and trust from transparency of a product, it still prevents counterfeits, as products in the system cannot be changed afterwards and can be tracked to the origin of the production.

The process of Provenance is simply: Organizations can sign up wit Provenance, add products and the stories of the products and company, and issue batches of items. Each physical product is to be identified with a unique ID, which allows customers to check the story and digital history of the product. Similar to Chronicled, they use the Ethereum blockchain as a secure and open registry [79]. They use the blockchain due to the inter-operable, auditable and cost-efficient structure. Furthermore, it is publicly available and the blockchain has guaranteed continuity, which ensures that it cannot be turned off by a single entity [85].

Provenance has successfully proven their concept by tracking tuna on the blockchain, a industry which is well-known for human rights abuse [58]. The pilot included three phases: In the first phase of the pilot, a producer (*i.e.* the fisher) who catches a tuna registers this via SMS. This creates the asset in the blockchain. The producers themselves are verified by "trusted local NGOs" [78]. These assets in the blockchain are then transferred to the supplier, allowing to link each tuna back to the fisher. The second phase of the pilot was concerned with how to integrate the technology into the process. As most tuna is processed, integration into existing enterprise resource planning (ERP) system is critical. In this phase, they ensured that raw material can be tracked even after being processed [78]. The final phase of the pilot focused on the consumers of the products, how the collected additional information can be made available to the consumers. They included NFC smart stickers with the products in their systems, both on products in stores, but also on menus in restaurants. These NFC tags can be scanned via smart-phone and all information available by Provenance is displayed.

The successful pilot if Provenance does not only show that blockchain is a suitable technology for tracking products, but that integration into existing systems and processes is an important aspect to consider.

Skuchain

Skuchain, a Mountain View, CA based organization, does not directly focus on preventing counterfeit, but is working on a solution for trade and supply chain finance. Instead of using intermediaries, Skuchain uses signals from the flow of goods to execute the flow of money [86]. They aim to reduce processing cost and increase transaction speed. They hold several patents in the area, including one for the "Cryptographic verification of provenance

in a supply chain" [83]. They are working with financial institutions to test the use of blockchain in trade finance in the cotton market [49].

Although Skuchain does not directly address the anti-counterfeit use case, their solution provides transparency and allows tracking. Thereby, even though their main goal is different, this benefits to reduce counterfeits.

Verisart

Verisart, Inc. is an organization based in Burbank, CA. They are focusing on art and collectibles and building an digital catalog [90]. Their goal is to have a digital history of physical works, enabling more efficient trading and removing the need to have intermediaries to ensure the authenticity of a product [13].

Verisart offers an iOS App and is free for artists and collectors. Certificates can be generated with two easy steps, but the process is not further described. At the time of writing, Verisart is not open for public, but invite only [99].

VeChain

VeChain is a project by BitSE, an Shangai based blockchain company. VeChain uses NFC chips, which each stores a private/public key pair, while the public key is also stored in the blockchain. Using the VeChain app, customers can validate the authenticity of a product. VeChain has partnered with Babyghost, a fashion label, to not only ensure the authenticity of their products, but also allowing the customers to see the story of a Babyghost fashion product [15].

2.3 Other Technology Based Anti-Counterfeit Solution

The previously discussed solutions are all blockchain based, but the targeted market varies between the solutions. Plenty of non blockchain-based anti-counterfeit solutions exist. Due to the context of this thesis, solutions in the pharmaceutical sector are introduced hereafter.

Sproxil

Sproxil is a private, for-profit organization based in Cambridge, MA. They offer several services in the context of anti-fraud, customer loyalty and track-and-trace context. For anti-counterfeit, they offer Sproxil Defender, a point-of-sale product verification product, which allows customers to verify the authenticity of a product. The process is rather

simple: The organization using Sproxil has a unique code, which is hidden behind a scratch label. The customers can use the code and then check if the product is authentic by SMS, using a mobile app, calling the Sproxil call center or using the web [88].

The National Agency for Food and Drug Administration and Control (NAFDAC) has introduced Sproxil in 2011 in Nigeria. The product is also in use in Kenya. In 2012, it was reported that more than one million products in Africa have been checked using the Sproxil service [2].

Sproxil uses IBM SmartCloud to offer its services [88]. Unlike the previous discussed blockchain based solutions, the data is therefore under full control of Sproxil.

mPedigree

mPedigree is a Ghana based organization, and according to its own words, the global leader in mobile and web technologies securing against counterfeiting [68]. The "Goldkeys" solution offered by mPedigree is very similar to Sproxils offering. Every product contains a hidden 12 digit key, which customers can then use to check the authenticity of the product via free text message. The system does not only benefit the customer, as the data gathered via authenticity check enables mPedigree to analyze and market intelligence to the product manufacturers.

mPedigree is active in Ghana, Kenya, Nigeria, Egypt and other countries [94]. Their Goldkeys product is not only used to secure pharmaceuticals, but also textiles, cosmetics and automobile spare parts [69].

In 2010, HP reported that they offer the infrastructure for the service [46]. This means, similar to Sproxil, that the infrastructure is under full control of private organizations.

2.4 Discussion Related Work

Many products which operate in the space of this thesis already exist, more than were expected in the beginning. The technologies and requirements of these different products vary greatly. Table 1 provides an overview of the technologies used, which products are supported and targeted, and the focus of the solutions.

Blockverify, Chronicled, VeChain, and Provenance all provide support for multiple products. While Provenance has a strong focus on transparency and story telling, the others have a stronger focus on anti-counterfeiting. Chronicled products enable companies to implement their own solutions while using their technology stack. Skuchain's focus lies on trade and automation, not directly on anti-counterfeiting. Verisart and Everledger are targeted at specific products, art and diamonds respectively. All these solutions use blockchain technology.

	Products	**Focus**	**Technology**
Blockverify	Luxury Items, Diamonds, Electronics, Pharmaceuticals	Counterfeit	Blockchain (Bitcoin and private), custom tags, mobile app
Chronicled	Initially: Sneakers Now: Everything	Counterfeit, Provenance, Supply chain	Blockchain (Ethereum, plans to support multiple). BLE and NFC tags and Inlays Mobile (Android- and iOS-) Apps, Web Dashboard
Everledger	Diamonds	Counterfeit	Blockchain (Bitcoin and private (Eris)), no tags required
Provenance	Consumer Goods (Food, Whine, Clothing, Accessories, etc.)	Trust, Traceability and Transparency of Products, Story of Product	Blockchain (Ethereum), custom tags
Skuchain	Cargo	Trade and supply-chain finance	Blockchain (unknown)
Verisart	Art	Digital catalog, more efficient trading, digital history, authentication	Blockchain (unknown) Mobile (iOS-)App
VeChain	Consumer Goods	Trust, Counterfeit, Story of Product, Transparency and Traceability	Blockchain (unknown), Mobile (Android-)App
Sproxil Defender	Pharmaceuticals	Counterfeit	Database Scratch Codes Mobile & Web App, SMS
mPedigree	Pharmaceuticals	Counterfeit	Database Hidden Code SMS

Table 1: Overview Related Work

The non-blockchain based solutions are mainly targeted for anti-counterfeiting in third world countries. They do, however, also offer other services, such as customer loyalty programs. Both, Sproxil and mPedigree, allow to access data using various technologies such as web and SMS and to check the authenticity of a product against their database.

Chapter 3

Blockchain Technologies

With the success of Bitcoin, the interest in blockchain, the technology behind Bitcoin, has risen. However, blockchain is not just the technology behind Bitcoin, but can be used for many other use cases. This chapter introduces blockchain, what it is and the different kinds of blockchains. Then, use cases behind crypto currencies are introduced and discussed, such as smart contracts. Finally, different blockchains are considered and discussed.

3.1 Blockchains

A blockchain is (typically) distributed ledger in which all transactions are stored. Considering the most well-known blockchain, the Bitcoin blockchain, this represents all executed transactions, which are stored in blocks [89]. All full nodes in the Bitcoin network, *i.e.* all nodes which also validate the transactions, have a complete history of all transactions and addresses from the original transaction of the blockchain (the genesis block) [89]. Since all data is stored from the beginning and available to everyone, it is easy to query previous transactions.

The technological revolution of blockchains is that it is "trustless". Unlike traditional systems, users do not need to trust central intermediary parties such as banks, but only the system [89]. The system ensures that there is no double spending. The algorithm enabling this trustless proof mechanism is based on a consensus mechanism. This mechanism decides how transaction are approved. One example for a consensus mechanism is the proof-of-work algorithm. This algorithm ensures that transactions which are written into blocks, cannot be changed afterwards. Nodes need to solve complex cryptographic problems to add a node to the chain, and are rewarded for that. The network prefers the most complex chain available. Since the problems are dependent on previous blocks, changing transactions would require nodes to recalculate many blocks. As the the network always prefers the longest chain, an attacking node would have to possess more than half of the computing power in the whole network. The more blocks are added, the less likely an attacking node is to succeed [82].

While the proof-of-work algorithms have been in use for a time, it does come with disadvantages. The complex calculations require lots of energy. "Miners", the nodes solving these algorithms, are typically compensated with an amount of the cryptocurrency for successfully calculating a the hash. Except for the energy consumption, this also requires a cryptocurrency usage of the blockchain technology, as this serves as incentive for the miner. As blockchain technology can also be interesting for other use cases, and non-public blockchain approaches exist, the question of efficiency arises. Other algorithms, such as proof-of-stake exist, but the largest public blockchains use proof-of-stake. Proof-of-stake does not depend on computational calculations, but transactions are approved by entities which have a stake in the network [4].

While the blockchain can be used for cryptocurrencies, the decentralized architecture allows for many other applications. As it is for an immutable, durable and reliable data structure, it can be used for all sorts of "recording, tracking, monitoring and transacting off all assets" [89]. Use cases do not only exist in the finance sector, but also for physical and intangible assets.

A blockchain can either be unpermissioned or permissioned. In an unpermissioned blockchain, all nodes have the same rights and the ledger is owned by everyone. This ensures that there is no censorship, as no entity has full control over the ledger. Unpermissioned ledgers can not be edited. While this is beneficial for many use cases (*e.g.* declaring a testament or assessing property ownership), it can also be problematic. As the blockchain is not editable, it is not possible to remove unwanted contents.

3.2 Blockchain Deployment Models

While a blockchain is typically a distributed ledger, other deployment models have emerged. Organizations see the advantages in the cryptographic storing of information, but still want to have control over who has access to the data. The three different blockchain deployment concepts are introduced hereafter.

Public Blockchains

A public blockchain is a blockchain open to everyone. Everyone can read and add transactions. Everyone can participate in the consensus process. It is unpermissioned, *i.e.* everyone has the same access rights. Centralized trust, like in a bank, is replaced by the consensus mechanism. A public blockchain is fully decentralized [14], everyone can download a full copy of it and there is no master which could be tampered with. The decision, which state is valid, is solely decided upon by the algorithms used.

Private Blockchains

A private blockchain is typically a blockchain where only one organization has write access. It is possible that read access is also limited to one organization, but read access can also

be public [14]. Typical use cases include database management and auditing in a single company [14].

Many of the general perceived advantages of blockchains are lost when they are deployed privately. Especially if there is no read and thereby auditability access from outside, the blockchain is under full control of a company. And as all nodes are under control of the organization, it is possible for an organization to change the history of transactions, as there are no competing nodes. Since one of the main benefits of blockchain technology, immutability, is lost, the true benefits of a private blockchain are questionable. Especially when using a technology based on proof-of-work, therefore requiring lots of energy.

Consortium Blockchains

A consortium based blockchain is a blockchain available to an industry, group of organizations or individuals. It is a shared ledger, but unlike a public blockchain, access can be limited to members of the consortium. It is possible that write access is limited, but all users are allowed to read. It is also possible to use "hybrid routes", so that some information is publicly available, while other is not [14]. Consortium blockchains are "partially decentralized" [14].

Consortium blockchains are especially interesting for a group of organizations, which do need to share information internally, but have no interest in sharing these with the outside world. An example could be a group of organizations which trade internally. A consortium based blockchain allows them to store transactions, and since the system is distributed, no single organization can alter the transaction history, thereby they do not require a trusted third party.

Discussion Deployment Models

	Access	**Key Characteristics**	**Typical Use Cases**
Public	Unrestricted	Immutable Distributed	Cryptocurrencies, general purpose
Consortium	Restricted to consortium members (read can be unrestricted)	(Immutable) (Distributed)	Consortium specific use cases, *e.g.* trade between consortium members
Private	Restricted to single entity (read can be unrestricted)	-	Internal auditing database management

Table 2: Overview Blockchain Models

Table 2 provides an overview of the three discussed blockchain deployment models, whom they are accessible to, their key characteristics and typical uses cases.

Consortium and private blockchains have several aspects which could be considered advantages compared to public blockchains [14]. The owner of the blockchain can undo transactions and change the rules of the network. It is clear who validates the transactions, unlike in public blockchains, where it requires a majority (and thereby includes a small risk of tampering). Privacy concerns are mitigated, as read access can be limited. Transactions are not only cheaper, as they do not have to be verified by as many nodes. Also, since the nodes are trusted, it is allowed for using consensus mechanisms which are faster and require less energy. Faults can be fixed more quickly, as the number of nodes running the software is limited and known.

However, these benefits also directly result in the loss of many benefits of blockchain technology. First of all, a permissioned layer does not have the quality of being trustless. There needs to be trust in the organization or consortium running the ledger, not just the technology. Public blockchains also "protect" the users from the developers of an application, as developers do not have the authority to do everything [14]. This can not only increase trust into the developer, but also makes applications censor resistance [14]. Public blockchains are also more likely to benefit from network effects. They are not only likely to be used by many entities, but can also deliver an integrated escrow service. [14] uses the example of a domain name escrow service. Traditional escrow services cost 3% to 6% of the transaction value. A public blockchain, which does not only have its own cryptocurrency but can also run a domain name system, allows for a fully automatic transaction. A smart contract (next section), which allows sending funds and automatically receiving the domain name, which cannot be altered by the entities involved. This can reduce transaction costs greatly.

3.3 Smart Contracts

Smart contracts are contracts in a computer language. Instead of defining the terms in a legal binding document, the terms are written as a computer executable program. Smart contracts can be deployed on a blockchain, ensuring that they cannot be altered. Smart contracts enable the of the blockchain to solve more complex problems than cryptocurrency transactions [89].

The benefits for using smart contracts and blockchain technology include low costs, such as enforcing, writing the contract and compliance [89]. The combination of smart contracts and cryptocurrencies allows for automation of money flows. One simple example might be the delivery of a product. Writing a smart contract which automatically transfers the funds upon delivery is possible. Using IoT and sensor technologies, it is even possible to build more logic into the smart contracts. For example, temperature sensitive products can be shipped with a temperature sensor, and only if the temperature range was always within the accepted range, the product is accepted and the money transferred.

While a legal contract might be legally binding, execution of the contract can still be problematic and costly. Due to these costs, transaction still require trust between the entities involved. The possibility to put the transaction details into code which is automatically executed removes this need. The contract is either executed or not (or partly, if so defined). Furthermore, smart contracts allow for faster execution, can remove the need for escrows and allow for automatic remittance [67]. This automation can be simple for some goods, *e.g.* digital goods, but physical products have somehow to be combined or mapped into digital world.

Mapping physical goods is, however, only one pending issue. Smart contract technology is still in its "infancy" [89]. Furthermore, the question if smart contracts can be legally binding arises [73]. Just because the term "smart contract" includes "contract", it does not make it automatically legally binding. While execution is automated, the question if these transactions could not be challenged via court remains to be seen [73].

Even though there are some technical and legal limitations, it is clear that smart contracts have the potential to have a great impact on the market. The precise impact is to be seen, but with technologies from today, simple processes can already be mapped and automated. Changing business units, organizations and processes within organization as well as developing more complex smart contracts, IoT devices supporting fully automated transactions will be a bigger challenge. However, with many startups and "sizeable" venture capital investments [67], growth in the area is inevitable.

3.4 Blockchain Technologies

Bitcoin was the first widely adopted and the most successful blockchain until today. However, many other blockchain based technologies have emerged and allow using blockchains for more purposes than cryptocurrencies transactions, *e.g* through the usage of smart contracts. In this section, several blockchain based technologies are introduced and the key differences discussed.

Bitcoin

Bitcoin is the first widely successful cryptocurrency. It is based on a paper published by "Satoshi Nakamoto" in 2008. "Satoshi Nakamoto" is a pseudonym, the true identity of the founder of Bitcoin is not known [18].

Bitcoin uses the blockchain as ledger to store all past transactions within the network. It uses proof-of-work as consensus mechanism. While the Bitcoin blockchain is less versatile than other blockchains discussed hereafter, it is very stable and the core protocol was never hacked.

Bitcoin is designed as electronic cash system [82]. However, since small amounts of data can be stored in the blockchain, it is possible to include small amounts of data in transactions [84]. Since the blockchain includes all past transactions, the information will remain

in the blockchain forever. The Bitcoin blockchain is public and the cryptocurrency is, like the technology, called Bitcoin (BTC).

Ethereum

Ethereum is a blockchain-based computing platform with smart contract support. It is developed by the Ethereum Foundation, a nonprofit Organization based in Zug, Switzerland [34].

The goal of Ethereum is to create "an alternative protocol for building decentralized applications", with an emphasis on security, development time and interactions between applications [98]. This is achieved by a Turing-complete programming language, which is built into the blockchain. To reach this goal, Ethereum uses a virtual state machine, the Ethereum Virtual Machine (EVM) [100].

Ethereum uses its own cryptocurrency, Ether (ETH). Since smart contracts can contain lots of logic, every transaction costs "gas". Gas is the anti-denial service model of Ethereum. Any computation on the Ethereum Blockchain costs gas. The more complex a transaction is, the more expensive it becomes. Generally, every computational step costs 1 gas, but depending on the complexity or data to be stored it can be more expensive [98].

After an attack in 2016, which exploited a weakness in a smart contract [29], the Ethereum blockchain was forked. This fork was controversially perceived, as it showed that even a blockchain is not immutable, even though a majority of the community must support it. This fork of the Ethereum blockchain lead to the arising of Ethereum Classic, a fork of Ethereum which continuous to operate on the pre-forked Ethereum blockchain [35].

Both Ethereum and Ethereum Classic use Solidity as smart contract language. Solidity is a contract-oriented, high level language which is similar to JavaScript, but statically typed. Using Solidity, it is simple to write Smart Contracts, for example for voting, crowdfunding, wallets and more, which are executed on the EVM [33].

While the Ethereum blockchain is public, the Ethereum technology can also be used for creating private and consortium blockchains. Microsoft's Azure offers a one-click solution to host a Ethereum-based consortia blockchain in its cloud services [16].

Factom

Factom launched as a Bitcoin extension which addressed three limitations of the Bitcoin blockchain: Speed, cost, and bloat [87].

- Speed:

  The Bitcoin blockchain requires 10 minutes to confirm a block. Users looking for greater security consider waiting for multiple subsequent blocks before accepting a transaction. This leads to waiting times up to over an hour.

- Cost:

  The default transaction cost on the Bitcoin blockchain is 0.01 mTBC [1]. This can become problematic, especially if using Bitcoin for applications which store many transactions.

- Bloat:

  The Bitcoin blockchain has a limit of 1MB per block and transaction throughput is limited to 7 transactions per second. For applications wanting to store more information in the blockchain this becomes problematic.

Factom overcomes these limitations by adding a Factom layer between applications and the Bitcoin blockchain, as shown in Figure 1.

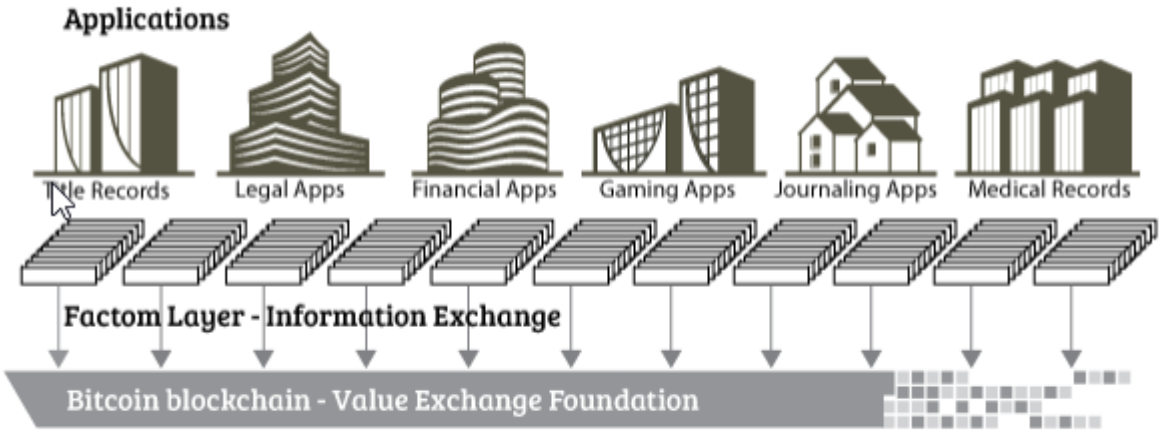

Figure 1: Factom Architecture [87]

The Factom layer is used to store data, and the hash of the information is then stored in the Bitcoin blockchain. This allows proof-of-existence (PoE) and auditability on the Bitcoin blockchain, without having to store all data in it.

As of 2016, Factom offers three different products [43]:

- Apollo:

  The focus on Apollo lies on reducing the risk of centralized databases and is targeted at bushinesses and governments. It ensures that data cannot be tampered with without the organization knowing it. Apollo audits different data sources and unifies this information in a chain of events, real-time. This single record ensures the integrity of the data, allowing for real-time verification that data was not backdated or altered [40].

[1] USD 0.08 at the time of writing

- Iris:

  Iris is Factom's digital identity product. With IoT devices storing more and more personal information, traditional approaches such as certificate authorities do not scale [42]. Iris provides approaches to "create security, based on identity, reputation, origin, and manufacturer" [42]. Unlike certificates, these can be updated with new information.

- Hera:

  Hera is a service by Factom to build private and permissioned blockchains. Factom argues, that this provides the "security and immutability of a blockchain with privacy of permissioned database" [41].

  The Factom whitepaper ([87]) does not provide any further information on Hera, it is thereby not clear if it is based on the same technology as their public offerings.

The public offering of Factom use "Factoids" as currency to add entries into the Factom blockchain [44]. Unlike Bitcoin, Factoids are to be issued at a fixed rate. As the protocol is yet to be fully deployed, now new Factoids are issued, but an initial supply was generated by a software token sale [44].

Chain

Chain Core is a "enterprise-grade blockchain" infrastructure offered by Chain Inc. [20]. The focus of chain lies on financial institutions, and the focus of their blockchain therefore lies on the issuing and transferring of financial assets. Together with Visa Inc., Chain Inc. they have introduced an international B2B payment solution [97]. Their blockchain is permissioned and focuses on high confidentiality of transaction data.

Chain Core is offered as a free, open source developer edition. It is also offered as an Enterprise Edition, including support and partnerships [23]. Chain is deployed at customers' locations and does not, except for a testnet, have any public blockchain.

Chain uses its own virtual machine, called Chain Virtual Machine (CVM). As the focus of the Chain blockchain is assets, the code that can be executed on CVM is more limited than EVM. Assets can be issued and transferred. All these transactions are then stored within the blockchain. While Chain protocol is agnostic to the consensus program used [22], the first version of the protocol defines a protocol using a block generator and multiple block signers [21], as shown in Figure 2.

The block generator is the only entity which creates blocks. It collects all transactions, combines them into blocks, and then sends them to the block signers. The default consensus protocol is specified such that N public keys are in the network, and for each block to be valid, M block signers must sign it to become valid. As long as no more than $2M - N - 1$ block signers violate this rule, the chain cannot be forked. However, since there is only one block generator in the network, there is a single point of failure. The block generator cannot fork the blockchain by itself, but it has control over the network aliveness. If it stops, no new blocks will be added. Chain argues, that for a permissioned

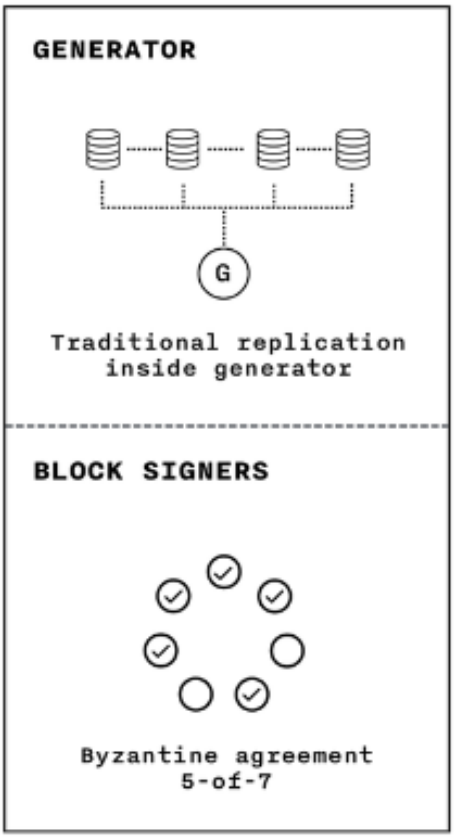

Figure 2: Chain Block Generator and Signers [21]

blockchain, it makes sense to have a single company responsible for creating blocks, and that if the block generator behaves maliciously or is shut down, it is "probably better (in these use cases) for the network to stop" [21].

eris by Monax.io

Monax.io (formerly eris industries) offers services in the blockchain sector. They sell "legally compliant smart contract-based SDKs", increasing time to market with "sophisticated ecosystem applaictions" [63]. Monax argues, that using distributed technologies, including blockchains and smart contacts, allows organizations to eliminate redundancies and increase communication efficiency within their business ecosystem.

Target use cases include banking, insurance, supply chain, shipping, transportation and many more.

From a technological perspective, Monax offers two services. First, they have developed the eris stack, an open blockchain platform. Figure 3 shows how this stack is made up. All elements in the green boxes are developed by Monax, while the purple are external, but managed by Monax. The other components are to be developed by the organization using the stack. Unlike Ethereum and Bitcoin, eris is targeted to be deployed in different

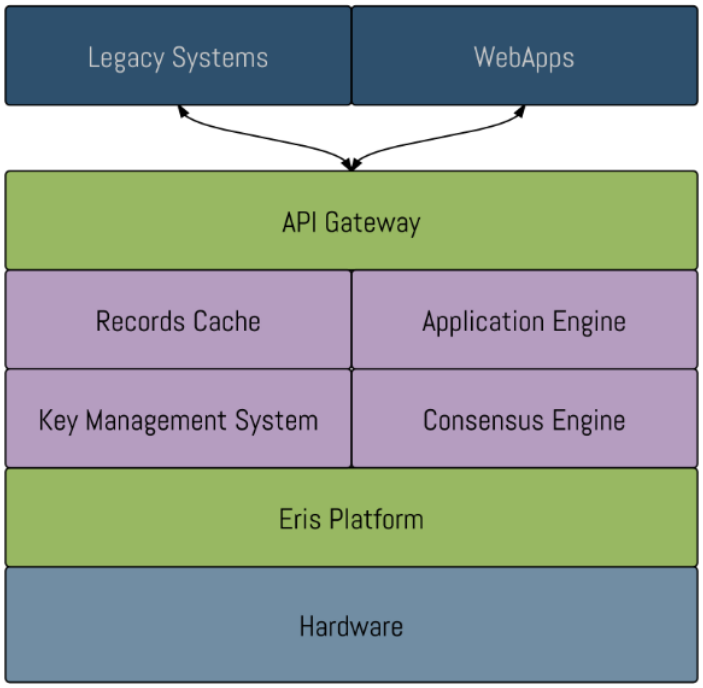

Figure 3: Eris Ecosystem Application Overview [65]

contexts, including private and consortium blockchains. eris uses a proof-of-stake algorithms and is thereby more energy efficient than Ethereum and Bitcoin. eris also includes a permission layer. eris is however built according to the EVM specifications [66], which enables portability between the two platforms.

The other technical service Monax offers are Software Development Kits (SDKs). These SDKs are accessible in a monthly developer license subscription and come in different tiers. Benefits of these SDKs include faster time-to-market, constant updates, high quality and compliance [64].

BlockApps STRATO

BlockApps STRATO is another blockchain which is compatible with Ethereum, but focused on enterprises. Scalability allows to develop early Proof-of-Concepts (PoCs) up to production systems [8].

The modular architecture of BlockApps STRATO allows the construction of hybrid private, consortium and public blockchains [8]. For consensus algorithms, proof-of-work and proof-of-stake are supported, as are instant consensus and signature pools. STRATO consists of three interconnected modules, the STRATO blockchain, the STRATO smart contract interface (RESTful API), and the STRATO network, which enables to connect to other STRATO nodes or public Ethereum nodes [9]. It also includes a "blockchain explorer page", which provides statistics about the history of the blockchain [62].

Ioata

Due to the growing file size, computational power required, and minimal transaction fees, blockchains are not well suited for IoT devices. Ioata tries to overcome these issues by using a Directed Acyclic Graph (DAG), called "tangle", instead of a blockchain. Using a DAG, Iota is targeted as "the backbone of IoT", allowing real time micro-transactions – real time micro-transaction without fees [55].

The tangle is based on the idea that each new transaction must approve two previous transactions. Nodes have the incentive to only approve valid transactions, as it is otherwise unlikely that their own transactions will be approved. Ioata does not specify how to decide which transactions to approve,but argues that all nodes should follow a "reference" rule. To issue a transaction, a node execute three steps: 1) Choose two transactions to approve, based on an algorithm. 2) Check that these transactions are not conflicting. 3) Solve a cryptographic puzzle to ensure authenticity of the transaction. As the tangle is considered to be an asynchronous network, it is possible that there are conflicting transactions. If there are multiple transactions, the network calculates the probability that a transaction is confirmed by a current tip (*i.e.* the newest transaction in the graph) and chooses the one with the higher priority. The more approvals a transaction has, the less likely the system is to accept a double-spending transaction [76].

Figure 4 shows how the DAG is setup. The shaded boxes represent tips of the network. The upper graph shows the network in a lower load scenario, where there is only one tip, as there are not as many new transactions to approve. The lower graph shows a high load regime. Since there are many new transactions, many tips exist, and it can take a while until a tip is approved by new transactions [76].

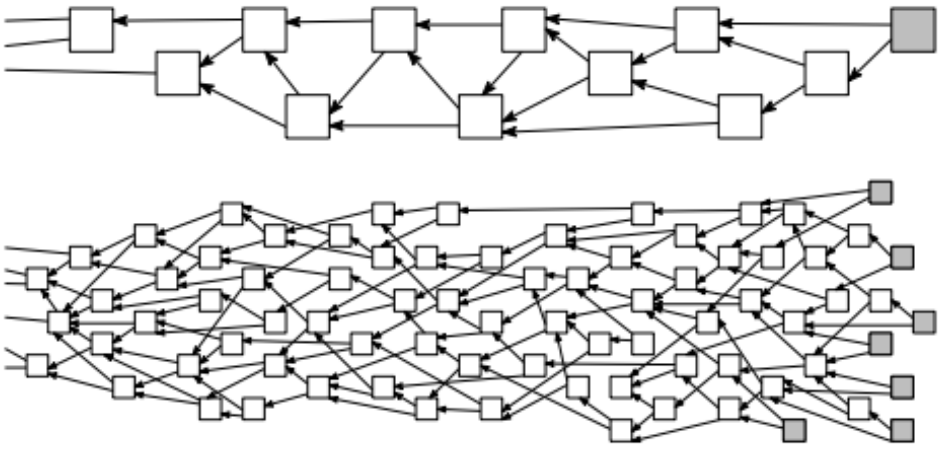

Figure 4: The Tangle in a Low Load (top) and High Load (bottom) Regime [76]

Unlike Bitcoin, all tokens will be created by the in the genesis, *i.e.* in the finder block. There is no mining in Ioata [76]. Ioata is currently in Beta, available as Java client.

Hyperledger

Hyperledger is a global open source project to advance "cross-industry blockchain technologies" [51]. The project was started in 2015 by the Linux foundation and members include organizations from finance, banking, IoT, supply chain, manufacturing and technology, including accenture, Intel, IBM and many more.

Hyperledger does not provide a single blockchain technology, but currently has four projects which are incubated. These projects include a Blockchain explorer, Hyperledger Fabric, Hyperledger Iroha, and Sawtooth Lake [52].

Hyperledger Fabric

Hyperledger Fabric was proposed at first at a hackathon. It is based on a modular architecture allowing components to be plug and play, *e.g.* the consensus mechanism and the membership service. Using container technologies, it allows to host logic in smart contracts using the chaincode [52].

Hyperledger Iroha

Hyperledger's Iroha project is focused on easy incorporate into infrastructural projects. It features a simple construction, is implemented in a domain-driven C++ design, has an emphasis on mobile application development and uses its own consensus algorithm, Sumeragi [52].

Sumeragi is visualized in Figure 5. It uses the concept of a global order of validating peers, which is based on a server reputation system. The reputation system takes the reliability of the servers into account, based on the time registered with the membership service and the number of successful transactions. The nodes are split into two sets, A and B. Set A consists of 2f+1 members. Sumeragi requires 2f+1 members to verify and sign a transaction, therefore the nodes in set B are typically not involved in signing a transaction. If a client sends a transaction, it is sent to the leader node (based on reputation), which then broadcasts it to the 2f+1 validating peers. If all nodes verify and sign the transaction, it is then committed. If there is an error or timeout in the verification process, the transactions are also broadcasted to additional (set B) nodes [102].

Hyperledger Sawtooth Lake

The final project incubated by Hyperledger. It is Intel's modular blockchain suite, which aims to support many uses cases from IoT to financials. It supports both permissioned and permissionless deployments and uses a novel consensus algorithm, called Proof-of-Elapsed-Time (PoET). PoET is aimed to deploy a consensus layer into "transaction families", which can be defined by the users themselves. PoET requires a trusted execution environment (TEE), which allows safety and randomness, without the disadvantages associated with other proof algorithms [54].

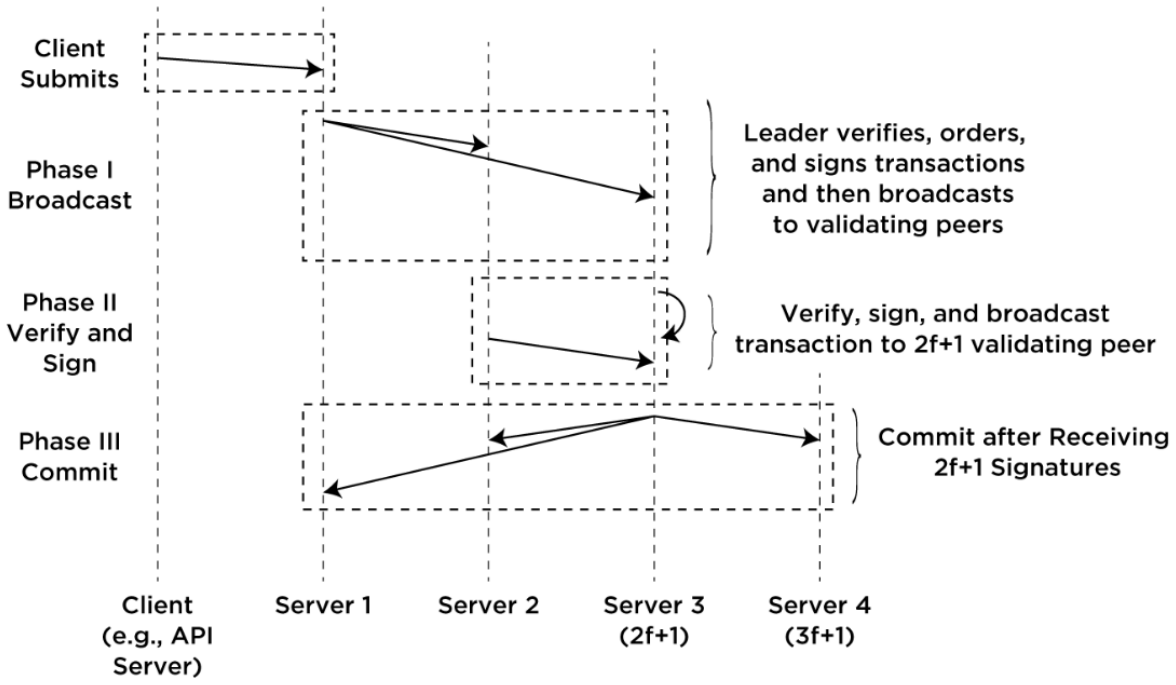

Figure 5: Iroha Consensus Mechanism: Sumeragi [102]

Nxt

Nxt is another blockchain platform, which includes its own cryptocurrency (NXT) and allows for decentralized systems. It supports an asset exchange, developing an own monetary systems, a data cloud, voting system and multi-signature access control [70]. For consensus, it uses a proof-of-stake algorithm [71].

Compared to Ethereum and other technologies, Nxt does not support arbitrary logic, but users are limited to what is offered by Nxt. Smart contracts are not supported.

3.5 Evaluation

The introduced blockchain-based technologies only covers a subset of all blockchain technologies available. CoinmarketCap, a website focusing on cryptocurrencies and their values, lists over 700 cryptocurrencies [28], of which most will use their own blockchain or distributed ledger. However, considering the complete market capitalizations of all these cryptocurrencies, Bitcoin makes up for over 80% of the total volume, with Ethereum being a distant second. Also, many cryptocurrencies do not offer additional features, such as smart contracts. There are also other blockchain based technologies, which do not include a public cryptocurrency or are targeted at specific use cases. Examples include BigChainDB, a distributed database with blockchain characteristics [61] and R3 Corda, a distributed ledger for financial services [11].

The technologies chosen are either leading (*e.g.* Bitcoin as largest cryptocurrency), introduced major new features (*e.g.* Ethereum and its Turing-complete virtual machine) or have created lots of traction (*e.g.* Hyperledger project with many industry leading organizations on board).

Table 3 and 4 provide an overview over the different blockchains discussed in this chapter, including their focus, support of smart contracts, deployment options, if it includes a permission layer, and the consensus algorithm used.

The important characteristics of a blockchain depends on the use case targeted by it. One important factor to consider is the deployment model. While public blockchains allow all users to look up the complete history, they might increase trust into the system. They are also not dependent on a single or multiple organizations to keep them alive. However, to ensure the integrity of a public blockchain, it must have enough members. A public blockchain which cannot attract and keep a critical user base, might have issues ensuring the authenticity of transactions. The consensus algorithm also has consequences, especially in public blockchains. The Bitcoin network, being around for a long time and providing great financial incentives, is yet to be hacked. The proof-of-work algorithm does hold up against any attacks. However, it also leads to great increase in energy consumption.

Consortium and private blockchains have the advantage, that the risk of using other consensus mechanisms are smaller. Since the access to the network is limited, not everyone can add transactions. Some blockchain-technologies even include central entities (such as the block generator in chain). This might allow the network to be more efficient, but also introduces single point of failures and opens potential attack vectors. The question if to use a private, consortium or public blockchain should be based on the application in mind. Using a public blockchain might increase trust from the public, but there should be no need for that if the blockchain should only be used as a ledger for a group of organizations. A consortium based blockchain can then still provide many benefits, without organizations worrying about data leaks and increased energy consumption.

There is also the question, if a blockchain should be built for a specific use case. Bitcoin, Chain, Ioata all have specific use cases. Nxt and Factom support more than one use case, but still have a fairly limited set of functionalities. The other technologies allow for more broad use cases, Ethereum, BlockApps Strato and eris being Turing-complete (all built to be compliant with EVM). While this allows plenty different use case being built upon a blockchain, it also makes the system more complex and likely more prone to error (*e.g.* Ethereum DAO hack).

Another aspect to consider is the maturity of the technologies. During the duration of writing this thesis, the technologies have changed significantly. As with all new technologies, many new implementations are likely to appear in the next months and years. Others will disappear. Bitcoin is the only technology which was around for multiple years and is

	Focus	Deployment Model	Supports Smart Contracts	Permission Layer	Consensus Algorithm
Bitcoin	Cryptocurrency	Public	No	No	Proof-of-Work
Ethereum	Decentralized Applications	Public[a]	Yes	No	Proof-of-Work
Factom	Audit and digital identities	Public and Private	No[b]	Yes (Hera)	proprietary (federated)
Chain	Financial Transactions	Private and Consortium	No	Yes	proprietary (federated)
eris by Monax.io	Decentralized Applications	Public, Private and Consortium	Yes	Yes	Proof-of-Stake
BlockApps Strato	Decentralized Applications	Public, Private and Consortium	Yes	Yes	Multiple Supported

Table 3: Overview Blockchains 1/2

[a]Can be used to setup private network or local cluster [57]
[b]Factom can be used as data source [72]

	Focus	**Deployment Model**	**Supports Smart Contracts**	**Permission Layer**	**Consensus Algorithm**
IOATA	Backbone of IoT	Public	No	No	DAG
Hyperledger Fabric	Decentralized Applications	Private and Consortium	Yes	Yes	Multiple Supported
Hyperledger Iroha	Decentralized Applications	Private and Consortium	Yes	Yes	Sumeragi
Hyperledger Sawtooth Lake	Mobile Applications	Private and Consortium	Yes	Yes	Proof-of-Elapsed-Time
Nxt	Cryptocurrency and Decentralized Systems	Public	No	No	Proof-of-Stake

Table 4: Overview Blockchains 2/2

therefore likely to stay. It is being used by many users, while many other technologies are still in beta (*e.g.* IOTA) or not widely adopted. Working with the different technologies also differs quite drastically. For example, eris was available and was well documented in Summer 2016. Other systems were available, but failed to start following the official tutorials. Many products were drastically improved and refined within the last few months, and it is likely that the landscape looks completely different in a few months.

The question which blockchain technology to use is therefore not only dependent on the use case of the application, but also the maturity of a system and how much trust organizations have into the future of a technology. Bitcoin, as the oldest blockchain, has yet to experience hack or other disruptive events, whereas Ethereum was already forked into two different chains. As of time of writing, using Bitcoin for ensuring integrity and longevity of data seems reasonable. However, if the blockchain should not only be used for proof-of-existence, but more complexity is required, Ethereum is the most advanced blockchain ready to use. As for private and consortium blockchains, both eris and BlockApps Strato have full EVM support, are easy to use and deploy. The Hyperledger project is widely supported by industry leading organizations. Hyperledgers technology is currently being used for multiple PoCs, for example in cotton trading [1] and cross boarders payments [17]. It is likely, that these three technologies (Bitcoin, Ethereum, Hyperledger) will stay in the market for a longer period of time.

Chapter 4

Legal Opportunities

The negative consequences of counterfeited pharmaceuticals can have, as discussed in Chapter 1, a severe impact on the health of consumers. Regulators are also aware of this and legislation changes in the European Union (EU) and the United States (US) are ongoing. These legislation changes open potential business perspectives for organizations, such as Modum.io. In this section, the legislation changes in the EU, which also affect Switzerland [92] and the US, are introduced and compared.

4.1 EU Falsified Medicines Directive

The Falsified Medicine Directive (FMD) [36] introduces a new legislation which is applicable for all EU member states. The goal of the new regulation is not only to reduce counterfeits entering the market, but also having an efficient system to recall products. Affected are all prescription drugs, which will need to comply with the new system. The legislation will apply for all EU members on February 9^{th}, 2019. Belgium, Greece and Italy have the option to defer the legislation for 6 years [37], as they already have verification systems in place [36].

The EU legislation includes two aspects, the physical individual packs of a product and data repositories to store relevant information. The system should provide end-to-end verification, but is not a full track & trace system [91].

The physical individual packs of medicines need to include two safety features [36]. First, it needs some sort of anti-tampering device. This allows customers and sellers to identify individual packs which were already opened and might have been replaced with counterfeits. Second, every package needs a two dimensional barcode, carrying a unique identifier. This identifier needs to be unique for each package, it is not enough to have a different identifier on every batch. The two dimensional barcode must not only be able to uniquely identify one specific package, but also includes information such as the product code, serial number sequence, batch number and the expiry date of the product. A national reimbursement or identification number can be included, but is optional. The data must

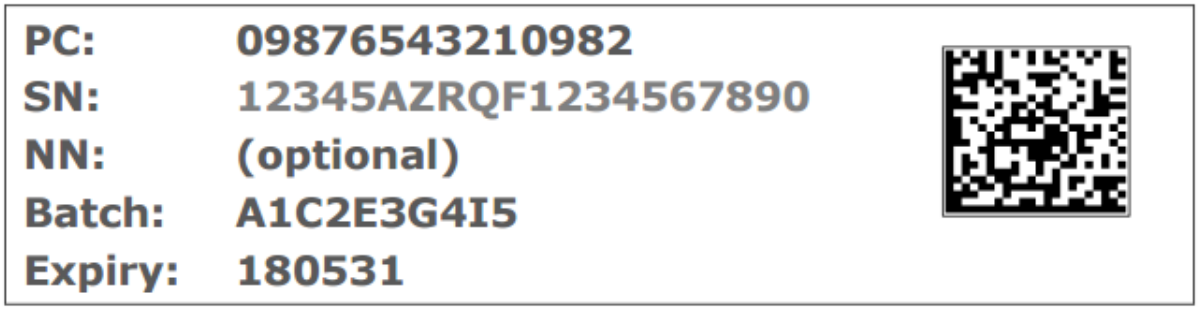

Figure 6: EUFMD Required Information on Medical Products [91]

also be on the individual packs in human readable form. Figure 6 shows an example of the information that needs to be on the individual packs.

To ensure that counterfeiters cannot guess the unique key, it should be randomized [36]. While every individual pack must have a unique identifier, it is allowed to have aggregated codes for aggregated packages containing individual packs. This ensures that not all individual packages have to be scanned, if multiple individual packs are decommissioned at once [37].

The second part of the system is the electronic data repository. The legislation has clear requirements what is supposed to be stored in the system and defines some non-functional requirements. Every product must be registered in the data repository when the product is produced. The same information as on the two dimensional barcode must be stored in the data repository. It must be decommissioned when the product is sold at a point of sale to a customer or given to a patient [36].

These two points, production and point of sale, are the only places most products must be scanned at, and the data repository updated. However, products which are at a higher risk of falsification need to be traceable throughout the supply chain and verified by wholesalers [36]. However, no clear definition of "higher risk of falsification" is to be found and it is not clear, if it is up to the producers or the legislation to define which products are included. The data repository also needs to provide functionalities to mark products as recalled, withdrawn or indicated as stolen. When a product is sold a at place of sale, a warning must pop-up and the product kept, not handed out to the customer or patient. Points of sale include pharmaceuticals, hospitals and other health facilities. The process is visualized in Figure 7.

The legislation has clear technical requirements, but the cost and organization of setting up the repositories is up to the marketing holders and manufacturers of medical products [36]. Implementation is up to EU member states, but the different data hubs must be able to communicate via central EU hub, which serves as exchange. Except for this communication between the data hubs, the legislation also clearly states that the system response time must be within 300ms for 95% of all transactions. Information must be available in the data hub for a minimum of five years or until the expiry date plus one and one-half years, whichever is later. Reverting a decommissioning of a product must also be supported, but only by the entity which decommissioned the product in the first

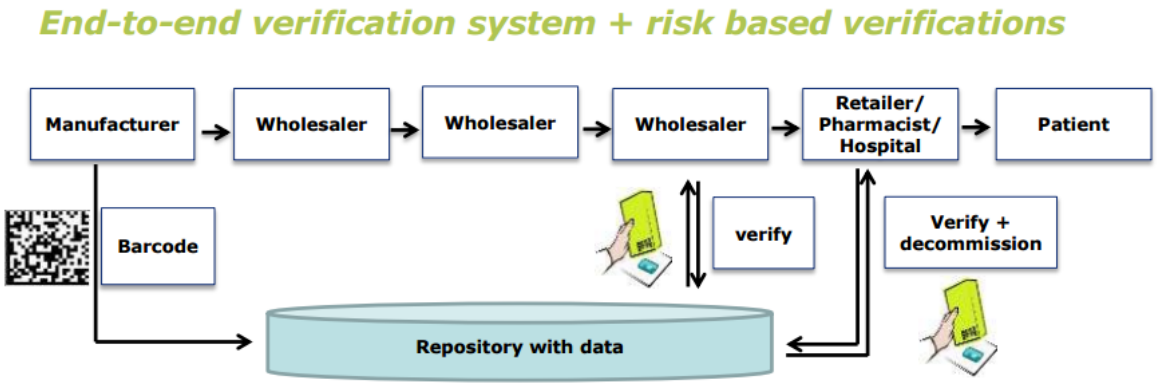

Figure 7: EUFMD End-to-End Verification System [91]

place and only if the decommissioning was not longer than 10 days ago, if the product was not recalled or marked as stolen. The reverting must be logged in the system.

One interesting aspect of the legislation includes the permission to access the system. The system should only be accessible by "authorized" entities [36], *i.e.* not by the public. An end-consumer of medicine is therefore not able to check whether the product bought is legitimate using the EU foreseen system, but must trust the point of sale.

4.2 US Drug Supply Chain Security Act

Similar to the EU regulation, there is also a new US legislation regarding pharmaceuticals. The US Drug Supply Chain Security Act (DSCSA), by the Food and Drug Administration (FDA), has the goal to build an electronic, interoperable system to identify and trace prescription drugs [96]. Similar to the EUFMD, the goal is to enhance detection of illegitimate products and enable faster notification upon finding counterfeits. It should also support efficient recalls of drug products [6].

The requirement are also similar o the EUFMD. Each product needs an identifier down to the package level and include product verification which is based on an identifier. This identifier must include a national drug code, the serial number, lot number and expiration date.

The electronic system must enable tracing, verification, detection and response in case of counterfeited products, and receiving notifications. The system, however differs from the EUFMD, as the goal is to have a complete transaction information, history, and statement of every product [6]. It is therefore not enough to have the information updated in the manufacturing process and then again when the product is being decommissioned, but every step in between must be recorded as well [6]. The US DSCSA also requires a notification system. Manufacturers and wholesalers must inform the FDA within 24 hours if they suspect to have an counterfeited product.

The EU legislation is expected to impact multiple stakeholders, including dispensers, manufacturers, repackagers and wholesale distributors [95]. The implementation of the new system is planned over a period of 10 years. This started in 2014 with the publishing of a guidance book and should be fully implemented in 2024. Important milestones include pilot projects in 2015, and the development regulations allow the electronic tracing of a product in an individual pack in 2017.

4.3 Comparison of EUFMD and DSCSA

Both the EUFMD and DSCSA aim to reduce counterfeits in the pharmaceuticals and have a strong focus on serialization of data [56]. However, there are also some key differences between the two approaches. Table 5 provides an overview of the similarities and differences.

	EUFMD	**US DSCSA**
Goal	Verification of product on individual pack level, enhance detection of illegitimate products, effective recall system	Verification of product on individual pack level, enhance detection of illegitimate products, effective recall system
Approach	Physical tampering proofness, serialization and verification at key checkpoints	Traceability at every step in supply chain
Data Hub Implementation	Legislation defines requirements, implementation up to member states	Implementation as co-effort, including secretary, federal officials and others to establish standards for interoperability
Rollout	New Legislation applies February 9^{th}, 2019	Phased roll-out over 10 years (2014-2024)

Table 5: Characteristics EUFMD and US DSCSA

The goals of both approaches are equal. They aim to reduce counterfeits, enable a system to act upon illegitimate product recognition and have an efficient system to recall products. However, the approach differs. While the US DSCSA requires traceability of a product at every step in the supply chain, the EUFMD focuses on key touch-points. Explicitly, the products must be registered during the manufacturing process, and then verified and decommissioned at the point of sale.

While both system require a data hub, the responsibilities are different in the two approaches. The EUFMD only states the requirements for the hub, but leaves the imple-

mentation up to its member states. In the US DSCSA, the role of the government is more central, and implementation is considered a co-effort.

Roll-out of the two systems also differ. The EUFMD applies to all member states in 2019. There is no in-between steps planned, it is up to the member states ensuring that this date is complied with. For the US DSCSA, roll-out is planned over 10 years, with multiple milestones in-between.

Chapter 5

Considered Approaches to Reduce Counterfeits Using Blockchain Technologies

Reducing counterfeit products is a very broad domain. Several key questions arise, like who the intended user-base of the system is, which data should be available to whom and when and how to record the data. Some characteristics of a blockchain based anti-counterfeit solution are the same as for all solutions, while others depend on the specific targeted use case. Due to the context of this master thesis and the collaboration with modum.io, it was clear that the focus lies on medical products. However, there are multiple options which can be proceeded in this field. Several approaches were developed in the space of pharmaceutical products. In this chapter the generic requirements for an anti-counterfeit system are introduced, and then three approaches are presented, discussed and evaluated. For all of these concepts, the role of blockchain-technology, which advantages it brings to the use case and which deployment models would be appropriate are discussed.

5.1 General Considerations

While the different concepts lead to different requirements for the system, a common set of information is required for all use cases. The previous discussed legislation changes and related work provide a good starting point for this.

Anti-Tampering Packaging:
An electronic system cannot ensure the authenticity of a product itself. Especially if the product itself is difficult or impossible to mark, the packaging must include anti-tampering mechanisms, so that it is visible if the content was replaced. Overt technologies include all packaging technologies which are visible in the product itself. This includes holograms, color shifting inks, security threads, water marks etc. The advantage of overt technologies is that they can be checked by the end-consumer.

Customer Awareness:
Having physical anti-tampering and an electronic system which allows to recognize potential counterfeits does not help, if there is no interest recognizing counterfeits by end-users or if the end-users are not aware how to check the authenticity of a product. To reduce counterfeits, it is therefore important to educate people about the consequences of counterfeits and make sure that they are aware of the mechanisms how to check for counterfeits.

Registration at Point of Manufacturing:
When using an electronic system, the product data should be inserted into the system by the original manufacturer. To ensure that the product can be verified, each product requires an unique identification of some sort. If a product requires multiple steps of production, it should be possible to track it back to the origin.

While the three points above do not ensure reduction in counterfeiting, they are prerequisite for all potential anti-counterfeit solutions. It shows, that for physical products an electronic register system in itself is not sufficient, but can only act complementary to other preventive measures. This is also true for the three developed concepts, which are introduced in the next Sections.

5.2 EUFMD Compliant System

The first considered approach was to create a system which is compliant with the new EU regulation discussed in Chapter 4. Using a blockchains does not affect the physical tampering mechanisms, but it can be used as data repository instead of a traditional database.

An initial set of requirements for the data hub system can be extracted from the legislation, such as:

- The system must be accessible by authorized entities, including wholesalers, persons authorized or entitled to supply pharmaceuticals
- Access to the system should be limited to these authorized entities
- It therefore must be possible to register and login
- Manufacturers must be able to store relevant data in the data hub, including:
  - Data elements of the unique identifier
  - The coding scheme of the product
  - Name and common name of the medical product
  - The member state or member states of its intended market
  - Name and address of manufacturer placing safety features
  - Name and address of the marketing authorization holder

  - A list of wholesalers who are designated to store and distribute the products

- Reversing the decommissioning of a unique identifier should be possible, if and only if:
  - The reversing is executed by the same entity as the product was decommissioned by
  - Reverting status was no longer than 10 days ago
  - The medical product did not expire
  - The medical product was neither marked as stolen, recalled, withdrawn or intended for destruction
- The system must keep track of a complete audit track for each product
- The system must be physically located in the Union
- Wholesalers must be able to update the location of a product
- It must be fully interoperable with the other data hubs

This list can be extended greatly by considering the whole legislation. However, there is no logic which cannot be built into a smart contract and a Turing-complete blockchain. The only aspect which might be problematic is the interoperability with other data hubs in the Union. Instead of only using a blockchain, it can be considered to use a blockchain to ensure the complete audit track of all transactions, but still keep a copy of the other data on a traditional database.

The requirement that the system can only be accessed by authorized entities reduces the options for which blockchains to use. The requirement that it must be physically in the Union also prevents the usage of a public blockchain, as copies of the data would be outside the Union. Due to multiple stakeholders, this approach would be ideal for a consortium based blockchain. It could be considered, that different member states each run one node in the consortium based blockchain.

The advantage of using blockchain technology is that many requirements are already built-in. Due to the immutability of a blockchain, changing data afterwards is not possible, and there is always a complete audit-trail available, since all transactions are stored.

5.3 Vaccines - Humanitarian Supply Chain

The second concept was developed at THE Port 2016[1], a humanitarian hackathon from CERN in Geneva, as part of the Pier71 team[2]. The challenge was to build an open system to reduce pharmaceutical counterfeits in developing countries.

[1] http://theport.ch/

[2] http://theport.ch/home/the-port-2016/#team-pier71

Instead of focusing on medicines, the idea focuses on vaccines for developing countries. This mainly due to the fact, that discussions with supply chain experts showed that there is a great reluctance of many organizations having their products traceable in open systems. According to discussions, this reluctance is mainly because the fear that an open system would allow competitors to explore the distribution channels. This results in a situation, where the system either has to be closed and has to include permission layers, similar to the EUFMD case, which was in contrast to the idea to build an open system. In the humanitarian supply chain of vaccines, these concerns do not exist.

Currently, distributors of vaccines do not know what happens with their vaccines when they enter the country of destination. This lack of information leads to a lack of decision data, which is intensified by the fact that there are no integrated system in many developing countries. It is often not known where how much vaccines are, and it is not possible to track them back to the origin. This does not only bring the risk of counterfeits being introduced, but also to waste and inefficient stock management. The trust in medical products and the government is weakened.

To overcome this, the ChainSafe[3] concept was developed. The target of ChainSafe is to provide an open and integrated platform for monitoring.

The process is in many regards similar to the EUFMD case. Vaccines manufacturers tag the vaccine vial with either a signed QR code or a NFC tag. Information about the product, such as producer, origin of the product and date of expiry is transmitted to a public repository, the blockchain and is also included in the NFC or QR code.

At every step of the vaccine, the QR code should be scanned. This does not only allow to update the public repository and blockchain, but also enables stock management, as all the relevant information about the product can automatically be pulled from the public repository.

At the point of usage of a vaccine, the product is to be scanned and decommissioned. If any unusual activity occurred with the product or it was marked as decommissioned before, a warning to the user is shown.

Finally, end users should also have the possibility to scan the products. This allows users to not only verify where the product was produced, expiry date and other information about the product, to track the path of the vaccine, but also to ensure that the product was decommissioned at the place where they have received it.

Except for the direct advantages mentioned above, this open approach would especially open up information of vaccines in developing countries. While it is not realistic to assume that every single transaction will be scanned and transferred to the open repository, even partial information is helpful. With enough information in the system, irregularities can be identified and acted upon. The more data in the system, the better analysis is possible and the more likely it is to not only reduce counterfeits but also inefficiencies within the supply chain.

[3] `https://chainsafetyinvestigators.files.wordpress.com/2016/09/chainsafe-concept-note-oct-20161.pdf`

The system would therefore not only benefit patients retrieving vaccines, but also warehouse managers, governance and international organizations, as they can all profit from the data available in the system. Patients can check the authenticity of the product, warehouse managers can automate part of their routine, governances and international organizations have data to support decisions, such as where bottlenecks are likely.

Blockchains provides severe advantages for such a system. First of all, trust into local authorities and governments might not be the highest in developing countries. Using a blockchain can reduce these concerns, as no entity can tamper with the data once it is in the blockchain. To fully benefit from the advantages of the blockchain technology, a public blockchain or a consortium based blockchain should be used. If a consortium blockchain is considered, it should be maintained by organizations in which people trust, for example a consortium based of multiple NGOs. As in the EUFMD approach, an additional database is beneficial for direct analysis of the data, while the immutability of the blockchain ensures that the data was not tampered with.

5.4 Extending the modum.io Solution

The final idea is to extend modum.io's current system. modum.io focuses on measuring temperatures of pharmaceuticals, as required by the legislation. it combines IoT and blockchain technology to do this, but does not include support for registering multiple steps in the process. The question arises, how and if the current system can be extended to also be used in other use cases, such as reducing counterfeits.

This approach has the benefit, that the system already exists and already uses blockchain technologies. It might also open opportunities for new markets.

5.5 Other Ideas

Except for the three previously discussed concepts, several other ideas were considered. Most obviously, the idea of a general anti-counterfeit system came to mind. The previously discussed key characteristics can be applied to a variety of anti-counterfeit solutions.

However, there is already strong competition in the field, as introduced in Chapter 2. Chronicled, Provenance and Blockverify offer solutions, which all tackle the anti-counterfeit use case directly. Some organizations bring added values, such as Provenance with a strong focus on the story behind the product. It was therefore decided not to pursue the work on a general system, as this would not bring any additional value, neither from a market nor research perspective.

5.6 Evaluation of Approaches

The three considered approaches all have their advantages and disadvantages. The EUFMD enables to derive clear set of requirements and a particular system to be built. The humanitarian vaccine supply chain is likely to have the greatest impact. It also allows for a system which is open to everyone, and offers great usage of blockchain benefits. Exploring the option of expanding modum.io approach has the benefit that key stakeholders are available and an existing infrastructure can be used.

During the course of the Kickstart Accelerator modum.io participated in, the possibility to talk to key stakeholders regarding the implementation of a EUFMD compliant system in Switzerland arose. These discussions clearly showed that it will not be possible to develop a system which could be considered in an evaluation process. It was also brought to attention that a more detailed technical specification exists, but is not available to the public. So therefore, while the approach discussed above shows that it is possible, this idea was not further pursued.

The approach using blockchain technologies to fight counterfeits in developing countries was started. Since it does not only include the team from the hackathon, but also gained traction from other parties. It was therefore decided to not pursue this idea within the context of this thesis. This due to the fact, that with a multitude of people, it was not possible to define a clear time-line for the project.

To evaluate if a blockchain based system can be used to reduce counterfeits, it was therefore decided to explore what changes would be necessary to modum.io's current system and how these changes could reduce counterfeits. The system and proposed changes are introduced in the next chapter.

Chapter 6

Expanding the modum.io System to Reduce Counterfeits

Since neither pursuing the EUFMD approach nor the vaccine case proofed to be reasonable, the question on how the existing modum.io application can be extended arises. The modum.io system is built on the use case of temperature tracking. In this chapter, the current architecture of modum.io is introduced, required changes to the system to enable blockchain based anti-counterfeiting are discussed and the advantage of expanding the existing system, instead of developing a new system is explored.

6.1 modum.io's Architecture

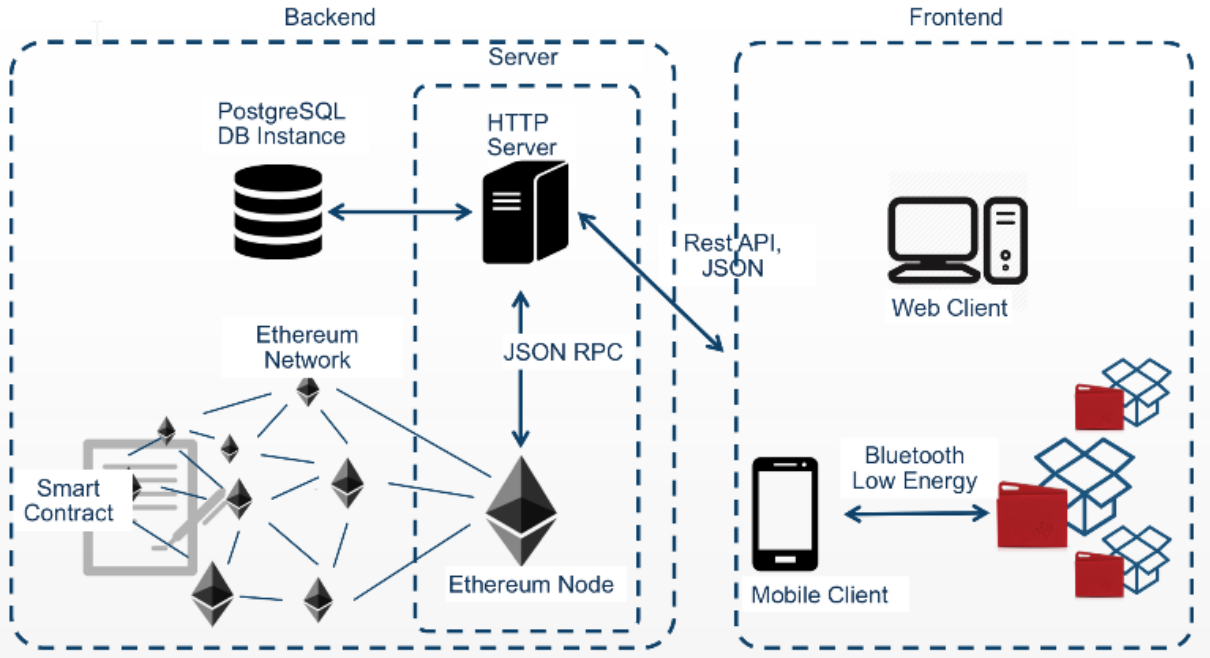

Figure 8: modum.io - High Level System Overview

Figure 8 provides an overview of modum.io's current architecture. The system can be split into front-end and back-end. The front-end consists of different clients, an Android and iOS (under development) mobile client and a web client which provides a better overview. The back-end consists of an HTTP server, a local PostgresSQL and also runs a full Ethereum node. A more detailed view on the server is provided in Figure 9. The server is written in GO, due to the integration with Ethereum. It also manages the smart contracts.

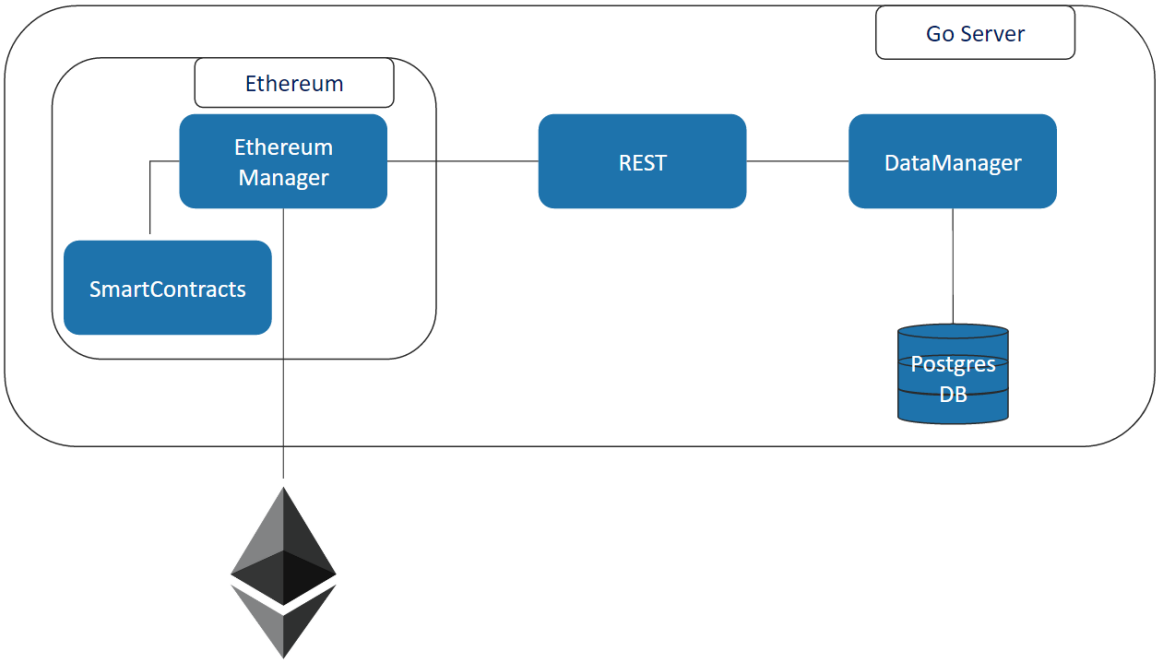

Figure 9: modum.io - High Level Go Server Overview [91]

The system is designed to track the temperature of parcels. To start the tracking of a new parcel, the mobile client starts an sensor, which registers the temperature. This beginning of tracking is transferred to the back-end, where a smart contract is deployed. Once the parcel is received, the temperature data is received from the mobile sensor and sent to the server. The server checks if the temperature always stayed within the temperature range and updates the state of the smart contract. Once the smart contract is successfully mined, the status of the shipment is visible in the web and android client (the android client also shows the expected result before the contract is actually mined).

The architecture and work-flow of the modum.io stack is focused on the temperature use case. To allow using the modum.io stack for a counterfeiting use case several changes are necessary, which are discussed in the next section.

6.2 Advantages of Expanding modum.io's System

Instead of building on the existing solution, one could pursue the option to build something new. However, due to the strong competition in the field of anti-counterfeit solutions using

blockchain technologies, it is unlikely to develop a solution with novice aspects within a reasonable time. Especially, since the market is moving rapidly and new startups working in this field appear constantly.

Combining modum.io's system, which allows for temperature tracking and uses a sensor can also track more environmental factors, can provide additional value. Unlike competitors, who only ensure the authenticity of the product, the combination of environmental data with anti-counterfeit aspects allows for ensuring authenticity and the quality of a product. This is especially interesting for products which are valuable and perishable, such as pharmaceuticals or certain food.

6.3 Required Changes

To use modum.io's system for the counterfeit use case, several key changes have to be introduced.

- Clear definition of entities:

  modum.io's system has grown rapidly over the last months. While the user management only included one entity type in the beginning (users), the notion of companies was added at a later stage. However, there is no clear guideline on when the user or company should be used to decide which data to return.

  In the anti-counterfeit use case, it should clearly be a company which has the competence to add new products. There is also the question which entity is allowed to do what, and if all organizations should be able to create a product.

- Registering of products:

  Since the current system focuses on temperature tracking, it only includes the option to create shipments. There should therefore be an option to register a product, and not just a shipment.

- Multiple hops:

  As stated before, the system is built on the idea that a product is shipped from location A to B. To allow better tracking, which helps with anti-counterfeiting (see Chapter 2), a product should not only be registered and tracked from A to B, but registered at every step. Depending on the use case, it should also be decommissioned at a final stop, this is however product specific. In the context of modum.io's focus (pharmaceuticals), it does make sense to include decommissioning. However, for other products, such as art and long-living consumer products, it should not be required.

- New smart contracts:

  The existing smart contracts store the information if a parcel stayed within the existing temperature range. New smart contracts are required, which enable product registration over multiple hops. Furthermore, instead of deploying a new smart

contract every time a parcel is sent, the same smart contract can be reused to save gas, as the temperature range must be complied with over the whole lifecycle of a product.

- Usage of decentralized storage for documents:

  Using a public blockchain does ensure data immutability, which also means that the data will exist, even if an organizations ceases to exist. Using decentralized storage would allow to also store documents independent of modum.io's future. Like using a public blockchain, this can increase trust. However, discussions with stakeholders have also shown, that this introduces concerns, even if the data is encrypted. The information that data is publicly available, even if only readable with a key, is not a desirable goal for some stakeholders, due to the fear of data leaks.

These changes have an impact on the current system. The impact, how and if they enable reducing counterfeits, and the role of the blockchain in this process is explored in the next chapter.

Chapter 7

Evaluation

After considering the changes to the modum.io system, the question arises how these can reduce counterfeits. This is discussed in this chapter, as well as which questions remain open and are still to be answered. Finally, the importance and benefits of blockchains for the use case are discussed in this chapter.

7.1 Effects of the Proposed Changes

The proposed changes in the last chapter allow the modum.io system for multiple more use cases. It introduces several mechanisms which can be used to reduce counterfeits.

Registering products by manufacturers is a first step in ensuring that the system can be adopted for an anti-counterfeit use case. Registering multiple hops allows for tracing a product over its lifetime, another measure which can helps to reduce counterfeits (see Chapter 2).

The smart contracts must represent these changes. For every physical product, a smart contract can be deployed on production and ownership as well as location updated within the blockchain. This information can be combined with the existing temperature reports, which does not only permit introducing anti-counterfeit measures, but can also track the quality of a product.

The usage of decentralized storage facilitates independent storage of documents. This moves modum.io's system more in the direction of a fully decentralized system. However, since a full Ethereum node is still required, a fully decentralized system seems unlikely until the Ethereum light client, which is schedule for release in 2017 [45], is available.

7.2 Limitations

The discussed changes still have several limitations. They are primarily concerned with an electronic data hub, not the physical protection of the goods. The question on how

to ensure non-physical tampering remains to be answered. This question is however highly product specific, and general approaches have been introduced in Chapter 2 and 5 respectively.

The explorative approach of this thesis resulted in many concepts. Only some of them could be pursued in the context of this thesis. The proposed changes to the modum.io system are still ongoing, and might be adapt when business cases become more evident.

Current technical limitations prevent moving the system into a completely decentralized direction for the moment. The upcoming light Ethereum client might however open possibilities to remove the central server from the architecture, and reduce single point of failures.

7.3 Role of the Blockchain in Reducing Counterfeits

The question remains, on how the blockchain can help with reducing counterfeits, or if it is required. It can be argued that most discussed measures, can also be undertaken without using blockchain technologies. However, many blockchain characteristics provide a great potential for the use case.

The immutability of a blockchain ensures that the data cannot be tampered with. The history of all transactions ensures auditability. Using public blockchains ensures that the system is not dependent on single entities, and that in case of a system failure, the data is still available. From a business perspective, the usage of a blockchain technologies can create trust into the system, especially if using an open system, as it adds transparency. This transparency can, however, also lead to fear of data leaks and loss of control. It is therefore important to ensure that the technologies used are in-line with the business goals.

Finally, blockchain technologies cannot be a standalone solution in reducing counterfeits, but only be part of a comprehensive approach. This must include technical means, as well as also physical attributes, such as tamper-proof packaging, legal and educational measures. Which aspects to focus on are highly dependent on the specific product and who the system should be used by.

Chapter 8

Summary, Conclusion and Future Work

This thesis aimed at exploring how blockchain technologies can be used to reduce counterfeits. To achieve this, the problem and consequences of counterfeiting were introduced and different blockchain technologies and deployment models analyzed and discussed.

Different approaches for specific use cases were developed and explored, discussing how and which blockchain technologies would be appropriate to use. It became obvious that blockchain technologies can be used for anti-counterfeit use cases, but that blockchains cannot be a standalone solution. They can only be considered as part of a holistic approach solving the issue, which needs to be problem specific and varies from case to case.

Finally, the research during the last few months showed that there is extensive movement in the blockchain field. Many technologies considered in the beginning have changed drastically over the course of the last few months, and so have other blockchain based products. Any work in the blockchain research should focus on a specific, tangible issue to be solved. Any general work would likely become obsolete within a short period of time.

8.1 Conclusion

The question if blockchains can reduce counterfeited products is a complex one. Blockchains cannot be considered as the solution to counterfeits, but they can be part of a technological stack to fight counterfeits.

It is important to note that reducing counterfeits cannot be achieved by only using technological means. Increasing awareness, fighting counterfeiters on a legal level, a good alert system, and having tamper-proof packaging must all also taken into account. A holistic approach is required to reduce and prevent counterfeiting.

However, blockchains can be an important layer in the technology stack to fight counterfeits. Using IoT or unique identifiers, physical goods can be linked to a blockchain, where

every transaction of the item can be stored. This allows for perfect traceability, combined with the fact that the data cannot be tampered with. Using public blockchains, trust in the system can be increased, which adds an extra benefit, especially if there is no trust into central authorities.

8.2 Future Work

Within this thesis, multiple approaches to reduce counterfeits were focused on. To be less dependent on external factors, changes to the existing system of modum.io were considered and their impact on reducing counterfeits evaluated. It was not possible to implement all the proposed changes, due to time constraints and the fact that multiple other changes to the system were also necessary. Further work includes the finalizing of these implementations for the modum.io system, and considering the possibility to run pilots.

The concept and implementation to reduce counterfeits in the humanitarian supply chain is still under development. Further work does not only include finalizing the implementation, but finding partners to run a pilot and evaluate the results.

Finally, the combination of IoT and blockchain technologies was looked at in this thesis, but not covered in depth. The combination of these two technologies might enable many more interesting use cases on how to reduce counterfeits.

Bibliography

[1] R. Aitken, *IBM's Blockchain Consortium With The Seam Deploys 'Hyperledger' For Cotton Trading*, 7.1.2017. [Online]. Available: `http://www.forbes.com/sites/rogeraitken/2017/01/07/ibms-blockchain-consortium-with-the-seam-deploys-hyperledger-for-cotton-trading`. [Accessed: 12.1.2017].

[2] E. C. Agbaraji, D. O. Ochulor and G. N. Ezeh, "Food and Drug Counterfeiting in the Developing Nations; The Implications and Way-Out", in *Academic Research International*, vol. 3, no. 2, p. 24-31, 2012.

[3] P. Aldhous, "Counterfeit pharmaceuticals: murder by medicine", in *Nature*, vol. 434, no. 7030, p. 132-136, 2005.

[4] I. Bentov, C. Lee, A. Mizrahi and M. Rosenfeld, "Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake", in *SIGMETRICS Perform. Eval. Rev.*, Vol. 42, no 3, p. 34-37, 2014.

[5] B. Berman, "Strategies to detect and reduce counterfeiting activity", in *Business Horizons*, vol. 51, no. 3, p. 191-199, 2008.

[6] I. B. G. Bernstein, *Drug Supply Chain Security Act - Overview & Implementation (Presentation)*, 12.3.2014. [Online]. Available: `http://www.fda.gov/downloads/Drugs/DevelopmentApprovalProcess/SmallBusinessAssistance/UCM388945.pdf`. [Accessed: 1.1.2017].

[7] Block Verify, *Block Verify - Blockchain Based Anti-Counterfeit Solution*, 2016. [Online]. Available: `http://www.blockverify.io/`. [Accessed: 26.12.2016].

[8] Blockapps, *Scalable Enterprise Blockchains*, 2016. [Online]. Available: `http://www.blockapps.net/`. [Accessed: 25.12.2016].

[9] Blockapps, *Strato - Build Smarter Blockchain Applications*, 2016. [Online]. Available: `https://consensys.net/static/StratoPR.pdf`. [Accessed: 29.12.2016].

[10] Bloomberg, *Company Overview of Venture Proxy Ltd.*, 2016. [Online]. Available: `http://www.bloomberg.com/research/stocks/private/snapshot.asp?privcapid=307764328`. [Accessed: 26.12.2016].

[11] R. G. Brown, *Introducing R3 Corda: A Distributed Ledger Designed for Financial Services*, 5.4.2016. [Online]. Available: `http://www.r3cev.com/blog/2016/4/4/introducing-r3-corda-a-distributed-ledger-designed-for-financial-services`. [Accessed: 25.12.2016].

[12] J. P. Buntinx, *Block Verify turns Bitcoin into a Life-Saving Technology*, 8.3.2015. [Online]. Available: http://bitcoinist.com/block-verify-turns-bitcoin-life-saving-technology/. [Accessed: 27.12.2016].

[13] M. Butcher, *Verisart Plans To Use The Blockchain To Verify The Authenticity Of Artworks*. [Online]. Available: https://techcrunch.com/2015/07/07/verisart-plans-to-use-the-blockchain-to-verify-the-authencity-of-artworks/. [Accessed: 24.12.2016].

[14] V. Buterin, *On Public and Private Blockchains*. [Online]. Available: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/. [Accessed: 10.12.2017].

[15] R. Campbell, *Babyghost and VeChain: Fashion on the Blockchain*, 18.10.2016. [Online]. Available: https://bitcoinmagazine.com/articles/babyghost-and-vechain-fashion-on-the-blockchain-1476807653. [Accessed: 21.12.2016].

[16] M. del Castillo. *Microsoft Doubles Down on Ethereum With New Blockchain Product*, 3.11.2016. [Online]. Available: http://www.coindesk.com/microsoft-launching-new-ethereum-blockchain-product/. [Accessed: 12.11.2016].

[17] M. del Castillo. *Microsoft Doubles Down on Ethereum With New Blockchain Product*, 12.1.2017. [Online]. Available: http://www.coindesk.com/swift-building-blockchain-app-optimize-global-cash-liquidity/. [Accessed: 13.1.2017].

[18] A. Chen, "We need to know who Satoshi Nakamoto is" in *The New Yorker*, 9.5.2016. [Online]. Available: http://www.newyorker.com/business/currency/we-need-to-know-who-satoshi-nakamoto-is. [Accessed: 15.12.2016].

[19] G. Caffyn, *Everledger Brings Blockchain Tech to Fight Against Diamond Theft*, 1.8.2015. [Online]. Available: http://www.coindesk.com/everledger-blockchain-tech-fight-diamond-theft/. [Accessed: 12.12.2016].

[20] Chain, *Chain - Enterprise Blockchain Infrastructure*, 2016. [Online]. Available: https://chain.com/. [Accessed: 24.12.2016].

[21] Chain, *Chain Protocol Whitepaper*, 2016. [Online]. Available: https://chain.com/docs/protocol/papers/whitepaper. [Accessed: 24.12.2016].

[22] Chain, *Chain Protocol Federated Consensus*, 2016. [Online]. Available: https://chain.com/docs/protocol/papers/federated-consensus. [Accessed: 24.12.2016].

[23] Chain, *Chain Enterprise - Your partner from design to deployment*, 2016. [Online]. Available: https://chain.com/enterprise/. [Accessed: 24.12.2016].

[24] Chronicled Inc., *Chronicled, Inc. Announces $1,400,000 Financing For Consumer Authenticity Technology Platform With Silicon Valley Investors And Seattle Seahawks RB Marshawn Lynch*, 9.9.2015. [Online]. Available: http://www.prnewswire.com/news-releases/chronicled-inc-announces-1400000-financing-for-consumer-authenticity-technology-platform-with-

silicon-valley-investors-and-seattle-seahawks-rb-marshawn-lynch-300140030.html. [Accessed: 23.12.2016].

[25] Chronicled Inc., *An Open Registry for the Internet of Everything*, 2016. [Online]. Available: http://chronicled.org/. [Accessed: 23.12.2016].

[26] Chronicled Inc., *Linking the Physical World to the Blockchain*, 2016. [Online]. Available: http://www.chronicled.com/. [Accessed: 23.12.2016].

[27] Chronicled Inc., *We're using breakthrough tech to eliminate fakes forever.*, 2016. [Online]. Available: https://web.archive.org/web/20160809222307/http://chronicled.com/, 2016 [Accessed: 23.12.2016].

[28] Coinmakretcap, *Crypto-Currency Market Capitalizations*. [Online]. Available: https://coinmarketcap.com/all/views/all/. [Accessed: 12.1.2017].

[29] P. Daian, *Analyisis of the DAO exploit*, 18.6.2016. [Online]. Available: http://hackingdistributed.com/2016/06/18/analysis-of-the-dao-exploit/. [Accessed: 24.12.2016].

[30] C. Decker and R. Wattenhofer, "Information propagation in the Bitcoin network," in *IEEE P2P 2013 Proceedings*, Trento, p. 1-10, 2013.

[31] Deloitte, *Israel: A Hotspot for Blockchain Innovation*, 2016. [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/il/Documents/financial-services/israel_a_hotspot_for_blockchain_innovation_feb2016_1.1.pdf. [Accessed: 2.11.2016].

[32] K. Dégardin, Y. Roggo and P. Margot. "Understanding and fighting the medicine counterfeit market", in *Journal of Pharmaceutical and Biomedical Analysis*, vol. 87, p. 167-175, 2013.

[33] Ethereum, *Solidity*, 2016. [Online]. https://solidity.readthedocs.io/en/develop/. [Accessed: 12.1.2017].

[34] Ethereum.org, *About the Ethereum Foundation*. [Online]. https://www.ethereum.org/foundation. [Accessed: 12.1.2017].

[35] Ethereum classic, *Ethereum Classic - Decentralized, Immutable, Unstoppable*. [Online]. Available: https://ethereumclassic.github.io/. [Accessed: 14.10.2016].

[36] European Commission. *COMMISSION DELEGATED REGULATION (EU) 2016/161 of 2 October 2015 supplementing Directive 2001/83/EC of the European Parliament and of the Council by laying down detailed rules for the safety features appearing on the packaging of medicinal products for human use*, 9.2.2016. [Online]. Available: https://ec.europa.eu/health/sites/health/files/files/eudralex/vol-1/reg_2016_161/reg_2016_161_en.pdf. [Accessed: 1.1.2017].

[37] European Commission, *Safety Features for Medical Products for Human Use = Question and Answers V.5*, 6.2016. [Online]. Available: https://ec.europa.eu/health/sites/health/files/files/falsified_medicines/qa_safetyfeature_v5_0.pdf. [Accessed: 1.1.2017].

[38] Everledger, *Everledger ∼ beta*, 2016. [Online]. Available: http://www.everledger.io/. [Accessed: 26.12.2016].

[39] Everledger, *Everledger - What Kind Of Technology Do We Use?*, 2016. [Online]. Available: http://www.everledger.io/smart_contracts. [Accessed: 26.12.2016].

[40] Factom, *Factom apollo: Real Time Auditing / Process Verification Engine*, 2016. [Online]. Available: *https://www.factom.com/products/apollo*. [Accessed: 26.12.2016].

[41] Factom, *Factom hera - Private, permissioned distributed ledgers built custom for enterprise needs*, 2016. [Online]. Available: *https://www.factom.com/products/hera*. [Accessed: 26.12.2016].

[42] Factom, *Factom iris - True Digital Identity*, 2016. [Online]. Available: *https://www.factom.com/products/iris*. [Accessed: 26.12.2016].

[43] Factom, *Factom - Products*, 2016. [Online]. Available: *https://www.factom.com/products*. [Accessed: 26.12.2016].

[44] Factom, *Factom Developers - Factoids*, 2016. [Online]. Available: https://www.factom.com/devs/tokens/factoids. [Accessed: 26.12.2016].

[45] Z. Feldöldi, 7.1.2017. *Introduction of the Light CLient for DApp developers*. [Online]. Available: https://blog.ethereum.org/2017/01/07/introduction-light-client-dapp-developers/, [Accessed: 7.1.2017].

[46] HP, *HP and African Social Enterprise mPedigree Network Fight Counterfeit Drugs in Africa*, 6.12.2016. [Online]. Available: http://www8.hp.com/us/en/hp-news/press-release.html?id=814373#.WGSobxsrL-h. [Accessed 7.12.2016].

[47] G. Greenspan and M. Zehavi, *Will Provenance Be the Blockchain's Break Out Use Case in 2016?*, 7.1.2016. [Online]. Available: http://www.coindesk.com/provenance-blockchain-tech-app/. [Accessed: 12.12.2016].

[48] A. Hertig, *Blockchain Startup Chronicled Launches Ethereum IoT Registry*, 24.8.2016. [Online]. Available: http://www.coindesk.com/blockchain-startup-chronicled-launches-ethereum-iot-registry/. [Accessed: 23.12.2016].

[49] S. Higgins, *Commonwealth Bank, Wells Fargo Test Blockchain for Cotton Trade*, 24.10.2016. [Online]. Available: http://www.coindesk.com/commonwealth-bank-wells-fargo-test-blockchain-cotton-trade/. [Accessed: 12.12.2016].

[50] C. Hulsenapple, *Block Verify Uses Blockchains to End Counterfeiting and 'Make World More Honest'*, 15.3.2015. [Online]. Available: https://cointelegraph.com/news/block-verify-uses-blockchains-to-end-counterfeiting-and-make-world-more-honest/. [Accessed: 27.12.2016].

[51] Hyperledger *Hyperledger - Bloickchain Technologies for Business*, 2016. Available: https://www.hyperledger.org/.[Accessed: 18.12.2016].

[52] Hyperledger *Projects - Hyperledger*, 2016. Available: https://www.hyperledger.org/community/projects. [Accessed: 18.12.2016].

[53] IBM, *Sproxil, Inc. Teams with IBM to Help Consumers, Industry, in the Fight Against Drug Counterfeiting - Press Release*, 1.5.2012. [Online]. Available: `http://www-03.ibm.com/press/us/en/pressrelease/37579.wss`. [Accessed: 27.11.2016].

[54] Intel Corporation, *Sawtooth Lake - Introduction*, 2016. [Online]. Available: `https://intelledger.github.io/introduction.html`. [Accessed: 1.1.2017].

[55] Ioata, *IOATA- The Next Generation Blockchain*, 2016. [Online]. Available: `https://www.iotatoken.com/`. [Accessed: 30.12.2016].

[56] C. Krähenühl, I. Haynes and F. Menardo, *2016: The year to take serialisation seriously*, 18.1.2016. [Online]. Available: `https://www.securingindustry.com/pharmaceuticals/2016-the-year-to-take-serialisation-seriously-/s40/a2652/#.WHldmRsrL-g`. [Accessed: 1.1.2017].

[57] F. Lange, *Setting up private network or local cluster*, 26.4.2016. [Online]. Available: `https://github.com/ethereum/go-ethereum/wiki/Setting-up-private-network-or-local-cluster`. [Accessed: 11.1.2017].

[58] T. Levitt, "Blockchain technology trialled to tackle slavery in the fishing industry", *The Guardian*, 7.9.2016. [Online]. Available: `https://www.theguardian.com/sustainable-business/2016/sep/07/blockchain-fish-slavery-free-seafood-sustainable-technology`. [Accessed: 10.12.2016].

[59] L. Li, "Technology designed to combat fakes in the global supply chain", in *Business Horizons*, vol. 56, no. 2, p. 167-177, 2013.

[60] N. Lomas, *Everledger is Using Blockchain To Combat Fraud, Starting With Diamonds*, 29.6.2015. [Online]. Available: `https://techcrunch.com/2015/06/29/everledger/`. [Accessed: 12.12.2016].

[61] T. McConaghy, R. Marques, A. Müller, D. De Jonghe, T. McConaghy, G. McMullen, R. Henderson, S. Bellemare and A. Granzotto, *BigchainDB: A Scalable BLockchain Databae (Whitepaper)*, 2.2016. [Online]. Available: `https://www.bigchaindb.com/whitepaper/`. [Accessed: 25.12.2016].

[62] Microsoft, *https://azure.microsoft.com/en-us/marketplace/partners/blockapps/strato-blockchain-lts-vm/*, 2016. [Online]. Available: `https://azure.microsoft.com/en-us/marketplace/partners/blockapps/strato-blockchain-lts-vm/`. [Accessed: 11.12.2016].

[63] Monax, *Monax - The Ecosystem Application Platform*, 2016. [Online]. Available: `https://monax.io/`. [Accessed: 12.1.2017].

[64] Monax, *Monax - Software Development Kits*, 2016. [Online]. Available: `https://monax.io/library/`. [Accessed: 12.1.2017].

[65] Monax, *Monax - Eris Platform*, 2016. [Online]. Available: `https://monax.io/platform/`. [Accessed: 12.1.2017].

[66] Monax, *Monax - Eris Platform | Blockchain Client*, 2016. [Online]. Available: `https://monax.io/platform/db/`. [Accessed: 12.1.2017].

[67] A. Morrison. “Blockchain and smart contract automation: How smart contracts automate digital business”, in *PwC Technology Forecast*, 2016. [Online]. https://www.pwc.com/us/en/technology-forecast/2016/blockchain/pwc-smart-contract-automation-digital-business.pdf. [Accessed: 4.12.2016].

[68] mPedigree, *mPedigree - Bring Quality to Life*, 2016. [Online]. Available: http://mpedigree.net/ [Accessed: 25.12.2016].

[69] mPedigree, *GoldKeys - Case Studies* , 2016. [Online]. Available: http://goldkeys.org/about-goldkeys/ [Accessed: 25.12.2016].

[70] Nxt, *Nxt decentralizing the future*, 2016. [Online]. Available: https://nxt.org/. [Accessed: 30.12.2016].

[71] Nxt Community, *Nxt Whitepaper Rev. 4 V1.2.2*, 12.7.2014. [Online]. Available: https://www.dropbox.com/s/cbuwrorf672c0yy/NxtWhitepaper_v122_rev4.pdf. [Accessed: 30.12.2016].

[72] N. Minichiello, *SmartContract + Factom Annaunce Collaboration*, 28.7.2016. [Online]. Available: https://www.factom.com/blog/smartcontract-factom-announce-collaboration. [Accessed: 10.1.2017].

[73] Norton Rose Fulbright, “Can smart contracts be legally binding contracts¿‘, *An R3 and Norton Rose Fullright White Paper*, 2016.

[74] OECD, *The Economic Impact of Counterfeiting and Piracy - Executive Summary*, 2007. [Online]. Available: https://www.oecd.org/sti/38707619.pdf. [Accessed: 2.11.2017].

[75] Y. B. Perez, *How Provenance is Channeling the Blockchain for Social Good*, 17.12.2016. [Online]. Available: http://www.coindesk.com/provenance-channeling-blockchain-social-good/. [Accessed: 12.12.2016].

[76] S. Popov, *The tangle*, 3.4.2016. [Online]. Available: https://www.iotatoken.com/IOTA_Whitepaper.pdf. [Accessed: 20.10.2016].

[77] Project Provenance Ltd, *Every product has a story*, 2016. [Online]. Available: https://www.provenance.org/. [Accessed: 12.12.2016].

[78] Project Provenance Ltd, *From shore to plate: Tracking tuna on the blockchain*, 15.7.2016.. [Online]. Available: https://www.provenance.org/tracking_tuna_on_the_blockchain. [Accessed: 12.12.2016].

[79] Provenance Team, *Provenance use Ethereum to make opaque supply chains transparent*, 28.3.2015. [Online]. Available: https://www.provenance.org/news/us/provenance-use-ethereum-make-supply-chains-transparent/. [Accessed: 12.12.2016].

[80] P. Rizzo, *Chronicled Raises $3.4 Million to Bring Blockchain Verification to Sneaker Trade*, 9.3.2016. [Online]. Available: http://www.coindesk.com/chronicled-blockchain-authentication-3-4-million/, 9.3.2016 [Accessed: 23.12.2016].

[81] P. Rizzo, *Why Chronicled Believes Sneakers Could Be Blockchain's Big Market*, 23.3.2016. [Online]. Available: `http://www.coindesk.com/chronicled-sneakers-blockchain-big-market/`. [Accessed: 23.12.2016].

[82] N. Satoshi, *Bitcoin: A peer-to-peer electronic cash system*, 2008. [Online]. Available: `https://bitcoin.org/bitcoin.pdf` [Accessed: 24.8.2016]. E

[83] S. Sriram and Z. N. Manian, "Cryptographic verification of provenance in a supply chain", U.S. Patent 14 562 303, 9.6.2016.

[84] K. Shirriff, *Hidden surprises in the Bitcoin blockchain and how they are stored: Nelson Mandela, Wikileaks, photos, and Python software*, 02.2014. [Online]. Available: `http://www.righto.com/2014/02/ascii-bernanke-wikileaks-photographs.html`. Accessed: [1.1.2017].

[85] J. Steiner, J. Baker and G. Wood, *Blockchain: the solution for transparency in product supply chains Provenance Whitepaper*, 21.11.2015. [Online]. Available: `https://www.provenance.org/whitepaper`. [Accessed: 10.10.2016].

[86] Skuchain, *Skuchain Brackets Blockchain Technology for Collaborative Commerce*, 2016. [Online]. Available: `https://www.skuchain.com/`. [Accessed: 10.10.2016].

[87] P. Snow, B. Deery, J. Lu, D. Johnston and P. Kirby, "Factom Business Processes Secured by Immutable Audit Trails on the Blockchain", *Factom Whitepaper*, 17.11.2014. [Online]. Available: `https://github.com/FactomProject/FactomDocs/raw/master/Factom_Whitepaper.pdf`. [Accessed: 12.12.2016].

[88] Sproxil, *Sproxil - Protection Through Engagement*, 2016. [Online]. Available: `https://www.sproxil.com/`. [Accessed: 25.12.2016].

[89] M. Swan, *Blockchain: Blueprint for a new Economy*. Sebastopol, CA: O'Reilly Media, Inc., 2015.

[90] J. Tarmy, *A Tech Startup Is Trying to Catalogue Every Piece of Art on the Market*, 21.7.2015. [Online]. Available: `https://www.bloomberg.com/news/articles/2015-07-21/a-tech-startup-is-trying-to-catalogue-every-piece-of-art-on-the-market`. [Accessed: 25.12.16].

[91] P. Tosetti, *Medicines verification in Europe: What to expect in 2019 - Stakeholder's Workshop Presentation*, 26.2.2016. [Online]. Available: `https://ec.europa.eu/health/sites/health/files/files/falsified_medicines/201602_stakeholders_workshop_final.pdf`. [Accessed: 1.1.2017].

[92] tracelink, *EU Falsified Medicines Directive Becomes Official With February 2019 Deadline*, 9.2.2016. [Online]. Available: `http://www.tracelink.com/resources/eu-falsified-medicines-directive-becomes-official-feb-2019-deadline`. [Accessed: 1.1.2017].

[93] S. Underwood, "Blockchain Beyond Bitcoin", in *Communications of the ACM*, vol. 59, no. 11, p. 15-17, 2016.

[94] US Africa Business Forum, *mPedigree at the 2016 US Africa Business Forum - Interview Bright Simons*, 2016. [Online]. Available: http://mpedigree.net/news/mpedigree-nigerias-leading-business-daily-business-day-magazines-cover-story/. [Accessed: 25.12.2016].

[95] U.S. Food & Drug, *Are you ready for the Drug Supply Chain Security Act?*, 15.12.2016. [Online]. http://www.fda.gov/Drugs/DrugSafety/DrugIntegrityandSupplyChainSecurity/DrugSupplyChainSecurityAct/ucm427033.htm. [Accessed: 1.1.2017].

[96] U.S. Food & Drug, *Drug Supply Chain Security Act (DSCSA)*, 2016. [Online]. http://www.fda.gov/Drugs/DrugSafety/DrugIntegrityandSupplyChainSecurity/DrugSupplyChainSecurityAct/default.htm. [Accessed: 1.1.2017].

[97] Visa Inc., "Visa Introduces International B2B Payment Solution Built on Chain's Blockchain Technology", *VISA Press Release*, 21.10.2016. [Online]. Available: http://pressreleases.visa.com/phoenix.zhtml?c=215693&p=irol-newsarticlePR&ID=2213700. [Accessed: 12.1.2017].

[98] B. Vitalik, "Ethereum: A next-generation smart contract and decentralized application platform", *Ethereum White Paper*, 2016. [Online]. Available: https://github.com/ethereum/wiki/wiki/White-Paper. [Accessed: 12.1.2017].

[99] Verisart, *Verisart*, 2016. [Online]. Available: https://www.verisart.com/. [Accessed: 25.12.16].

[100] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger", *Ethereum Project Yellow Paper*, 2014. [Online]. Available: http://bitcoinaffiliatelist.com/wp-content/uploads/ethereum.pdf. [Accessed: 12.1.2017].

[101] World Health Organization, "Growing threat from counterfeit medicines", in *Bulletin of the World Health Organization* , vol. 88, no. 4, p. 241-320, 2010.

[102] T. Yamakoto and M. Sonoko, *Iroha Whitepaper v1.0 (draft)*, 2016. [Online]. Available: https://github.com/hyperledger/iroha/blob/master/docs/iroha_whitepaper.md. [Accessed: 11.1.2017].

List of Figures

List of Tables

Appendix A

Contents of the CD

/Abstract.txt English abstract, as required by the department office

/CD_Content.txt This index as plaintext

/Masterarbeit.pdf Digital copy of this thesis

/Presentations Folder containing the presentations

/Thesis Folder containing all LaTeX source files

/Thesis/graphics Folder containing all graphics used in thesis

/Zusfsg.txt German abstract, as required by the department office

Appendix B

Abbreviations

API	Application Programming Interface
App	Application
OECD	Organisation for Economic Co-operation and Development
BTC	Bitcoin
BLE	Bluetooth Low Energy
CVM	Chain Virtual Machine
DSCSA	Drug Supply Chain Security Act
DAG	Directed Acyclic Graph
EPC	Electronic Product Code
ERP	Enterprise Resource Planning
ETC	Ethereum Classic
ETH	Ether
EU	European Union
EVM	Ethereum Virtual Machine
EUFMD	EU Falsified Medicines Directive
FDA	Food and Drug Administration
FMD	Falsified Medicine Directive
IoT	Internet of Things
NFC	Near Field Communication
PoE	Proof-of-Existance
PoET	Proof-of-Elapsed-Time
PoS	Proof-of-Stake
PoW	Proof-of-Work
NGO	Non-Governmental Organization
REST	Representational State Transfer
RFID	Radio Frequency Identification
SDK	Software Development Kit
SMS	Short Message Service
TEE	Trusted Execution Environment
US	United States
WHO	World Health Organization