Aalto University
School of Business

Benefits and guidelines for utilizing blockchain technology in pharmaceutical supply chains

Case Bayer Pharmaceuticals

Bachelor's Thesis
Jani Kurki
20.12.2016
Business Technology

Approved in the Department of Information and Service Economy xx.xx.20xx
and awarded the grade

Table of contents

1 INTRODUCTION

Implementing general purpose technologies, steam engine and electricity among them, has been the most effective way to improve businesses, industries and whole economies (Helpman & Trajtenberg 1994). The latest general purpose technology is information technology which still has not achieved its full potential. The most disruptive innovation within IT is the Internet. However, in 2009, possibly the second most disruptive one began its way to the books of history.

In 2009, a new digital asset and paying system, Bitcoin, was released by an unknown person or group that called itself "Satoshi Nakamoto". Simply put, Bitcoin is a digital currency that has no central bank controlling it. The entire system is decentralized, its transactions are automatically verified by users and the public ledger is secured through extremely strong encryption (Nakamoto, 2008). Bitcoin is the first implementation of the new disruptive technology – blockchain (Antonopoulos, 2014).

Blockchain will most likely transform the economy similarly to general purpose technologies in three phases presented by Helpman and Trajtenberg (1994). First, it will increase productivity in form of new products, then the new products are utilized in various industry and business processes and lastly companies and other entities of the economy change the way they work to match the benefits of the new technology. Blockchain is now in both the first and the second phases: New products are constantly developed and the financial sector is now the first one beginning to implement blockchain to its existing business processes (Swan, 2015). Little academic research has yet been done and, according to Yli-Huumo et al. (2016), it has mostly focused on only privacy and security. Furthermore, they state that new research must be done on scalability and blockchain applications beyond Bitcoin in order to achieve the next step, namely the expansion to other industries. This is where I step in.

The goal of this thesis is to explore how blockchain technology can be utilized in pharmaceutical supply chains. I chose this area to focus on, because it is very dependent on trust, contracts, negotiations, supervising, human interaction and payments through a third party. Product counterfeiting, production and distribution problems, thefts and fraudulent drugs cause multi-billion-dollar revenue losses in the world and pose a serious threat to public health (Papert, Rimpler & Pflaum, 2016). Blockchain technology can tremendously improve performance in all these areas and decrease the risk of the aforementioned issues.

Furthermore, I examine how the proposed measures would impact Bayer AG, a large life science company which was founded in 1863 in Germany and had a revenue of 46.3 billion euros in 2015 (Bayer, 2016). Its core competencies are "in the areas of healthcare and agriculture", and Bayer Pharmaceuticals division is the largest division measured in sales by generating a revenue of 13.7 billion euros in 2015. According to Bayer's annual report 2015 (2016), the division "focuses on prescription products, especially for cardiology and women's healthcare, and on specialty therapeutics in the areas of oncology[1], hematology[2] and ophthalmology[3]". Bayer is also a major conductor of research and the company spent 4.3 billion euros in research in 2015.

2 CONCEPTS

2.1 Blockchain

Blockchain is a *decentralized database* which stores accounts and transactions between them (Swan, 2015). Due to this functionality, blockchain can be described as a *public ledger*. Yli-Huumo et al. (2016) state that every participant, also known as *node*, has the complete and automatically updated list of records of the transactions on the blockchain from the very beginning and the list can be queried, making information about transactions retrievable. List of terms related to the blockchain can be found in appendix.

Figure 1 presents the ledger structure and why the ledger is called a blockchain. Every new transaction broadcast to the network arrives at a "pool" of transactions that require addition to a block, and therefore blocks consist of several transactions. Every block in the list of records refers to the previous one and the network automatically notices if some party tries to modify the chain afterwards (Antonopoulos, 2014). All blocks are identified with a *cryptographic hash* (Christidis & Devetsikiotis, 2016). Swan (2015) writes that cryptographic hashing transforms data to a fixed size of bits through a mathematical algorithm. Antonopoulos (2014) continues that it is "virtually impossible" to find two different inputs that give the identical output. Cryptographic hashes cannot be inverted, so they keep their original data private.

[1] Treatment of cancer
[2] Blood diseases
[3] Diseases of the eyeball

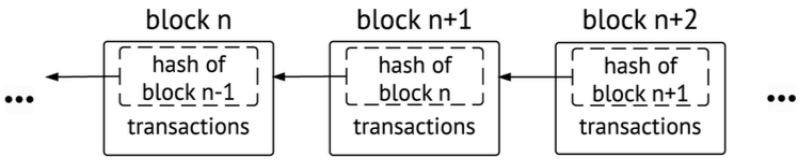

Figure 1. Blocks linked to a chain (Christidis & Devetsikiotis, 2016).

The key idea behind the decentralized system is to get rid of third parties (Yli-Huumo et al. 2016), for example banks, that now verify transactions. In addition to making transactions more efficient, this enables the key breakthrough of the blockchain technology: disrupting trust. No trust must be put to middlemen or other users.

Individuals and organizations can create new accounts for the blockchain network. The account numbers are random, and therefore the individuals and organizations behind the addresses are not exposed. Transactions are executed with certain units. The units represent assets that the users agree upon. Swan (2015) states that they can be physical assets (such as real estate, cars and mobile phones), intangible assets (such as bonds, votes, patents and licenses) or digital assets (such as images, music and e-books) For example, on the Bitcoin blockchain the Bitcoin itself is the unit and represents value in the digital currency. Various kinds of assets can exist on one blockchain (Swan, 2015).

Nakamoto (2008) explains that transactions are executed by creating a transaction message that is then broadcast to the whole network so that every node updates their list of records appropriately. Nakamoto (2008) also presents the process of accepting new transactions as follows:

1) New transactions are broadcast to all nodes.
2) Each node collects new transactions into a block.
3) Each node works on finding a difficult proof-of-work for its block.
4) When a node finds a proof-of-work, it broadcasts the block to all nodes.
5) Nodes accept the block only if all transactions in it are valid and not already spent.
6) Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

Next I clarify these steps. In order to prevent fraud, the transactions require a signature to prove the sender's identity. Every account has an individual *private key* which is a set of numbers and letters that is mathematically linked to the account number, also known as the *public key*, as it is visible to other users (Yli-Huumo et al. 2016). One can also think of the private key as a password and the public key as an email address to demonstrate how they work.

Figure 2 demonstrates how a transaction is first signed by a user and then verified by other users. A signature is created by putting the message and the private key into a cryptographic hash algorithm (Decker & Wattenhofer, 2013). This basically means that the signature keeps the transaction message and the private key secret. Antonopoulos (2014) explains that in order to check if a signature is valid and belongs to the right account number (public key) and transaction message, other users can use another algorithm. Because signatures are made of both the message and the private key, they are unique for every single transaction. In other words, one can verify that parties and transactions are real, but still no information about them is exposed. Hence, no trust is needed between parties. For example, on blockchain network one could verify that a user is of age without ever knowing their name or date of birth.

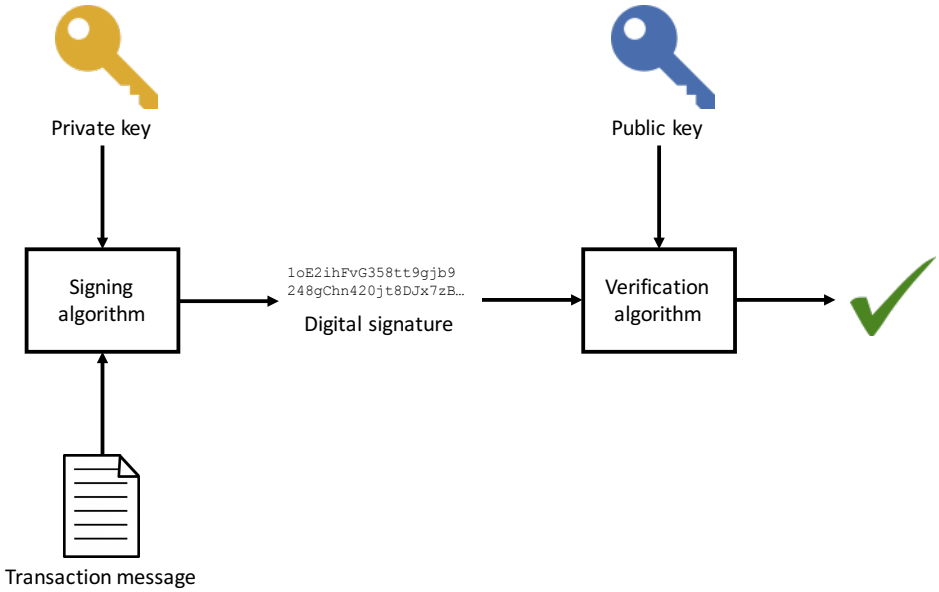

Figure 2. Signing and verifying a transaction.

The signatures indicate the parties of a transaction but not the time of it. The network must in some way agree on the order of transactions. According to Swan (2015), before blockchain technology, the challenge of all digital payment systems has been the *double-spending problem*: digital assets can be copied over and over again and it couldn't be verified if an asset was already spent before. Solving this problem is the key technical innovation of blockchain technology.

Blockchain technology tackles the double-spending problem by requiring computational processing work to verify transactions (Decker & Wattenhofer, 2013). This process is also called *mining*. Antonopoulos (2014) explains that "mining is the process of hashing the block header repeatedly, changing one parameter, until the resulting hash matches a specific target." The specific target changes every time a new block is created. One can

produce a hash result, that matches the specific target, only by randomly guessing the input until the desired hash result is found.

On average, getting the right guess requires trillions of guesses, but when a great number of miners are simultaneously working on the task, it gets solved within a few minutes. Depending on how many miners participate in the task it can naturally get faster or slower to solve the task. In this case, the blockchain is calibrated to change the difficulty of the task so that it will always be solved in about ten minutes.

When the result to the target is found, the solver broadcasts the answer, or *proof-of-work*, to all the nodes of the network and others can prove it automatically (Decker & Wattenhofer, 2013), because they can just insert the result to the function and prove that it matches to the original target. The solver gets a reward for the computing work provided and their block is added to the chain of previous blocks that together make up the list of records. Hence the name *blockchain* technology. Then the process starts again with new unverified transactions.

Because the mining is virtually a guessing game, all miners can get a reward at some point and the odds only depend on how much computing power one can provide (Swan, 2015). The chance of reward is the motivation to keep mining in the future, too. For example, on the Bitcoin blockchain the reward is a certain number of Bitcoins for the solver and this is the way new units are created into the system (Antonopoulos, 2014). He continues that another way of rewarding miners is to implement a small transaction fee that is then given to the successful miner by the user who sent the transaction message in the first place.

Information in the network doesn't universally get updated simultaneously, because it is transferred node by node. This may occasionally cause several different versions (different blocks and thus different transactions) of the blockchain to exist in the network if the same mathematical task is simultaneously solved by several miners. Decker and Wattenhofer (2013) describe these different versions of a blockchain *forks*. Every blockchain calculates how much computing work it has cumulatively required to produce and nodes will eventually adopt the "longest" chain. In a case of three miners solving the block simultaneously the longest chain is defined by which chain the next block is first added to, as visible in Figure 3.

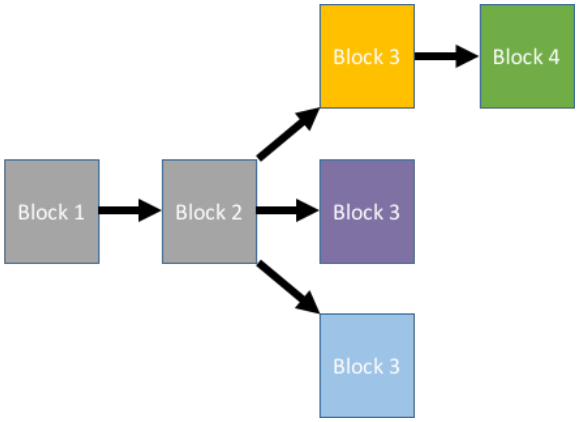

Figure 3. Different versions of one blockchain. The longest one will be adopted in the network.

This is then the longest chain in the whole network and all nodes will eventually adopt this fork (Decker & Wattenhofer, 2013). Taking into account that it takes ten minutes on average to create one block, this transition does not take long. This mechanism ensures that consensus can be reached in a peer-to-peer network. Because a blockchain can have several forks, transactions only become secure after a few further blocks are created. Transactions in abandoned forks are transferred back to the pool of unverified transactions and get eventually added to the longest chain.

Because of forks, a blockchain is in theory prone to fraud through intentional double-spending. Decker and Wattenhofer (2013) describe a situation, where a user could first spend units to buy something and after the transaction send another transaction message to the network, in which the user transfers the same units back to themselves. If the user can beat the odds by solving a new mathematical task for a block that contains their new transaction, there is a fraudulent fork in the network (see Figure 4).

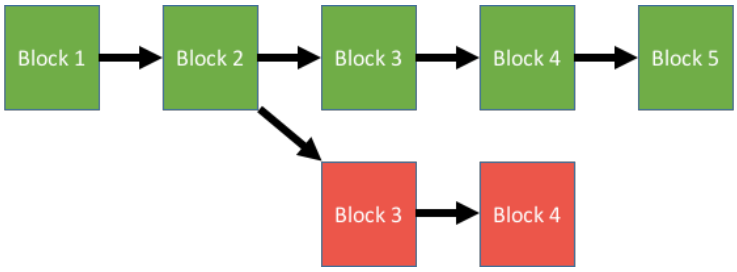

Figure 4. A fraudulent fork on a blockchain (presented as red).

The longest chain is the "honest" chain and it gets new blocks added to it continuously by all other miners. The fraudulent user would need to solve several mathematical tasks in a row to overcome the original chain and get others to use their fork of the blockchain. The probability of succeeding is extremely theoretical. According to Swan (2015), in order to

get a fraudulent chain to become the longest one in practice one must own more than half of the computing power of the whole network (known as *51-percent attack*). However, in decentralized and global networks it is virtually impossible to achieve.

To conclude, a blockchain is a decentralized database that works as a public ledger which stores accounts and a continuously growing list of transactions. Blockchain technology disrupts trust. Every participant in the chain has an automatically updating copy of the ledger and consensus of its transactions is automatically reached. This makes central intermediaries unnecessary and users do not have to put trust on a third party, such as a bank. No trust is needed between strangers on a blockchain, because strong cryptography protects users and transactions and maintains total privacy. Blockchain has solved the double-spending problem by requiring a huge amount of computational processing work to validate transactions. The transactions are then added to the blockchain and cannot be modified afterwards. This makes the chain reliable and safe to use.

2.2 Smart contracts

The fundamental function of blockchain technology is handling asset transfers, as explained in the previous section. However, transactions are not the only function blockchains enable. The idea of smart contracts was first introduced by Szabo (1994). He described them as "a computerized transaction protocol that executes terms of a contract". In other words, smart contract is a paragraph of code that represents a contract and is digitally signed by parties. It is autonomous in the sense that the contract and its issuer do not need to be in further contact after deployment (Swan, 2015). Unlike a conventional legal agreement smart contracts are automatically executed and enforced if agreed terms occur after signing, thus replacing trust with functioning software and erasing the need for a third party enforcer. Christidis and Devetsikiotis (2016) clarify that smart contracts are deterministic and, unlike legal contracts, are not prone to ambiguity: the same input always produces the same output. Bitcoin blockchain does not support smart contracts (Swan 2015) and currently users of Bitcoin utilize smart contracts by using parallel blockchains outside Blockchain network that improve its protocol. The most developed blockchain platform that also enables usage of smart contracts in the same environment is Ethereum.[4] Unlike Bitcoin that only provides a pre-defined set of operations, Ethereum is

[4] Ethereum (2016). Homestead documentation. Retrieved from: http://www.ethdocs.org/en/latest/

a re-programmable blockchain so that new applications can be developed on its platform. This contributes to Ethereum's goal to be "adaptable and flexible", thus becoming a universal platform for developing and using blockchain-based applications.

In the example of Figure 3, a smart contract to sell the admin rights of a website is created on Ethereum's blockchain. The code is represented in a protocol language EtherScript which makes the underlying code readable to laymen (see Figure 5).

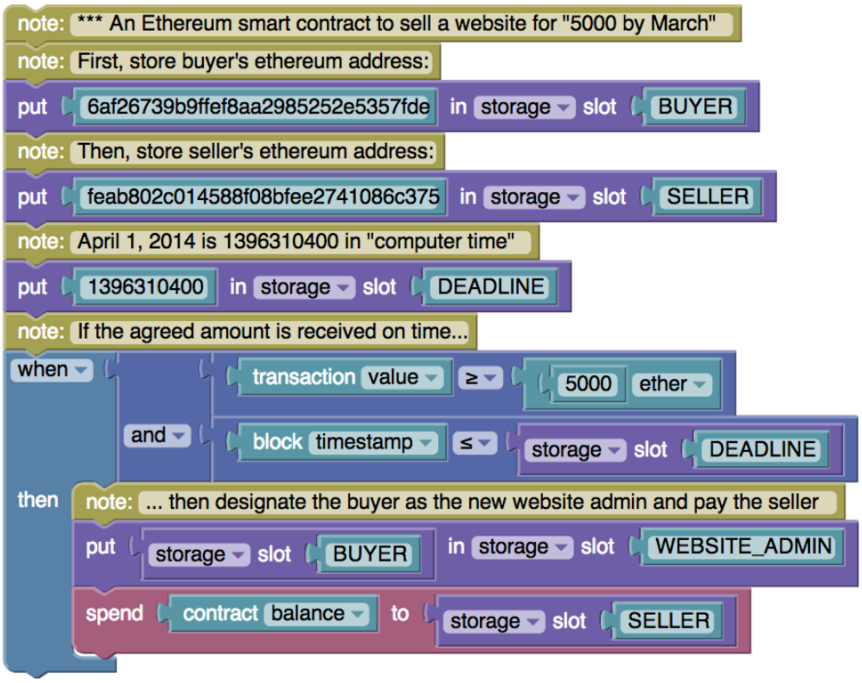

Figure 5. Example of a smart contract. Source: "What is Ethereum?" EtherScripter, 2016, http://etherscripter.com/what_is_ethereum.html. Accessed on November 8th 2016.

Smart contracts are naturally applicable in digital environment only and cannot automatically enforce agreements in the physical world. Internet-of-Things applications must be implemented in order to achieve that (Christidis & Devetsikiotis, 2016).

Only after introduction of blockchain technology have smart contracts become relevant in practice. The secure digital currency of blockchain technology provides a "convenient billing layer" (Christidis & Devetsikiotis, 2016) and automates all contractual conditions because for the first time contracts and objects of contracts reside in the same digital environment. Smart contracts are their own units that exist on the blockchain and they can be spectated by every node of the network.

2.3 Pharmaceutical supply chain

Pharmaceutical supply chains are very different from typical supply chains that start with extracting raw materials and after a few production phases continue with shipping to stores and selling to end customers. The products in the chain are different, too. Shah (2004) describes the life cycle of drugs: Before the typical processes of manufacturing and distribution start it usually takes 10 years to come up with a new potential drug, after which it is protected by a patent. Then another 6-8 years are required for safety and efficacy tests and manufacturing processes.

Failures in pharmaceutical supply chains may even cause death for the end user. According to Chircu et al. (2014) pharmaceutical supply chains have undergone transformations during the last decades. These include strict and diversified regulations and requirements of compliance, complex distribution channels, faster expiration of patents, new requirements of drug safety and the eternal fight against product counterfeiting.

As the basis of my research I will use the model of a generic global pharmaceutical supply chain (Figure 6) created by Chircu et al. (2014).

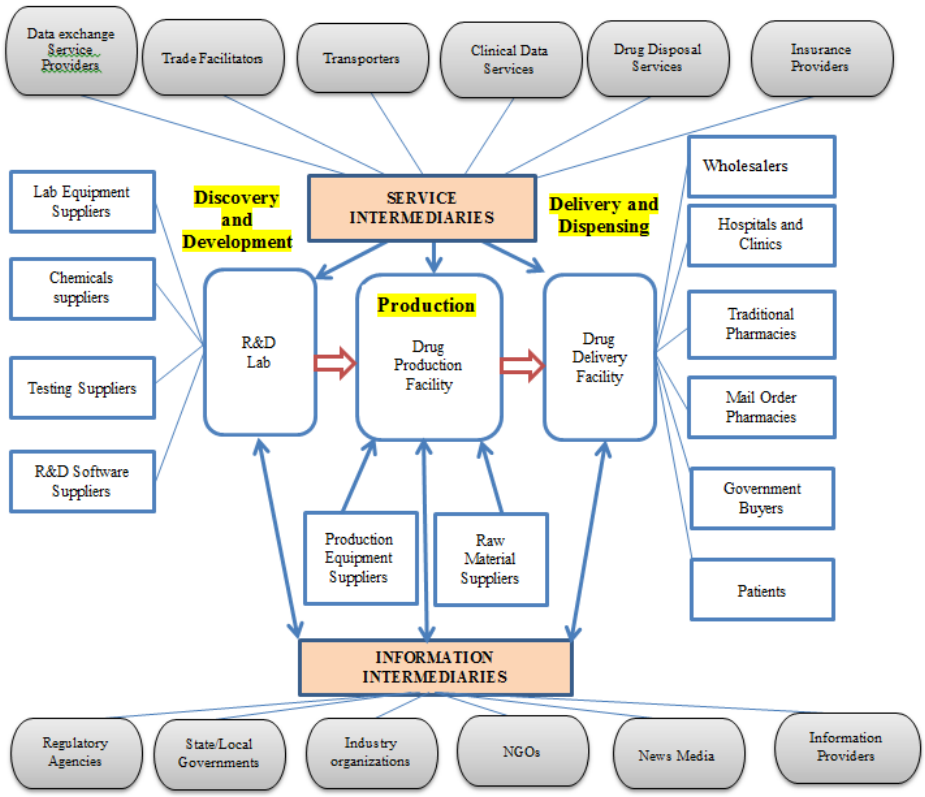

Figure 6. Generic global pharmaceutical industry supply chain (Chircu et al. 2014).

The supply chain in Figure 4 is divided into three parts: discovery and development, production, and delivery and dispensing. In addition, there are two kinds of intermediaries involved: service and information intermediaries. Service intermediaries mainly provide logistics services and information intermediaries exchange data with companies of the supply chain.

3 PARTICIPATING ENTITIES AND INFORMATION FLOW

Although blockchain technology was originally intended to be truly public and distributed (i.e. *public blockchain*), *private blockchains* have also been developed (Swan 2015). Private blockchains limit access to them and they are controlled by one or more entities. Otherwise, public and private blockchains do not differ from one another. According to Christidis & Devetsikiotis (2016) private blockchains are more suitable "for stakeholders who operate in a controlled, regulated environment or who wish a higher throughput than a public network could offer". They argue that mining on a public blockchain requires more computational power than in private ones and it tends to cost more, because miners must be rewarded in one way or another. Also, transactions are computationally more efficient, because fewer nodes participate in the mining process.

The financial industry is now developing blockchain technology to make their existing business processes more efficient and there is a consensus that private blockchains are the correct solution for them (Swan, 2015). Even the Nordic bank Nordea has joined a partnership of 25 major banks to develop blockchain solutions for the financial services.[5] Taking into account that pharmaceutical supply chains also act in a controlled and regulated environment, I suggest a private blockchain to be implemented.

I believe that the private blockchain platform should be developed and implemented by a governmental organization that is responsible for supervision of medicines already. Consequently, I see that the private blockchain in the EU should be hosted by the European Medicines Agency, or short "EMA", that "is responsible for the scientific evaluation, supervision and safety of medicines developed by pharmaceutical companies for use in the EU" (EMA, 2016). A medicine agency's task on the pharmaceutical blockchain is to authorize stakeholders willing to join the network, monitor their actions

[5] Larsson, P. (2015, October 28). Nordea joins groundbreaking technology partnership. *Nordea*. Retrieved from http://www.nordea.com/en/press-and-news/

and medicines and provide information so that only trusted stakeholders are let to do business on the blockchain.

As mentioned earlier, the generic pharmaceutical supply chain represented in Figure 4 is the basis of the pharmaceutical supply chain, but not all stakeholders of the chain need to have access to the shared ledger. The main objective of the shared ledger is to provide safe medicine and make information, material and cash flows more efficient and secure. I present, which stakeholders should join the network.

Starting from the beginning of the (forward) supply chain, the first stakeholders required are R&D labs. Based on their work, I suggest that new patents are created which will exist on the blockchain as intangible assets, and drug producers can buy rights for production with the help of smart contracts. The suppliers of R&D labs are not required to join the blockchain, because their products will not end up in the medicines transported through the supply chain.

Drug production facilities are represented on the blockchain. Their suppliers providing raw materials for drug production are in the network, too. I present that by certifying raw material producers and monitoring material flow from them to production facilities, the risk of counterfeit drugs can be lowered. Suppliers of production equipment are not required on the blockchain, because they only take part in production, not the supply chain itself.

All the stakeholders in delivery and dispensing are represented in the network, as they are involved in the supply chain and medicines are distributed through them. These include delivery facilities, wholesalers, hospitals, clinics, pharmacies, government buyers and the end users – patients. Patients are included in the network if they purchase medicines themselves (through pharmacies) and thus determine themselves, which medicine should be used in which situation. For example, in hospitals staff is responsible for giving the right drugs and hospitals make the last purchase of the supply chain before consumption of the product.

All service intermediaries contribute to at least one of the three flows of the supply chain (cash, information, materials) and thus they should be included on the blockchain. For example, third-party transporters can provide information regarding location of the product and drug disposal service providers can automatically be rewarded for disposing of drugs.

Information intermediaries play a big role on the blockchain. As stated earlier, a government-run regulatory agency should host the blockchain, but also other organizations can be included in the network in order to gather vital information regarding the pharmaceutical supply chain. These organizations can include NGOs and organizations that unite companies in the industry.

As explained in Section 2.1, blockchain technology enables verifying transactions and participating entities without revealing the information and the entities themselves to the public. This is achieved by encryption and the combination of private and public keys. Considering the pharmaceutical supply chain, this allows regulators, supervisors and other stakeholders to verify secure transactions and still lets business partners maintain their trade secrets. For the first time competitors may share all their transactions with one another and still protect their privacy.

As Bayer Pharmaceuticals is active in both R&D and production phases in the supply chain, it benefits greatly from the new blockchain platform. Now that only relevant and trusted stakeholders participate in the network, it is easier for Bayer to find new business partners among both subcontractors and service providers, and choose partners through competition and bidding. For example, choosing raw material suppliers and insurance providers can now safely be done based on competition on price, as the quality is ensured.

According to Bayer's annual report 2015 (2016), most of Bayer's products are covered by patents. Commercializing new products is vital for the company to continue R&D work in the future, too. Still, it takes a lot of time from the patent application to market launch and Bayer only has a few years before the patents expire (Bayer, 2016). Thus, improvements in protecting and commercializing patents can have an enormous impact on the bottom line. On the blockchain, patents are secured with strong encryption so that virtually no intellectual property may be stolen. Furthermore, smart contracts allow flexible ways to commercialize patents, as stated earlier. In Bayer's case, the company could, for example, sell rights to limited usage of its patents before they expire in order to lower motivation to contest patents before expiration.

4 CONTRACTS AND PAYMENTS

As explained in Section 2.2, smart contracts provide an efficient way of creating and executing contracts on a blockchain, because contracts themselves and assets involved in them exist in the same digital environment.

An example: Person A wants to sell an apartment that she owns and creates a smart contract that states the terms of the agreement: If blockchain units worth of 100,000 euros are sent to their account, the sender will automatically gain ownership over the apartment. Person A broadcasts this smart contract to other users of the network and soon person B fulfils the agreement by sending the required amount of money. All stakeholders of the blockchain can now verify that person B owns the apartment in question.

Still, this does not necessarily mean that person A will hand over the physical key and move out from the apartment. Agreements made on the blockchain must in some way be enforced in the physical world. Christidis and Devetsikiotis (2016) propose that Internet-of-Things (IoT) applications can provide a solution to this challenge. They even present an example of smart electronic locks that can only be unlocked by using the owner's digital signature. This way person A would be enforced to leave the apartment that person B now owns in our example. The smart electronic lock is a simple example of *smart property*: property whose ownership is controlled on a blockchain (Swan, 2015).

Chircu et al. (2014) explore possibilities of radio-frequency identification (RFID) tags in pharmaceutical supply chains and find that the technology can tremendously improve for example product security and cost efficiency. These findings are very similar to benefits of blockchain technology and the combination of these two is very suitable for pharmaceutical supply chains. In pharmaceutical supply chains, products are shipped in bulk (Chircu et al. 2014), and Asif and Mandviwalla (2005) also state that pallet-level tagging is much more cost efficient than item-level tagging. Consequently, RFID tags can be installed to packages to track product location (Christidis & Devetsikiotis, 2016). As seen in Figure 5, RFID tags can keep track of the whereabouts of products in the supply chain and automatically inform the location on the blockchain. If a signed smart contract has a term to deliver the package to a certain destination, this information can be verified with the help of RFID tags that broadcast the message on the blockchain and thus to the smart contract (Figure 7).

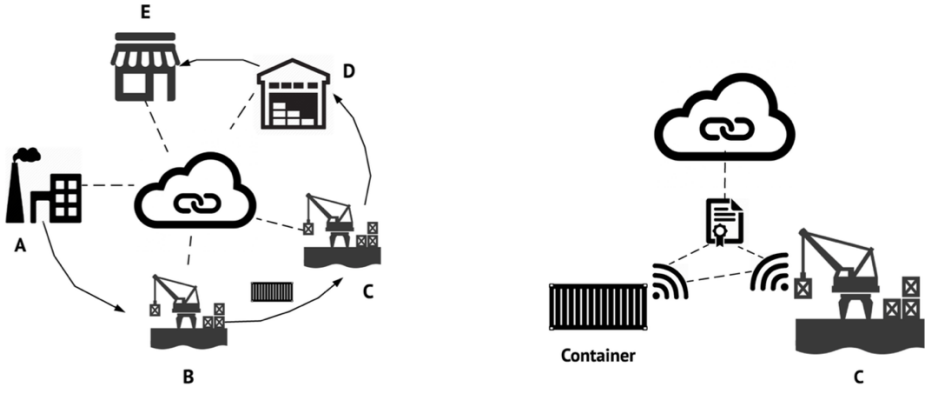

Figure 7. Product tracking and payment with RFID tags on blockchain (Christidis & Devetsikiotis 2016).

The contract is now fulfilled and both the payment and the change in ownership are executed automatically and simultaneously. Smart electronic locks could also be installed to packages, and only the party who has ownership over the products inside could open the package. Other benefits of the combination of RFID and blockchain technology are discussed in Section 5.

Blockchain environment enables executing smart contracts in real time, but it also provides a payment network for machine-to-machine transactions (Swan, 2015). IoT powered machines linked to blockchain can be programmed to perform various tasks independently. In pharmaceutical supply chains, I see that independent machines would be valuable for monitoring stock levels and making smart contracts to order more supplies when required.

With the help of smart contracts and devices linked to the Internet-of-Things, many business processes can be automated and thus supply chains can become leaner than ever before. Swan (2015) even represents the concepts of *decentralized autonomous application (Dapp)* and *decentralized autonomous organization (DAO)*. She describes these as "increasingly complex and automated smart contracts that become more like self-contained entities, conducting pre-programmed and eventually self-programmed operations". In other words, smart contracts can be programmed to a level, where they act like independent applications or even organizations on the blockchain.

Before this becomes reality, I propose that the combination of IoT devices and smart contracts should be used to automate processes in determining, negotiating and executing contracts. Comparable to software that buys and sells stocks, smart contracts could be programmed to negotiate contracts according to pre-determined algorithms. For instance, an RFID sensors of a production facility could keep track of raw materials coming in and going out of the facility and, when the stock level reaches a pre-determined low-point, contact suppliers and negotiate the best contract from the facility's point of view.

Essential challenge in issuing smart contracts is to determine when the conditions of a contract are met. Some conditions can be measured by IoT devices themselves (for instance number of products in stock and weather conditions) but often external information is needed to determine conditions that are met. Swan (2015) calls these external sources of information *oracles* and raises the question of which sources can be trusted by the entire network. She uses the example of a smart contract that is issued to

share heritage after a person passes away. An external source is needed so that smart contract can determine when this condition is met.

A company called Oraclize[6] is tackling this issue by developing a generic oracle service that acts "as a data carrier". It connects to web APIs and delivers required information to blockchains and thus to smart contracts. Oraclize provides cryptographic proof to show that information was not altered by the oracle. The source of the information must still be trusted, though. For the pharmaceutical supply chain Oraclize provides inspiration.

As the pharmaceutical blockchain would be run by a governmental agency, I suggest that a government-run oracle service is integrated onto the blockchain. As stakeholders anyway consent to state-run environment, it is only logical to provide the oracle service as state-run. Like Oraclize, the service would connect to web APIs and share information with the blockchain. In addition, I propose that stakeholders may request the oracle to get access to various sources. This means that smart contract issuer still decides what source is reliable, and the oracle just transfers that data safely utilizing cryptographic proof. Of course, the oracle could proactively offer reliable sources, for example material from the state-run Statistics Finland.

The Bitcoin blockchain's goal is to implement its own decentralized digital currency that gets rid of *fiat currency*. A fiat currency is a currency, the usage of which is determined by law in a country (Selgin & White, 1999). Virtually every current currency worldwide is a fiat currency. As the pharmaceutical blockchain does not strive to run its own independent currency, I see that a connection to the fiat currency must be formed. It is possible to exchange Bitcoins to fiat money on external platforms (Antonopoulos, 2014). As Bitcoin also fluctuates, the exchange rate varies over time.

Companies on the pharmaceutical blockchain will eventually want to exchange their assets to fiat money and thus fluctuating value of assets poses a major risk for trade. In order to avoid fluctuation, I suggest that the government controls the exchange of assets to fiat money. In practice, companies would "buy in" to the network by paying a certain amount in fiat money to the host. The buyer then gets an equivalent number of assets on the blockchain and they can always exchange their assets back to fiat money from the host.

This process is comparable to how casinos issue playing chips to players. As a result of this process, the host virtually creates a new regulated currency that has a fixed exchange

[6] http://docs.oraclize.it/

rate to other currencies. This process also is the way how new value is created in the network, so unlike on the Bitcoin blockchain, mining does not generate new value on the chain.

As banks and other central intermediaries are not involved in transactions, international trade within the supply chain becomes faster and more cost efficient. Now it takes a couple of days for banks to transfer money between each other internationally. On the blockchain, all stakeholders act in one single environment and transactions take place in real time. In order to verify a transaction one must only wait for a few more blocks to be added on top of the block which contains the transaction in question. Direct international transfers pose challenges in taxation, too, due to varying taxation policies between countries.

Walport (2016) suggests, though, that blockchain technology can also be used for collecting value-added tax (VAT). According to him, if EU-wide standards and protocols are developed, collecting VAT in the EU can be performed on a blockchain. This would "reduce the administrative burden imposed on other organizations" and "increase transparency of real-time transactions" (Walport, 2016). Collecting VAT would be proactive instead of retroactive, as it is nowadays. I see it unrealistic that all transactions, where VAT applies, can be controlled on one general blockchain in the near future. Thus, I suggest that after EU-wide standards exist the implementation would be started one industry at a time. As the blockchain for pharmaceutical supply chain would be controlled by an EU-wide organization (EMA) automatic collection of VAT could be implemented when developing the blockchain environment.

As public ledgers blockchains could automatically provide all accounting services a company needs from bookkeeping to reporting taxes and closing the books (Swan, 2015). This would also be proactive instead of retroactive like collecting VAT. As I stated earlier, I find it unrealistic to see one general blockchain in the near future. Still, companies can benefit from automatic accounting. The real-time accounting gives real-time information regarding budgets, income and costs and companies can respond to unwanted changes more quickly.

Bayer Pharmaceuticals can directly utilize all the proposed measures presented in this section. International trade becomes more efficient and secure via direct payments and RFID tags combined with smart locks on the blockchain. Machine-to-machine transactions combined with smart contracts are beneficial for Bayer in maintaining appropriate stock levels in production. The company's workload in accounting and

taxation reduces significantly with the help of blockchain platform, as Pharmaceuticals is the largest division of the company measured in sales.

Oracle services would benefit Bayer especially in developing more flexible smart contract terms. Referring to the flexible patent rights mentioned in the previous section, the company could, for instance, allow patent usage only when the demand peaks higher than what Bayer can independently manufacture. This situation in the markets can be determined, for example, by comparing medicine sales and production, or even proactively by forecasting epidemics globally and reacting to them before they reach the market in question.

5 LOGISTICS, TRANSPARENCY AND PRODUCT SECURITY

Continuing with RFID implementation in pharmaceutical supply chains described by Chircu et al. (2014), RFID tags "can improve communication of data and information, reduce counterfeiting, and enable monitoring of drug quality in supply chain". According to them, RFID tags are suitable for keeping up pharmaceutical supply chain regulations because the tags are easily readable without line of sight, are tamper-proof, have mechanical and chemical stability, and additional sensors can be added for data collection.

Chircu et al. (2014) developed a tentative model for RFID usage in pharmaceutical supply chains. Their model "uses RFID passive tags as well as temperature and motion sensors, coupled with a central infrastructure that enables tracking and tracing of items". Chircu et al. (2014) observed a pilot model launch and stakeholders involved in it were satisfied by the results. In my view, the problem of their model is the "Pharmaceutical Trust Center", which sets up the infrastructure of servers and databases and verifies all products. All stakeholders are required to trust this central intermediary which may act dishonestly or fail to deliver its responsibilities. Also, RFID tags cannot in general identify if the reader device can be trusted, which may lead to unauthorized access to the tags (Asif & Mandviwalla, 2005).

In my view, combining RFID and blockchain technology the aforementioned challenges can be solved while still retaining all the benefits of RFID tags. On a blockchain a central intermediary is unnecessary and on the suggested pharmaceutical chain the only verification process takes place when new stakeholders join the network. This regulated access to the network provides one layer of security, as the participating parties have been at least once verified by the governmental body hosting the network. RFID tags linked to

an asset on the blockchain are also secure, thanks to strong encryption the blockchain provides. Only devices of the current owner of the goods can read the encrypted information, as they have the private key that makes the information readable.

In the pharmaceutical supply chain RFID tags could provide package metadata, when they are read with a permitted device. This could include place of origin, time of production, a map of its travel to the current destination with GPS information and client contact information, among others. Chircu et al. (2014) interviewed manufacturers, wholesalers and end users who had participated in the pilot model and they confirmed that RFID tags lower the cost of human error and make deliveries more efficient. Especially in the end of the supply chain, when the package has reached for example doctors and patients, having easily accessible and reliable information can prevent errors in treatment (Chircu et al. 2014).

RFID tags enable tracking of products, but implementing the proposed blockchain technology makes tracking and tracing automatically available for every stakeholder in the network. The attached sensors proposed by Chircu et al. (2014) make drugs more secure, as they give a signal for example if transportation conditions are poor or if the package is opened during transportation. Blockchain improves sharing information regarding damaged or fraudulent assets (products), because every node on the blockchain can immediately notice if a certain asset is not secure.

The combination of RFID tags and IoT devices linked to blockchain provides improvements in product security. The smart electronic locks introduced in Section 4 prevent unauthorized access to goods and blockchain controls access to the lock. If the package is accessed by an unauthorized person with force, the RFID tag notifies the whole network of a damaged package and can inform the location of the package in case of theft.

Bayer AG is now implementing an innovation of their own for battling counterfeit drugs. The company has developed software called BayCoder[7] which works like a QR code, but randomizes the serial numbers on pharmaceutical packages so that only one in ten thousand possible serial numbers is real. This means that only one counterfeit product in then thousand will not be identified when comparing the serial number to the central database provided by Bayer. I still find problems in this solution. Although the serial number cannot virtually be faked anymore, BayCoder does not provide the benefits of RFID tags: tracking and being tamper-proof. The central database provided by Bayer also contradicts with blockchain principles. With the suggested blockchain and IoT

[7] Bayer (2016). Hard Times for Counterfeiters. *Bayer technology solutions Magazine, 1, 46-49*.

combination, Bayer can also raise the level of privacy in the supply chain, as explained in the next paragraph.

Cryptographic functions and combination of public and private keys enable transactions on blockchain to be verified without exposing the content of them, as explained in Section 2.1. In the pharmaceutical supply chain this provides transparency, privacy and security simultaneously. Trusted parties make transactions with one another, verify that the products were produced in trusted sources and transported by trusted stakeholders and still keep the content of a transaction private.

I see that in the suggested pharmaceutical supply chain stakeholders can, in practice, trade goods in two ways. The first way is using smart contracts as explained in the previous section. Smart contracts are available for every stakeholder if they can just deliver the terms of the contract. The second way is a more conventional one: direct trade with another party. I propose that the host of the network would keep the list of participants public and therefore stakeholders could communicate with each other. In case of a negotiated outcome, parties can just share their public keys so that transactions can be performed. Knowing other parties' public keys still does not expose their privacy and trade secrets. As described in Section 2.1, transaction messages are encrypted and digital signatures require both the private key and the message to be created. So by only knowing other party's public key one cannot make any conclusions on the blockchain.

6 BLOCKCHAIN INFRASTRUCTURE AND GOVERNANCE

Setting up the blockchain platform for the pharmaceutical supply chain is a task of a governmental body. In the EU, this would fall to European Medicines Agency, as discussed in Section 3. The platform will be a private blockchain, because it is controlled by a governmental body and access to the network is controlled. New value is generated on the blockchain via the host that exchanges fiat money to assets on the chain, as explained in Section 4. Thus, mining does not generate new value to the network.

The platform must enable smart contract usage similarly to Ethereum platform in order to facilitate trade, which was discussed in Section 4. The "rules" of the blockchain must be programmed during development – for example, authorization of new participants and collection of taxes. A functioning user interface, enabling all the functionalities discussed in this thesis, must also be developed. Furthermore, I believe that the user interface must

provide means for communication so that direct transactions between parties are easier to carry out. Blockchain networks are connected via Internet (Antonopoulos 2014) and the pharmaceutical supply chain network should be accessed with its own software that runs for example on computers, tablets and mobile devices.

According to Christidis and Devetsikiotis (2016), mining on a private blockchain is more efficient than on public ones, because fewer nodes participate in verifying transactions. Furthermore, they state that not all nodes need to mine and not all miners need to be involved in transactions. If only certain stakeholders would mine, consensus could be reached faster and therefore lighter algorithms for reaching consensus can be used (Christidis & Devetsikiotis, 2016). This would lead to shorter slack in adding new blocks to the chain and thus shorter transaction verification time. Another scenario with external miners would mean that the ledger is public, although not everyone is allowed to participate in transactions and smart contracts. This scenario would require an incentive (reward) for the external miners to provide their computational power. Furthermore, Christidis and Devetsikiotis (2016) state that if only the trusted transacting nodes of a network perform the mining, there is virtually no risk of the 51-percent attack, where one party can tamper the ledger.

Taking these arguments into account, I suggest that on the pharmaceutical supply chain platform no external miners should provide computational process work for verifying transactions. The consequences of a 51-percent attack would be too harmful considering that healthcare depends on continuous supply of medicines. When mining is limited to the participating nodes, either the host (governmental agency) or all approved nodes can perform the computational work. When mining is distributed between several locations, the risk of malfunctioning software and hardware is far lower. Thus, I propose that it is mandatory to provide computational processing work when entering the network.

Bayer AG should, consequently, provide computational power for mining in the network. As mining is very similar to maintaining a data center, the company needs to establish a new facility that can run thousands of computers inside. The Nordics are a suitable location for data centers, thanks to developed infrastructure, cool weather and access to green energy, and the market is growing strongly[8]. Bayer already runs a significant

[8] Smolaks, M. (2015, September 10). Nordic data center market expected to triple power by 2017. *DatacenterDynamics*.
Retrieved from: http://www.datacenterdynamics.com/content-tracks/design-build/nordic-data-center-market-expected-to-triple-power-by-2017/94767.fullarticle

pharmaceutical production site in Turku, Finland (Bayer, 2016) and, in my opinion, could establish the new “mining center” in the same area.

An exception for the mandatory mining can, in my view, be allowed for individuals. For instance, patients that simply utilize the blockchain to verify the authenticity of their medicine with the help of a cell phone cannot provide much hardware to maintain the platform. The option is to have “lightweight clients” (Antonopoulos, 2014), which do not store the entire list of records on their hardware and thus do not participate in mining. They can just create an account that is then approved by the host, for example by verifying their identity and citizenship via bank account, and then connect to the network by downloading software. Lightweight clients can perform transactions and queries with the help of user interface and other nodes approve their actions.

7 CONCLUSION

In this thesis, I have studied what benefits blockchain technology can have on pharmaceutical supply chains and how it should be utilized in practice. I started the thesis with presenting the essential concepts of blockchain, smart contract and pharmaceutical supply chain. Then the benefits and implementation were discussed in the parts of participating entities and information flow, contracts and payments, logistics, transparency and product security, and also blockchain infrastructure and governance.

Blockchain technology provides a platform for transactions and contracts. The distributed database verifies transactions automatically, but still privacy and trade secrets are safe. No central intermediary is needed to perform transactions on the blockchain. One cannot tamper the ledger and transactions are secured via strong encryption. Blockchain technology disrupts trust, because users do not have to put trust on a third party intermediary and other users are automatically verified by the network. Smart contracts provide a way of automatically negotiating and executing contracts and the payments connected to them on the blockchain.

Pharmaceutical supply chain should implement a private blockchain that is developed and controlled by a governmental organization that supervises medicines already. This host then verifies stakeholders willing to join the network. These stakeholders include, for example, production facilities, transporters, wholesalers and end users. Stakeholders are responsible for processing transactions (mining), but individual end users can join as lightweight users that do not provide computational power for the network. Transactions

on the blockchain are based on exchanging assets that represent real property or value in the physical world. The host of the network exchanges fiat money to assets on the blockchain and this way the network can trade with existing currencies. The host also provides an oracle service that connects the blockchain to external information, which widens the scale of possibilities of smart contract applications.

Products moving in the pharmaceutical supply chain are attached with an RFID tag and in some cases additional Internet-of-Things (IoT) devices in order to keep track of their whereabouts and to collect data. These devices also contribute to product security, as they can provide smart locks and inform if a package was opened violently without permission. The combination of smart contracts and IoT devices automates trade and even enables machine-to-machine transactions. The platform can also automate taxations and accounting within the blockchain.

As a bachelor's thesis the scope of this thesis was narrowed to only exploring benefits and potential implementation of blockchain network for the pharmaceutical supply chain. Further research could and should be done in testing the suggestions of this thesis in practice. In my view, this work could be started by studying potential stakeholder's capability of joining the blockchain network in the first place. In more detail, this would mean studying, for example, stakeholder's capability to provide computational power, providing smart contract based insurance, the host's ability to maintain a trusted oracle and a study case of end user's expectations of software functionalities. Another research field is to compare the benefits and implementation between different industries or, more specifically, between different supply chains.

In general, studying potential applications of blockchain technology still requires an enormous amount of work and I am eager to follow the results of future research.

8 REFERENCES

Antonopoulos, A. M. (2014). *Mastering Bitcoin*. O'Reilly Media Inc.

Asif, Z. and Mandviwalla, M. (2005). Integrating the supply chain with RFID: A technical and business analysis. *Communications of the Association for Information Systems*, 15(24), 393-426.

Bayer AG (2016). *Bayer annual report 2015.* Retrieved from: http://www.annualreport2015.bayer.com/

Chircu, A., Sultanow, E., and Saraswat, S. P. (2014). Healthcare RFID in Germany: An integrated pharmaceutical supply chain perspective. *Journal of Applied Business Research*, 30(3), 737-752.

Christidis, K. and Devetsikiotis M. (2016). Blockchains and Smart Contracts for the Internet of Things. *IEEE Access*, Vol. 4, 2292-2303.

Decker, C. and Wattenhofer, R. (2013). Information Propagation in the Bitcoin Network. *Peer-to-Peer Computing (P2P), 2013 IEEE Thirteenth International Conference on*, 1-10.

European Medicines Agency (2016). About us [Document]. Retrieved from: http://www.ema.europa.eu/docs/en_GB/document_library/Other/2016/08/WC500211862.pdf. Accessed on November 8th 2016.

Helpman, E. and Trajtenberg M. (1994). A Time to Sow and a Time to Reap: Growth Based on General Purpose Technologies. *NBER Working Paper*, 4854.

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Retreived from: https://bitcoin.org/bitcoin.pdf.

Oraclize (2016). Overview. Retrieved from: http://docs.oraclize.it/. Accessed on November 17th 2016.

Papert, M., Rimpler, P. & Pflaum, A. (2016). Enhancing supply chain visibility in a pharmaceutical supply chain. *International Journal of Physical Distribution & Logistics Management*, 46(9), 859-554.

Selgin, G. and White, L. H. (1999). A fiscal theory of government's role in money. *Economic Enquiry*, 37(1), 154-165.

Shah, N. (2004). Pharmaceutical supply chains: Key Issues and Strategies for Optimisation. *Computers & Chemical Engineering*, Vol. 28, 929-941.

Swan M. (2015). *Blockchain: Blueprint for a New Economy*. O'Reilly Media Inc.

Szabo, N. (1994). Smart Contracts [Article]. Retrieved from: http://szabo.best.vwh.net/smart.contracts.html. Accessed on October 25th 2016.

Yli-Huumo, J., Ko, D., Choi, S., Park, S., and Smolander, K. (2016). Where is current research on blockchain technology? – A systematic review. *PLoS One*, 11(10).

Walport, M. (2016). Distributed Ledger Technology: beyond block chain [Government report]. Retrieved from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf. Accessed on November 16th 2016.

9 APPENDIX

List of terms and explanations in blockchain technology

51-percent attack	Having more than half of the entire network's computational power to create fraudulent transactions to double-spend money (see double-spending below). The only way to double-spend on a blockchain.

Cryptographic hashing	Transforming data to a fixed size of bits through a mathematical algorithm. Makes the message in question unreadable.
Double-spending problem	Successfully spending exact same money more than once. Blockchain tackles this problem by requiring mining to verify transactions (see below).
Fork	Alternative chain that has partly different blocks included. A part of the network considers the fork correct. Eventually forks will disappear automatically.
Mining	Process of adding transaction blocks to the chain. Performed by solving a cryptographic function by guessing the correct answer. Mining requires an enormous amount of computational processing work.
Oracle	A server outside the blockchain that transmits information for smart contracts.
Private blockchain	Blockchain network with limited and regulated access to it.
Private key	Every account has a code (private key) that the owner uses to verify their own transactions. Comparable to password.
Proof-of-work	The result of successful mining. The solution to the aforementioned cryptographic function.
Public blockchain	Blockchain network that everyone can participate in.
Public key	Number that presents account address in the network. Comparable to email address or bank account number.