University of Zurich[UZH]

Burkhard Stiller,
Sina Rafati,
Eder John Scheid,
Bruno Rodrigues,
Corinna Schmitt (Eds.)

Communication Systems XI

TECHNICAL REPORT – No. IFI-2018.04

June 2018

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

ifi

B. Stiller et al. (Eds.): Communication Systems XI
Technical Report No. IFI-2018.04, June 2018
Communication Systems Group (CSG)
Department of Informatics (IFI)
University of Zurich
Binzmühlestrasse 14, CH-8050 Zürich, Switzerland
URL: http://www.csg.uzh.ch/

Introduction

The Department of Informatics (IFI) of the University of Zurich, Switzerland works on research and teaching in the area of computer networks and communication systems. Communication systems include a wide range of topics and drive many research and development activities. Therefore, during the spring term FS 2018 a new instance of the Communication Systems seminar has been prepared and students as well as supervisors worked on this topic.
The areas of communication systems include among others wired and wireless network technologies, various network protocols, network management, Quality-of-Service (QoS) provisioning, mobility, security aspects, peer-to-peer systems, multimedia communication, and manifold applications, determining important parts of future networks. Therefore, this year's seminar addressed such areas in more depth. The understanding and clear identification of problems in technical and organizational terms have been prepared and challenges as well as weaknesses of existing approaches have been addressed. All talks in this seminar provide a systematic approach to judge dedicated pieces of systems or proposals and their suitability.

Content

This new edition of the seminar entitled "Communication Systems XI" discusses a number of selected topics in the area of computer networks and communication systems.
The first talk on " SLAs and Smart Contracts: A Feasibility Study" explains the potential of replacing traditional SLA contracts with blockchains.
Talk 2 "Network Neutrality Laws: The Swiss Case Study" evaluates the current Internet-usage related regulations and user/producer expectations and rights.
Talk 3 "Requirements and Challenges for Blockchain Governance" focuses on the governance applications could be possible with blockchains and its various aspects.
Talk 5 "Advanced Message Queuing Protocol as a Communication Protocol Standard for IoT" explains the message queuing protocol with elaboration on different layers of implemented protocol to be used as a Communication protocol standard.
Talk 6 " Introduction to IoT Use Cases With an Evaluation of Integration Possibilities with Blockchains" introduces the challenges of the Internet of Things solutions and evaluates the possibility of addressing those challenges with current blockchain systems.
Talk 7 "An Overview of Emerging Wireless Communication Systems in 5G" introduces some of the newest technologies and products used in the fifth generation of wireless communications.

Talk 8 “Overview and Use Cases of Blockchain Interoperability” evaluates the proposed systems which are based on integrated blockchain regarding the potential advantages and disadvantages.
At the end, the Talk 9 “Commonalities of Network Function Virtualization, Blockchains, and Smart Contracts” specifies the possibilities of leveraging blockchain based systems and network function virtualization.

Seminar Operation

Based on well-developed experiences of former seminars, held in different academic environments, all interested students worked on an initially offered set of papers and book chapters. Those relate to the topic titles as presented in the Table of Content below. They prepared a written essay as a clearly focused presentation, an evaluation, and a summary of those topics. Each of these essays is included in this technical report as a separate section and allows for an overview on important areas of concern, technology architectures and functionality, sometimes business models in operation, and problems encountered.
In addition, every group of students prepared a slide presentation of approximately 45 minutes to present its findings and summaries to the audience of students attending the seminar and other interested students, research assistants, and professors. Following a general question and answer phase, a student-lead discussion debated open issues and critical statements with the audience.
Local IFI support for preparing talks, reports, and their preparation by students had been granted by Bruno Rodrigues, Corinna Schmitt, Eder John Scheid, Sina Rafati, and Burkhard Stiller. In particular, many thanks are addressed to Sina Rafati and Corinna Schmitt organizing the seminar and for her strong commitment on getting this technical report ready and quickly published. A larger number of pre-presentation discussions have provided valuable insights in the emerging and moving field of communication systems, both for all groups of students and supervisors. Many thanks to all people contributing to the success of this event, which has happened in a lively group of highly motivated and technically qualified students and people.

Zurich, June 2018

Contents

Chapter 1

Requirements and Challenges for Blockchain Governance

Lucas Pelloni, Erion Sula

In recent years, the Blockchain technology has slowly become one of the most discussed topics. While it is sure to say, that the Blockchain has played a fundamental role in revolutionizing the way of storing transactions, when applied to concepts like Governance and/or services offered by today's centralized institutions, there are some precautions that need to be taken into consideration. In this paper, an overview over the requirements and challenges of Blockchain-based Governance is provided. The concept of Governance will be first introduced, along with its characteristics. Additionally, an example of both centralized and decentralized organization will be analyzed under the Governance point of view and the main differences will be highlighted accordingly. Lastly, a real-world example of a decentralized, Blockchain-based Institution will be presented.

Contents

1.1 Introduction

In this paper, we will discuss the main Governance properties of both centralized and decentralized environments by focusing more on the decentralized one. The definition of Governance will be explained in the first section so that the reader can get an understanding of the main concept which will be applied and observed in some use cases. After that, some main characteristics of a good Governance will be given and used as an instrument for analyzing whether in a specific environment a good Governance is present. Successively, we will have a look in the Software Development Industry by taking an example of software development process and analyzing it with the help of the characteristics previously defined, in order to see how the Governance process is organized in such a centralized approach. Afterwards, we will briefly introduce the reader to the Blockchain Technology, thus making a clear distinction between two different types of it. After this small introduction, we will have an in-depth look at the Governance process of both the public and the private Blockchain, by discussing the main characteristics mentioned at the beginning. In addition to that, we will also have a look at a particular use case, namely at Science Matters by focusing on the Governance aspect.

1.2 Related Work

The definition as well as an overview of the main characteristics of a good Governance were provided and explained in detail by Yap Kioe Sheng [2] and also here [4, 5, 6]. More details regarding the example used for describing the centralized Governance (Scrum Governance) approach can be found here [12, 13, 18, 20, 21]. Consequently, a brief description of the Blockchain technology itself can be found in the work of Melanie Swan [3]. An overview of the main characteristics and challenges of Blockchain-based Governance are given by Justin Barbaro [32] and other writers [31, 33, 35, 38]. Finally, an in-depth description of the use case is presented here [40, 43].

1.3 Governance

1.3.1 Definition of Governance

In the literature, there are several definitions of Governance, but in general, Governance can be described as *"The process of decision-making and the process by which decisions are implemented(or not implemented)."* [2]. This definition implies that in this complex process there are entities, that need to be involved in it, like for example a government or other similar institutions. These entities, also known as governing bodies, are essential for establishing laws in a given organization [4].
Due to its general definition, the concept of Governance can be found in different environments, from smaller organizations like families (*Family Governance*), companies (*Corporate Governance*) to larger ones, like for example entire nations (*Nation Governance*). In this work, we are mainly going to analyse the implementation of Governance in both centralized and decentralized organizations.

1.3.2 Main characteristics of a trustworthy Governance

In order to be accepted by its participating member, a Governance has to fulfill 7 main criteria. These indicators are essential as they can determine if a governance can actually persist over time or not. In the first place, a Governance should guarantee participation for both men and women. **Participation** also means gender equality, because every actor

that is actively involved in this decision-making process should have the same rights and opportunities to be able to express his own opinion independently of their gender. In a democracy, for example, participation by the citizens plays a fundamental role. Besides being informed about everything related to public issues, the citizen is also required to actively participate by voting in elections. They have also the right to protest if a decision that has been made does not take their needs into consideration [9].

A Good Governance should provide a stable legal Framework, i.e. law or other written down rules, that define whenever an action can be made or not. Such concept is called **Rule of Law**. It is through the law that the authorities of government can express their will and exercise their sovereignty. However, it is important to point out that every participant, that is directly or indirectly affected by the made decisions, must obey the law. This includes also the authorities themselves [7].

Transparency is also an important factor that has to be taken into consideration when talking about good Governance. A transparent Governance should allow people to have access to the information of decisions that have been made [8]. Another important characteristic of a stable Governance is **effectiveness** and efficiency, that is the Governance should ensure that, by making efficient use of the resources that are available, the result produced should meet the needs and the expectations of the whole society [2, 6, 5].
Accountability is another core-characteristic of a Good Governance. For every decision that has been made, there should be at least one person that should take responsibilities for the consequences. In the example of a democracy, after government officials are elected, they are responsible for their decisions and action. According to Simon Lowe [14], the principle of Accountability is "more than meeting regulatory requirements or explaining how things went wrong, it is about holding others to account and being accountable to others".

Responsiveness is also another important aspect of a Good Governance, that will be used later to analyze the Scrum Governance. In fact, a Good Governance requires that organizations and their processes are designed to serve the interests and needs of stakeholders within a reasonable period of time and a decision should only be made after a thorough screening of all implications and possible alternatives [2, 15]. It's also important to point out, that most companies nowadays are composed of individuals that have different viewpoints and perspectives regarding common issues. In this case, an optimal reaction of a Governance would be helping the institutions to find a common ground and to achieve as broad consensus on an issue as possible, by identifying best suitable solution and how it can be achieved. A Good Governance should be therefore **Consensus-Oriented** [2].

1.3.3 Governance implementation in the Software Development Industry

In the following section, we will have a look at the Governance process in the Software Development industry. Nowadays Software Development companies are confronted with complex and demanding tasks, which require a stable Governance. In the next sections, we will use the main characteristics to analyze the governance in a centralized environment, like Scrum. We will also focus on the main authorities that are responsible for taking important decisions and making sure that the whole process runs smoothly.

1.3.3.1 Scrum

Scrum is an iterative and incremental Software Development Process. Scrum structures the software development in **Sprints**, i.e. iterations of fixed duration(1 to 4 weeks) where

the features of the product are implemented. The Scrum Process does not define the techniques that are used in the implementation of a software itself, but it concentrates more on how flexibility and productivity can be reached in the organisation [12]. There are three core roles in the Scrum methodology, as shown in Figure 1.1: Product Owner, Scrum Team and the Scrum Master.

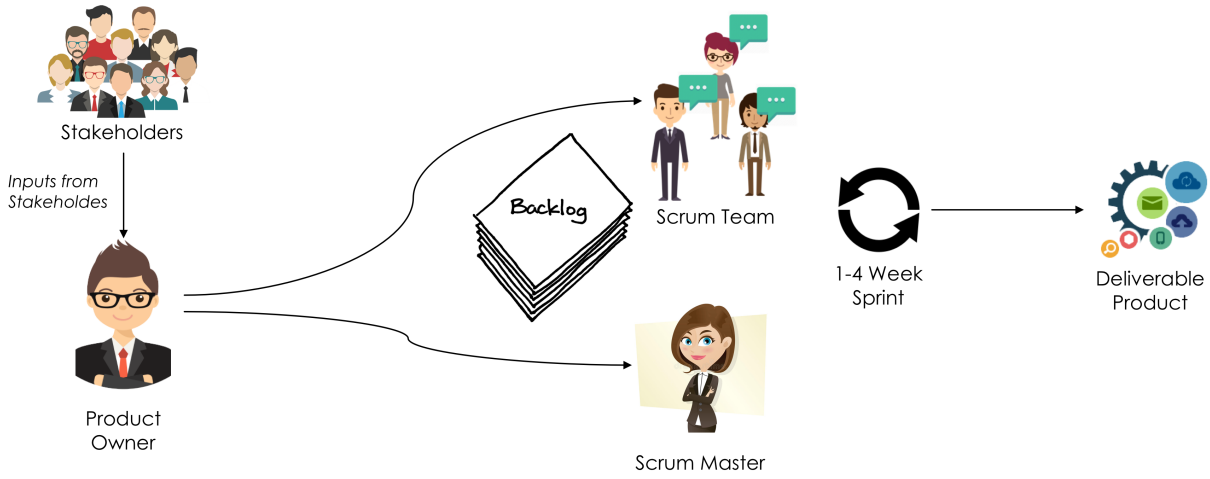


Figure 1.1: Scrum Roles

Product Owner : The Product Owner is responsible for gathering inputs from the Stakeholders and defining the Product Backlog, a document where the product requirements and goals are listed. The Product Owner also manages and controls the entire project, participates actively in estimating the development effort for Backlog Tasks and turns the issues in the Backlog into features to be implemented [12, 17]. The Product Owner can be understood as a customer representative or a customer proxy.

Scrum Team : The Scrum Team, normally composed of three to nine members, is in charge of taking important decisions in order to organize itself and to make sure that the goals of each Sprint are reached. The team has to ensure that at the end of each iteration a potentially shippable product is delivered [12, 13, 17].

Scrum Master : The Scrum Master is responsible for coaching the Scrum Team and more importantly helps the Scrum Team to reach consensus. In addition to that, the Scrum Master also ensures that the Scrum framework is followed and also promotes self-organization within the team [12, 13, 17].

With the help of the characteristics we mentioned before, we will now discuss the Governance process of Scrum. As shown in Figure 1.2, the Scrum process is characterized by four different types of meetings which potentially offer a certain degree of participation inside and outside the process. Before each Sprint, the *Sprint Planning Meeting* is held. This event is typically organized by the Scrum Master and involves several actors such as the Management, Product Owner, Scrum team and other Stakeholders(costumer, user). This meeting session consists of two phases. In the first part of the meeting, the Product Owner presents the highest priority features, accurately selected from the Product Backlog to the Scrum Team. The Team then actively participates by asking questions and reviewing the proposed items. The main goal for the team here is to gain enough understanding of which tasks can/should actually be implemented in the next Sprint [19, 20].

The most important output of the first phase is the *Sprint Backlog*, a list of prioritized Product Backlog items that serve as a starting point for the upcoming Sprint session. The

second phase of the meeting is held by the Scrum Master and the Scrum Team. In the final stage of the meeting, both the Scrum Master and the Scrum Team focus on how the product increment is implemented during the Sprint [18]. During each day of the Sprint, *Daily Scrum Meetings* take place. This 15 minutes daily events are another opportunity for the Scrum Team and the Scrum Master to interact with each other but most importantly to keep track of the progress of the Sprint itself. According to Outi Salo et al., the Daily Scrum Meetings actually help to identify impediments in the systems development process and should also help to remove these, leading to improvements in the process. The goal here is to get a global overview of the project and more specifically adjust the work plan [18, 20].

At the end of each Sprint, the *Sprint Review Meeting* is held. In this particular session, the Scrum Team and the Scrum Master present the potentially shippable product to the costumer, user and other stakeholders who are interested to attend the meeting. The Product Owner together with the Scrum Team and stakeholders define the goal of the next Sprint, by discussing and prioritizing the remaining features in the Product Backlog [21, 18, 20].

The *Sprint Retrospective Meeting* is usually the last thing done in a Sprint. According to Richard Cheng, one of the main keys that leads to a successful Scrum process is integrating feedback into process as early and as often as possible and he also argues that the Sprint Retrospective is one of the best methods for integrating the feedback to the process and also for giving the Scrum Team the opportunity to improve. This meeting will usually last 1 hour and it involves the Scrum Team, Scrum Master and the Product Owner. During the retrospective, the team identifies and reflect elements of their process that did or did not work as planned during the Sprint, along with potential solutions. The Experience of the Scrum Master may, in this case, facilitate the retrospective since there are many different ways of identifying issues and the Scrum Master responsible for designing each retrospective to address the needs of the Scrum Team at any moment in time [23].
There are different approaches in conducting a Sprint Retrospective Meeting and these they vary depending on the company. One of them is the *start-stop-continue meeting*. Using this approach, each participant is in charge of identifying specific things that the Scrum Team should: Stop doing, Start doing or Continue doing. In this case, the Scrum Master facilitates this meeting by asking the participants to bring their own ideas and they are asked to identify possible things that should stop, start or even continue doing. Successively, a list of ideas is defined and the Scrum Team will commonly vote on specific items in this list and will eventually focus on them during the next Sprint. At the end of the next Sprint, the next Sprint Retrospective Meeting is usually opened by reviewing the list of items previously selected by the Scrum Team. This is a very simple approach but has been proven to be very effective in practice [22].

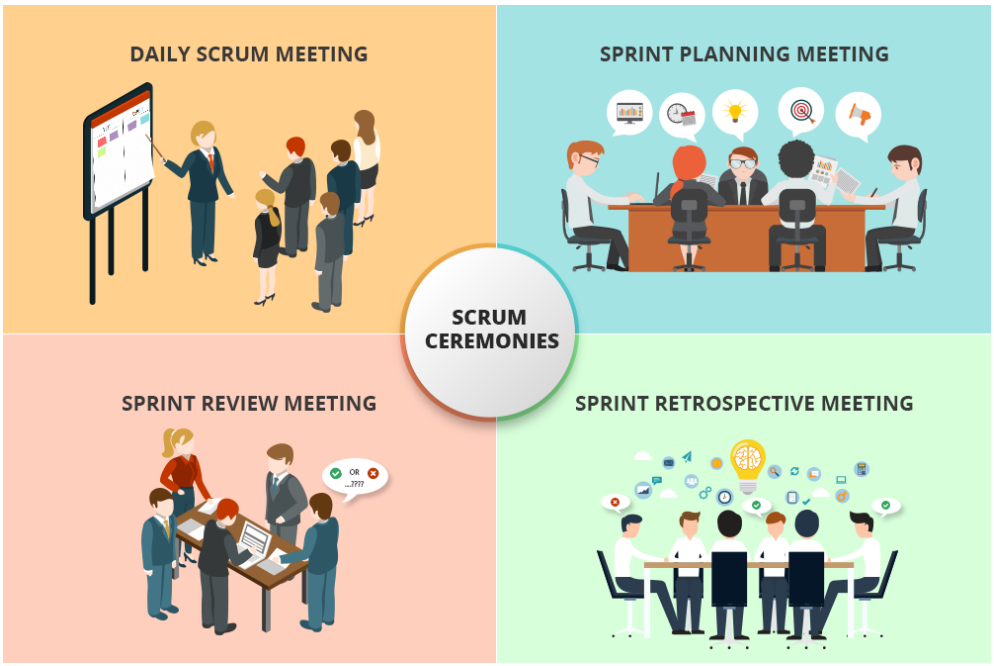


Figure 1.2: Scrum Meetings [16]

Scrum is a framework that also promotes transparency. Allowing any participant to see and understand what is actually happening behind each iteration is what makes the Scrum process transparent. It is therefore important to share information with everyone actively involved in the process and assuring that there is no hidden work being done. One example of transparency is the moment when the Product Owner defines the Product Backlog. By using it, the Scrum Team is able to see and predict future tasks for the upcoming Sprints. Transparency is also present during Sprints, that is with the help of the Scrum Task Board. The Scrum Task Board, or also called Scrum Board, is a physical board where all the tasks previously defined in the Sprint Backlog are listed and allows anyone to see for each planned task its actual state. In order to remain clear and readable to everyone, the Scrum Board should be kept as simple as possible [24].

"Scrum keeps everything about a project visible to everyone."
(Ken Schwaber [21])

In the Software Industry being flexible and responsive in every aspect is essential. That's one major reason why an increasing number of companies today are continuously adopting *Agile Methodologies*. The Scrum process is one of the most known frameworks of the Agile Methodology(other frameworks: Kanban, Hybrid, Binomial, Lean and XP [25]). The Agile Methodologies are software development approaches that are considered to be both people-focused and communication-oriented (as discussed before with the different Scrum ceremonies [Figure 1.2]). Their governance is so well organized, that it allows a high degree of flexibility, effectiveness and responsiveness. According to Altexsoft, Agile Methodologies allow for delivering cutting-edge products and cultivating innovative experiences while keeping the product in sync with the market trends and user requirements [25].

The main idea behind Scrum is that nowadays systems development involves several environmental and technical variables, such as requirements, resources, and technology, that are likely to change during the process. This could possibly lead to an unpredictable and complex software development process, which will eventually require the flexibility of the systems development process in order for it to be able to respond to those changes [12]. Due to its organization in Sprints and to the different number of meetings, Scrum

is considered to be flexible and responsive, since it reacts appropriately to expected and unexpected changes while taking into consideration that the requirements of the stakeholder might change over time.

The last characteristics that we are going to analyze are effectiveness. As already mentioned, effectiveness means producing a result at the end. In practice, the Scrum process is effective since at the end of each Sprint a potentially deliverable product is reached, but despite being effective, the process is considered to be inefficient. Viktor Grgic argues that the causes for the inefficiency might be: decision making by the whole team but in specific the high number of meetings, that in the majority of cases could lead to a waste of resources like time [26]. That's what usually companies take into consideration when adopting an Agile Methodology like Scrum. Most companies nowadays tend to significantly reduce the frequency and duration of meetings, in particular, the Daily Scrum Meeting, that instead of being held at each day of the Sprint, it only takes place every 2-3 days. As shown in Figure 1.3 the main characteristics of a Good Governance are also present in a centralized environment like Scrum.

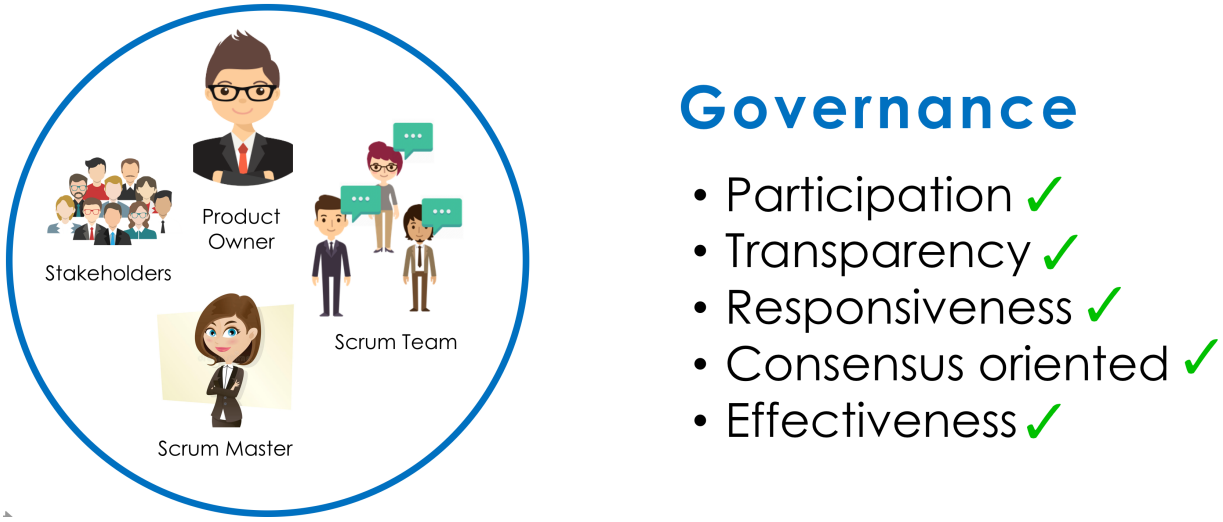


Figure 1.3: Scrum Governance

1.4 Blockchain Technology

A Blockchain is a constantly growing and distributed ledger, which keeps track of every transaction that has been executed, storing them in so-called *blocks*. The goal of this revolutionary technology is to create a decentralized environment where third parties become unnecessary [10]. Each transaction in this distributed database is verified by consensus of a majority of the participants, so-called *miners* [11]. In the following sections, we will have a closer look at two different types of Blockchain, namely the public and the private Blockchain in regards to their Governance processes.

1.4.1 Public Blockchain

The *Public Blockchain* is defined as a permissionless Blockchain that anyone in the world can read, anyone in the world can send transactions to and also receive them. The most known example of public Blockchain is Bitcoin. Bitcoin is a very popular cryptocurrency, which uses the public Blockchain for storing transactions. Being a permissionless network, there are no authorities deciding who should partecipate and who should not, which means that anyone is free to join the network. Compared to a centralized network like Scrum

where the participation was only restricted to a limited number of actors, the public Blockchain offers a higher degree of participation by eliminating this restriction.
Public Blockchains are generally considered *fully decentralized* since there are no authorities with a specific role such as supervising the whole process or establishing important decisions/role that must be followed by the community. In the example of Bitcoin, after a user created a transaction, the transaction is then broadcasted to any node in the network. This implies that a transaction in order to be categorized as valid, it has to be processed by each node, also called miner, in the network. This process, also known as *Consensus Mechanism*, is a very important characteristic of the public Blockchain that differentiates it from any other centralized system.
In Scrum, for example, there was only a few people were responsible for reaching consensus on a particular issue, but in this case, the whole network of miners is responsible for reaching consensus and validating a transaction.
The validation process is done by cryptography, which means that a mathematical equation has to be solved. Nowadays. solving those equations has become really challenging since they are difficult and require a lot of computing power [27].
After a transaction is validated, it gets stored somewhere. All valid transactions are stored in the public distributed ledger and each node of the network holds a copy of it. All transactions are also open to the public, which means that anyone can access and read the data. Such level in transparency has not existed in financial systems before [31]. Even though there are no authorities making sure that the process runs as expected the public Blockchain can be considered responsive. The miner that managed to validate a transaction has to be rewarded somehow. After spending a lot of resources, a miner should be incentivized somehow in order for continuing doing its work. Such incentives are present in the Blockchain and they are called *miners reward*. The miner that first found the right hash is rewarded with a certain amount of, in the case of Bitcoin, Bitcoins.
Lastly, the public Blockchain Governance is also considered to be effective. In the case of Bitcoin, once a transaction is considered to be valid via the consensus process, the user immediately receives the transaction [1, 3, 28, 29, 30].
There are also some *challenges* regarding the Governance of the public Blockchain. In particular, there are two main challenges that need to be taken into consideration when adopting the Blockchain-based Governance:

Limited Scalability : As mentioned before, the decentralized consensus mechanism is a very important aspect that distinguishes the blockchain from any other centralized system. Other than current financial institutions like Visa or Paypal, in the case of Bitcoin after a transaction is broadcasted to the miners, they have to work at a single transaction at a time, leading to *low throughput* and consequently to *slow transaction times* (time required to process a block). As shown in figure 1.4, the fact that every miner in the network can not work on multiple transactions in parallel has a significant impact on the number of processed Transaction per Second (TPS) [33].

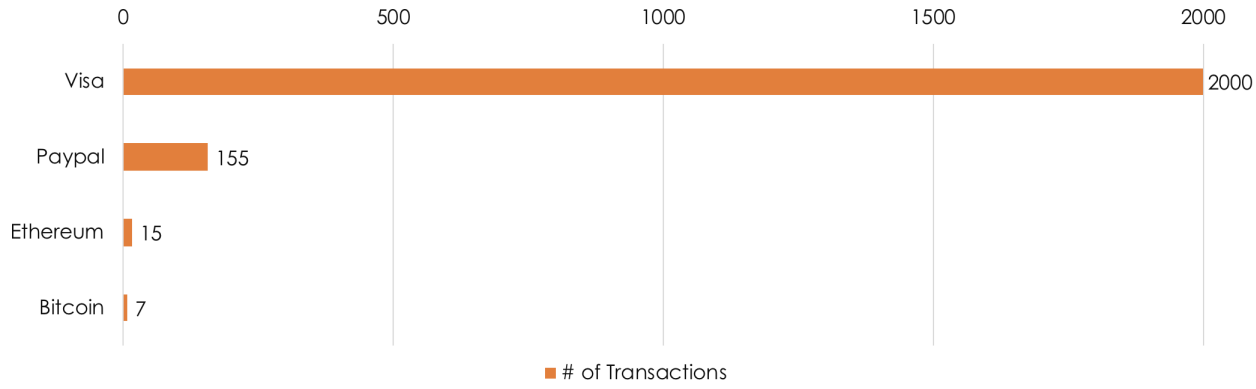


Figure 1.4: Processed Transaction per Second (TPS)

Generally, as the Blockchain grows in size, the requirements for storage, bandwidth, and compute power required for processing transactions also increase. At some point, it becomes unwieldy enough that only a few nodes are actually able to afford the required resources to process new blocks, thus leading to a risk of centralization. This means, that the power to decide which transaction should be processed first would only reside in a few number of miners. Those miners would with high probability prefer transactions with higher transaction fees first, leading to delays for smaller transactions [35, 36, 37, 38].

Privacy Leakage : The Privacy leakage is correlated to the characteristic of transparency in the public Blockchain Governance. The traditional Banking system achieves a level of privacy by limiting access to transactions information to the entities involved. In the public Blockchain, however, that's not the case. The Blockchain is believed to be very safe as users only make transactions with generated addresses rather than real identity. Having only a generated address attached to the transaction, the involved parties may seem impossible to track. However, since every transaction is accessible and visible to anyone (transparency), the risk of deanonymization is high [32, 37, 38].
There are many examples of deanonymization in the field of public Blockchain. One known example goes back to 2015, where a former federal agent was able to trace hundreds of thousands of Bitcoins from the personal computer of Ross Ulbricht, a 30-year-old accused for running an anonymous marketplace named Silk Road. Due to the transactions being visible to the government and other federal institutions, after a long investigation, they were able to make a link between the generated address and the real identity of the user, in this case Ross Ulbricht. Although the main goal of Bitcoin is providing privacy to their users, the former federal agent Ilhwan Yum claims that the cryptocurrency is by no means untraceable or anonymous by default [34, 38].
These two major challenges are the main reason why most companies nowadays do not see the public Blockchain as an option.

1.4.2 Private Blockchain

Unlike public Blockchains, private Blockchains are permissioned networks. Indeed, those networks presuppose the existence of a central authority (e.g. an organization with few individuals), that controls and places restrictions on who is allowed to join it. This implies, that *read-write* permissions on those particular Blockchains are not fairly distributed among each peer in the world, but are strongly defined by the network starter. In fact, the latter determines the access control mechanism of that specific network.

The most known example of private Blockchain is Ripple [39]. Ripple is a enterprise (semi-permissioned) Blockchain solution for global payments. It is especially designed for Banks (or any other payment provider) for cross-border payments in real time with end-to-end tracking. As the definition of private Blockchain states, Ripple uses a protocol where it is the startup itself that determines who may act as transaction validator on that network. In the sense, the decision-making process implemented by Ripple goes through the supervision of a single central entity and it is not fully consensus-oriented and community-driven as for the case of public Blockchains.
In relation to the *main characteristics of a trustworthy Governance* presented in the section 2, Ripple and any other type of private Blockchain causes limited **participation** and **transparency** for all peers in the world. This is because, as mentioned above, not every peer can *participate* and for example trigger a transaction within that network. At the same time, transactions that have been executed and in a second step validated in that Blockchain are not visible for everyone. Thus, *transparency* can only be guaranteed for those members that already received the permission from the regulatory authority to join the network. This is the reason behind the term *limited*. Just permissioned peers can participate and are able to read and see all blocks that have been inserted in that specific private distributed ledger. Regarding the Governance characteristic **Effectiveness**, private Blockchains do not fully satisfy this requirement. This is because, the Governance model provided by them, do not ensure that the resources that are used aim at meet the needs and the expectations of the **whole** society. Indeed, they are just limited for the permissioned members within that network. With the assumption that private Blockchains may have a lot of permissioned peers operating in the network, we can state that they are privately **Consensus-Oriented**. This means, that each member with access to network is able to participate in the process of verifying transactions. For example, if the validator entities are members of a consortium and thus the consensus process is controlled by a pre-selected set of nodes, the majority of them must sign every block in order for the block to be valid [41].

1.5 Science Matters

In order to highlight the main Governance aspects and put them in a relation with a real use case, we have chosen to present ScienceMatters [40]. In this sense, ScienceMatters will shift in the next months its core business from a centralized environment to a decentralized and distributed ecosystem. Concerning ScienceMatters' Governance aspects, this will have a lot of implications. In the next section we will describe how the current platform works and how the current Governance model is structured. Afterwards, we will introduce the future decentralized application and explain the impact that it will have on all Governance-related factors.

Figure 1.5: ScienceMatters, the open-access digital publishing platform

1.5.1 What is ScienceMatters?

Typically, the publication process of an article starts with a research that submits his/her article to be peer-reviewed and in a second step be published in a journal. Nowadays, the current publication model has several well-known issues affecting the research community. Indeed, the research publishing industry is dominated by a very small number of publishers that charge high fees to authors for publishing their work [42]. Since there are just a limited

number of reputable publishers, the process of peer-reviewing can last months (in some cases even years) and authors do not have the warranty that their discoveries at the end of this process will be published. Science Matters is a Swiss-based company that tries to fill this lack of efficiency. It offers a open-access digital publishing platform for the entire scholarly publishing process. This process includes different phases such as authoring, submitting, reviewing, editing and publishing and it is all in one unified workflow.
In this sense, ScienceMatters enables scientists to rapidly publish their results by accepting single observations, trying to remove the barriers imposed by Journals by democratizing the science publishing process.

1.5.2 Governance model of the current Academic Publishing process

As mentioned before, the current publishing industry is dominated by a small number of publishers. The following picture illustrates how the current academia scientific publishing process works.

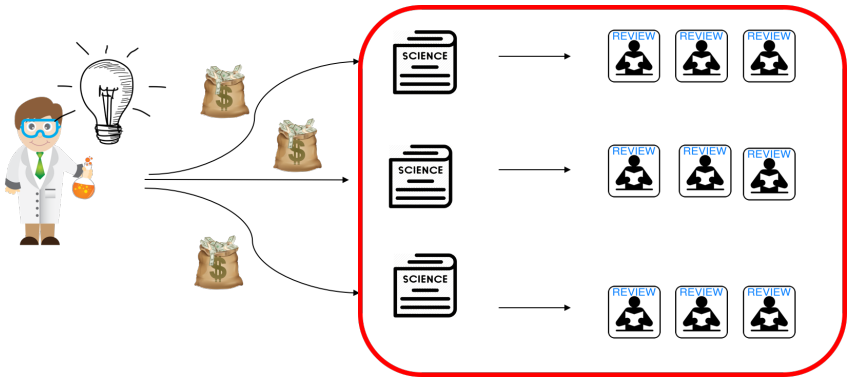


Figure 1.6: The current Academic Publishing process

Let's consider a scientist that makes a discovery and would like to share it with the entire world. He usually goes to a journal with the purpose of publishing it. Normally, it takes just few months to format the paper which describes the discovery, so that it fits the guidelines and standards provided by the Journal. Once the manuscript is properly formatted, the editor of that Journal analyses the submitted article and **decides** if it could be attractive for the Journal or not. In this sense, the decision-making process behind the publication of a particular manuscript, is concentrated in few Journal-related people's hands.
Let's suppose that the submitted article is well-formatted, in a second step it is sent to a set of reviewers that are in charge of peer-reviewing it and judge its technical and novelty quality. This step can be viewed as a peer-to-peer transaction, since the science gets transmitted from a scientist who made the discovery, to a peer-reviewer who judges the quality of the submitted article. As mentioned in the paragraph before, the process of peer-reviewing can take up few months, even years and at the end of it the Journal can actually reject the work. Let's suppose again, the peer-reviewing process is finished, the article has been approved by the editor and it is camera-ready for a particular Journal. Once a manuscript wants to be published, the Journal which wants to publish it ask for a very high publication fee. The cost to publish is on average around 5000 USD, based on the total annual revenue for scholarly publishers divided by the total number of articles published each year. Moreover, journals charge individual subscription fees of between 200 USD to 300 USD a year to access the published research [42].
In this sense, the Governance model applied in the academic publishing process can be

defined as *oligarchic*, since the power of publishing science rests with a small number of individuals. In relation to the *main characteristics of a good Governance* presented in the Section 2, we can consider the current model as **not transparent**, **not Consensus-Oriented** and **not efficient**. Indeed, a *transparent* Governance should allow people to have access to the information of decisions that have been made. This is not the case in the current science publishing process. Scientists, who submit their own research to a particular Journal do not exactly know the entity behind the editorial assessment process. Moreover, they do not know which set of reviewers is going to be assigned to the submitted manuscript. Since the process of peer review is fundamental to scientific research and publishing and it forms the basis for quality control of academic research, the non-transparency in the editor-reviewers decision-making process leads to large potential for professional, personal and social *Bias*. *Bias* is the behaviour when editors and reviewers know the identity of the authors, and as editors and reviewers are typically in the same field, they frequently know each other personally. This may lead the process of peer-review to be subject for example to conflict of interest between editors and reviewers.
The Governance model is also *not efficient*. After assembling research data to form a narrative, researchers submit it to a scientific journal, where most of the time the paper gets rejected or revisions are requested and the authors start the process of submitting to another journal all over again, making this process *inefficient*. Each journal can take few months (even years) to review a submitted paper. The publication rate varies amongst journals, but most renowned journals typically have very low publication acceptance rates (often less than 10%). Finally, the decision-making process behind science publishing is also *not community-driven and participative*. This is because, the number of people involved in the decision-making process for publishing science are a extremely small number compared to the number of people who provides the discoveries and the science.
In the next sections, we are going to present how ScienceMatters will try to fill this lack in the decision-making process. Firstly, without the application of Blockchain Technology. Afterwards, presenting a next-generation Blockchain-based platform, which changes the rules in the decision-making process for science publishing.

1.5.3 Governance Model of the current ScienceMatters platform

ScienceMatters' current platform consists of a next-generation science publishing platform for publishing, extending and replicating observations. The platform tries to fulfil the requirements for a *good Governance* that are not fulfilled with the current academic publishing process. Concerning the *efficiency* aspect, the platform enables scientists to rapidly publish their results by accepting single observations. Since, traditional publishers demand that only story-based studies be accepted for publication (often authors are unable to be fully objective with their own research and they may overestimate the validity of their findings in order to create a story), Matters and Matters Select[1] publish single, validated observations, thus highlighting the fundamental unit of scientific progress, *i.e.* the observation.
In relation to the *transparency* aspect, ScienceMatters' current platform still do not allow people involved in the publishing process of a single observation to have access to the information of decisions that have been made during the editorial assessment process. However, concerning the possibility to have personal, professional or social *Bias* in process of peer-review ScienceMatter's platform provides *Triple Bind Review*. This ensures an unbiased review process, since the identities of authors, editors and reviewers are unknown to one another.
Finally, the editorial assessment as well as the peer-review process are still not driven by

[1]The two Journals provided by ScienceMatters

the community and so they are not *Consensus-oriented*. The reviewers are still assigned by (handling)-editors and the decision-making process still rests centralized and in a few people's hands.
The following pictures provide an overview of the current plaftorm.

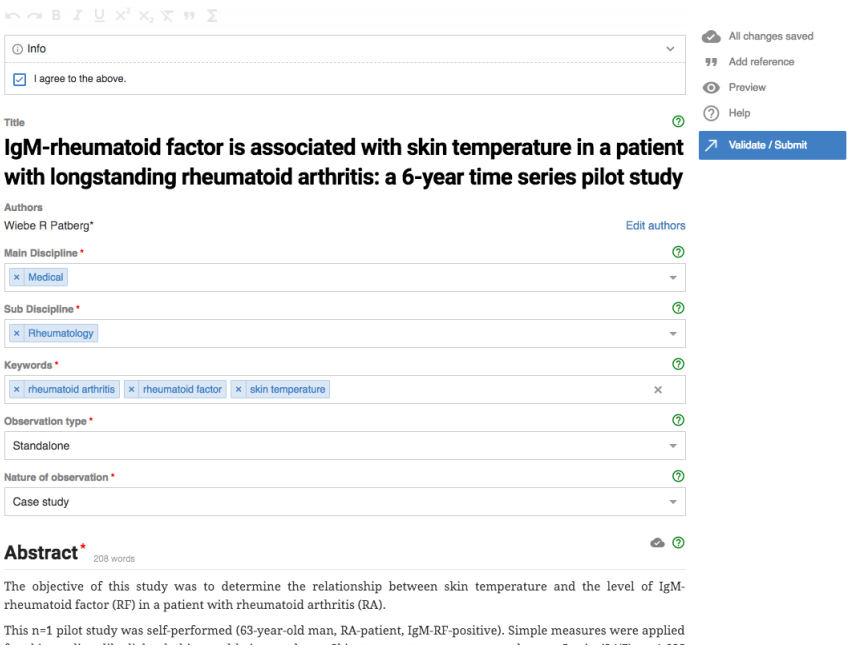


Figure 1.7: ScienceMatters next-genereation publishing platform: Browser-related authoring

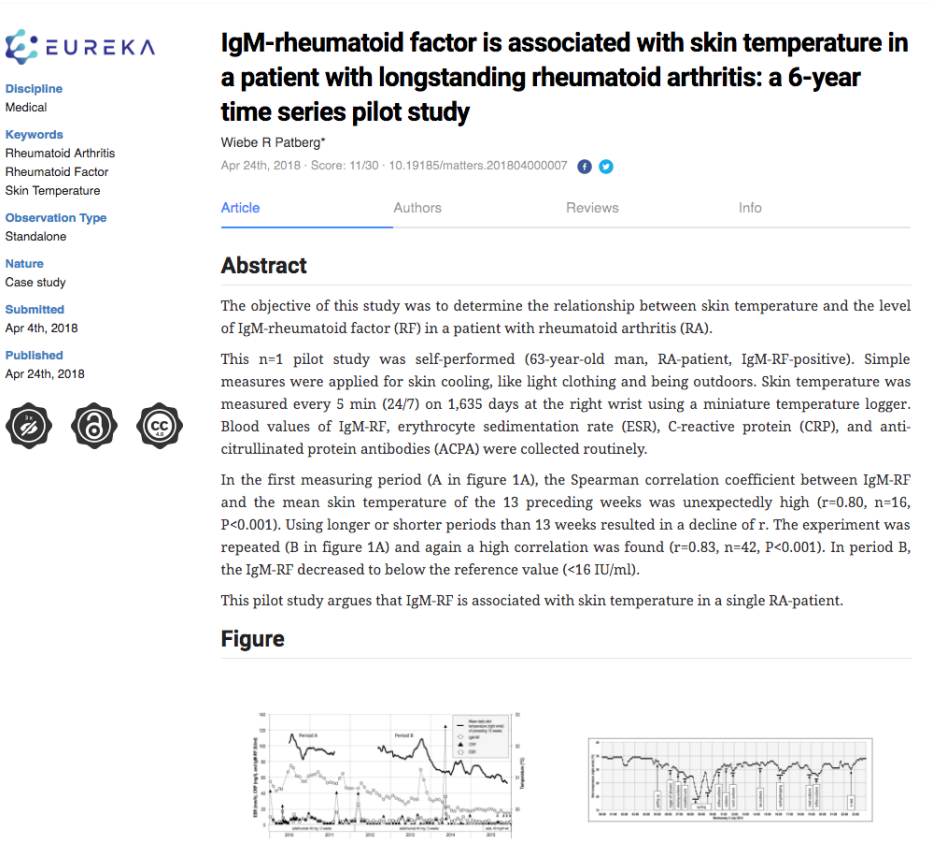


Figure 1.8: ScienceMatters next-genereation publishing platform: Matters

1.5.4 EUREKA, Blockchain-based Governance model

In the following Section, we are going to present **EUREKA** [43]. EUREKA is a scientific review and rating platform fuelled by the EUREKA token which has its core logic on the Ethereum blockchain [44]. It aims at changing the scientific publishing and reviewing process by making it more efficient and fair using the EUREKA token to compensate all parties involved.

Figure 1.9: EUREKA token

1.5.4.1 Decentralized decision-making process

The Governance model behind the Eureka platform is quite distinct to those presented in the sections *1.5.2 and 1.5.3*. We are going to explain with the help of the following illustration, by highlighting how Blockchain technology can radically change the decision-making process of an entire ecosystem. We are going to put the focus on the Governance aspect and how this Blockchain-based solution allows for new use-cases. However, the low-level technical elements will be not explained in a detailed way.

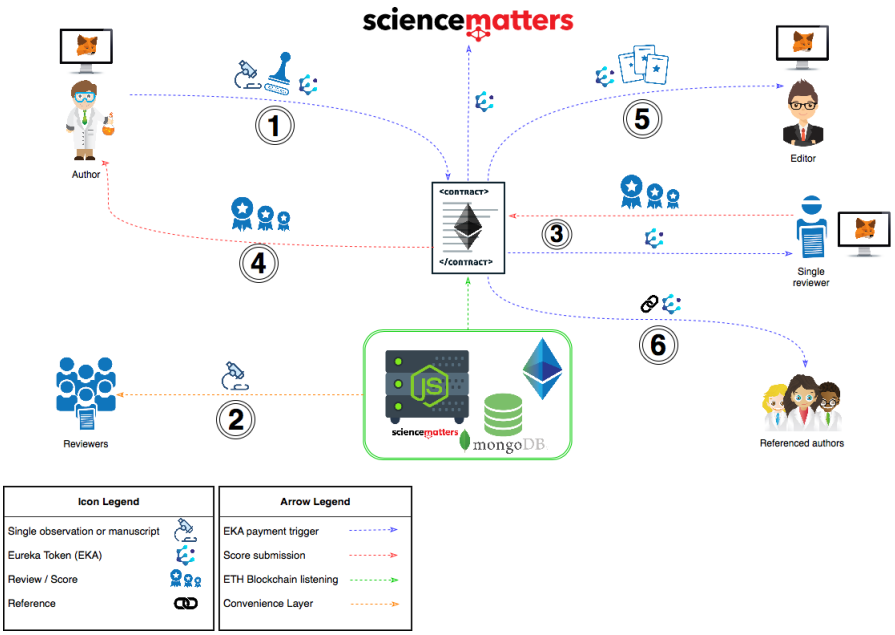


Figure 1.10: EUREKA - REWARD system

First of all, the initial scenario stays the same, *i.e.* a researcher wants to submit his/her manuscript in the Eureka platform (**step 1**). Afterwards, once an Ethereum node hosted by ScienceMatters servers triggers a new event in the smart contract (*i.e.* a new submission), it broadcast it to set of reviewers (**step 2**). The main difference between the Governance models presented in the sections *1.5.2* and *1.5.3* and this Blockchain-based Governance can be explained in this step.
In this Blockchain-based decision-making process the figure of the editor is still present, however non-editor approved reviewers can also be involved in the peer-review process. Thus, the regulatory authority of the Eureka platform is not more the editor of a Journal, but a Smart Contract. In this sense, each peer in the world could potentially become a reviewer just by calling a public function on the Smart Contract and it will not be any

more the editor of a Journal who decides the list of adequate reviewers. Thus, when a new individual wants to apply as a potential reviewer, others already established reviewers will be responsible to ensure his/her reliability and professionalism. In doing so, the network will create a self-regulatory ecosystem which is extremely **community-driven and Consensus-oriented**. Back to Figure 1.10, **step 3** represents the scenario when a reviewer submits his/her rating for a certain topic. Again, by calling a public function the Smart Contract. Once it is submitted, it is immutably recorded on the Blockchain and it is tamper-proof. With regards to the *good Governance characteristics*, EUREKA could also improve **transparency**. Since reviews as well as observations are public to everyone thanks to the power of Blockchain, authors could see also previous reviews of a reviewers. Thus, any potential social bias can become visible.
In **step 4** the author gets notified and can read his/her score from the Blockchain and once the peer-review process is terminated, the editor gets informed that a new article is ready to be approved (**step 5**). If the manuscript gets published, all referenced authors (for which an address was found in the Eureka platform) get rewarded with Eureka token (**step 6**).
In the current academic publishing industry, typically, both authors and reviewers currently get almost no direct compensation for the scholarly work that they perform in publishing and reviewing. The EUREKA Blockchain-based solution aims at improve the incentive mechanism and thus fairly compensate all parties involved in the Governance of publishing science. Since the EUREKA ecosystem is self-regulated and is driven by the community, all parties involved in the decision-making process need explicit incentives to stoke the token flow within the network. Thus, reviewers, editors as well as referenced authors will fairly be rewarded with Eureka tokens for their operations. The following list provides an overview of how the paid amount for submitting a manuscript or a single observation will be split among all parties:

- 28% for ScienceMatters,
- 25% for first-reviewers (i.e. reviewers who review a submitted manuscript or single observation),
- 2% for second-reviewers (i.e. authors, editors and a set of experienced reviewers who judge the quality of a review),
- 10% for handling editor. In case of a conference, an additional amount can be charged for organizing the conference if a minimal amount of successfully accepted papers until a certain deadline is reached,
- 15% for referenced authors,
- 20% will be locked (e.g. for one year) and if another researcher can invalidate the results within this year, this 20% will go to the other researcher. If no one invalidates, the amount is sent to the author.

1.6 Conclusion

The term Governance has definitely become a very iridescent and widely used concept in recent years. The Governance approach behind a centralized and oligarchic ecosystem (*i.e.* the current publishing industry) can not always ensure *transparency*, *efficiency* and *consensus-oriented* mechanisms. Furthermore, since the decision-making power rests in a few people's hands, this kind of Governance does not always imply full *partecipation* of all parties involved. Indeed, such Governance models are usually hierarchically structured

and consists of a entity of power at the top.
With the advent of Blockchain technology, hierarchical approaches to governance seem to become more and more obsolete. In fact, Blockchain technology has the power to improve *transparency* and to create self-regulated ecosystems, where decision-making processes are purely *community-driven* (**e.g.** EUREKA [43]). Furthermore, usually these ecosystems provide fairly rewarded incentive mechanism and thus they stimulate the *partecipation* of all members within that specific network.
In conclusion, we argue that Blockchain technology is a good and innovative way to change traditional hierarchically structured Governance models. However, since most of these Blockchain-based ecosystems are subject to network effects (*i.e.* new additional users who join the network increases the network's value), the process of changing will require a long time.

Bibliography

[1] Marcella Atzori: *Blockchain Technology and Decentralized Governance: Is the State Still Necessary?*, December 2015.

[2] Mr. Yap Kioe Sheng: *What is Good Governance?*, United Nations Economic and Social Commission for Asia and the Pacific.

[3] Melanie Swan: *Blockchain*, 2015.

[4] Wikipedia: *Governance*. `https://en.wikipedia.org/wiki/Governance` (Last accessed March 2018).

[5] Michael Jhon M., *What is Governance?*. `https://tamayaosbc.wordpress.com/2014/08/21/what-is-governance` (Last accessed March 2018).

[6] Thomas G. Weiss: *Governance, good governance and global governance: Conceptual and actual challenges*, Third World Quarterly, August 2010.

[7] Rule Of Law: *What is the Rule of Law?*, Institute of Australia. `https://www.ruleoflaw.org.au/what-is-the-rule-of-law/` (Last accessed March 2018).

[8] Alice Rubba: *Why transparency in governance is so important.* `http://www.rightforeducation.org/all-topics/law-governance/good-governance-transparency/` (Last accessed March 2018).

[9] *What is Democracy?*, Hilla University for Humanistic Studies. `http://web.stanford.edu/~ldiamond/iraq/WhaIsDemocracy012004.htm` (Last accessed March 2018).

[10] Jesse Yli-Huumo, Deokyoon Ko, Sujin Choi, Sooyong Park, Kari Smolander: *Where Is Current Research on Blockchain Technology? - A Systematic Review*, October 2016.

[11] Michael Crosby, Nachiappan, Pradan Pattanayak, Sanjeev Verma, Vignesh Kalyanaraman: *BlockChain Technology: Beyond Bitcoin*, Applied Innovation Review, June 2016.

[12] Pekka Abrahamsson, Outi Salo, Jussi Ronkainen and Juhani Warsta: *Agile Software Development Methods: Review and Analysis*, 2002.

[13] Wikipedia: *Scrum(software development).* `https://en.wikipedia.org/wiki/Scrum_(software_development)` (Last accessed April 2018).

[14] Simon Lowe: *Five principles of good governance - accountability*, December 2016.

[15] Governance Pro: *Eight Elements of Good Governance.* `http://www.governancepro.com/news/` (Last accessed April 2018).

[16] QuickScrum: *Scrum Ceremonies*. https://www.quickscrum.com/ScrumGuide/184/sg-Scrum-Ceremonies (Last accessed April 2018).

[17] Aaron Sanders: *Agile Team Members - Roles and Responsibilities*. https://thisagileguy.com/agile-team-members-roles-and-responsibilities/ (Last accessed April 2018).

[18] Pekka Abrahamsson, Outi Salo, Jussi Ronkainen and Juhani Warsta: *Agile Software Development Methods: Review and Analysis*, 2002.

[19] Mountain Goat Software: Sprint Planning Meeting. https://www.mountaingoatsoftware.com/agile/scrum/meetings/sprint-planning-meeting (Last accessed April 2018).

[20] Jeff Sutherland, Ken Schwaber: *The Scrum Papers: Nuts, Bolts, and Origins of an Agile Process*, 2007.

[21] Ken Schwaber: *Agile Project Management with Scrum*, February 2004.

[22] Mountain Goat Software: Sprint Retrospective. https://www.mountaingoatsoftware.com/agile/scrum/meetings/sprint-retrospective (Last accessed May 2018).

[23] Richard Cheng: What Is A Sprint Retrospective?. https://www.excella.com/insights/what-is-a-sprint-retrospective (Last accessed May 2018).

[24] David Cordeiro: *Transparency in Scrum*. http://www.mindsource.pt/en/content/transparency-scrum (Last accessed May 2018).

[25] Altexsoft: *Agile Project Management: Best Practices and Methodologies*. https://www.altexsoft.com/whitepapers/agile-project-management-best-practices-and-methodologies/ (Last accessed May 2018).

[26] Viktor Grgic: *Scrum is a very inefficient framework*. https://leanarch.eu/2013/01/31/scrum-is-a-very-inefficient-framework/ (Last accessed May 2018).

[27] Mark van Rijmenam: *https://www.linkedin.com/pulse/what-blockchain-why-so-important-mark-van-rijmenam/*. https://www.linkedin.com/pulse/what-blockchain-why-so-important-mark-van-rijmenam/ (Last accessed May 2018).

[28] Vitalik Buterin: *On Public and Private Blockchains*. https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/ (Last accessed May 2018).

[29] Febin John James: *3 Popular Types Of Blockchains You Need To Know*. https://hackernoon.com/3-popular-types-of-blockchains-you-need-to-know-7a5b98ee545a (Last accessed May 2018).

[30] steemit: *Do you know there are different types of Blockchain?*. https://steemit.com/blockchain/@geek4geek/do-you-know-there-are-different-types-of-blockchain (Last accessed May 2018).

[31] Lisk: *Blockchain Transparency Explained.* https://lisk.io/academy/blockchain-basics/benefits-of-blockchain/blockchain-transparency-explained (Last accessed May 2018).

[32] Justin Barbaro: *Five challenges facing Bitcoin and Blockchain Governance.* https://www.digitalcurrencycouncil.africa/five-challenges-facing-bitcoin-and-blockchain-governance/ (Last accessed May 2018).

[33] Globant: *Roadblocks of Blockchain.* https://stayrelevant.globant.com/en/roadblocks-of-blockchain/# (Last accessed May 2018).

[34] Andy Greenberg: *Prosecutors Trace $13.4M in Bitcoins From the Silk Road to Ulbricht's Laptop.* https://www.wired.com/2015/01/prosecutors-trace-13-4-million-bitcoins-silk-road-ulbrichts-laptop/ (Last accessed May 2018).

[35] Preethi Kasireddy: *Blockchains don't scale. Not today, at least. But there's hope.* https://hackernoon.com/blockchains-dont-scale-not-today-at-least-but-there-s-hope-2cb43946551a (Last accessed May 2018).

[36] Alejandro Reyes: *Bitcoin Scalability Solutions.* https://medium.com/michiganblockchain/bitcoin-scalability-solutions-f5686ffd2ba4 (Last accessed May 2018).

[37] Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, Huaimin Wang: *Blockchain Challenges and Opportunities: A Survey*, 2016.

[38] Preethi Kasireddy: *Fundamental challenges with public blockchains.* https://medium.com/@preethikasireddy/fundamental-challenges-with-public-blockchains-253c800e9428 (Last accessed May 2018).

[39] Ripple: *The world's only enterprise blockchain solution for global payments.* https://www.ripple.com/ (Last accessed April 2018).

[40] ScienceMatters: *The next-generation science publishing platform.* https://sciencematters.io/ (Last accessed April 2018).

[41] Blockchains and Distributed Ledger Technologies: *Blockchains & Distributed Ledger Technologies* https://tinyurl.com/yb5ujtbq (Last accessed April 2018).

[42] **Piwowar et. al.** The state of OA: *a large-scale analysis of the prevalence and impact of Open Access article* https://peerj.com/preprints/3119/ (Last accessed April 2018).

[43] Eureka token: *The next-generation open science platform powered by blockchain* https://eurekatoken.io/ (Last accessed April 2018).

[44] Ethereum: *Blockchain App Platform* https://www.ethereum.org/ (Last accessed April 2018).

Chapter 2

SLAs and Smart Contracts: A Feasibility Study

Kristin Schläpfer

The management of Service Level Agreements (SLAs) is expensive. However, technologies, such as blockchain and Smart Contracts, may help to reduce these costs. In this paper, we look into the possibility of implementing SLAs with blockchain-based smart contracts. The promising factors of such an implementation are mostly the trustworthiness of blockchains, the time reduction, and cost efficiency of automatic enforcement of compensation when agreements are not fulfilled, i.e., when an SLA violation is encountered.

Contents

2.1 Introduction

Service Level Agreements (SLAs) and smart contracts are tools for human interaction. They, generally speaking, act as a middleman for us to lower uncertainties and find out with whom it is safe and beneficial to interact. In the early stages, humans only interacted with people from their villages that they knew they could trust. Now when we interact with very much larger groups of people in our every day and our business life we can not have an overview over everybody's trustworthiness ourselves, so we need institutions to verify trustworthiness and keep track of possible interaction partners for us to reduce uncertainties. Institutions can be governments and banks and other social structures. Today institutions can however also be digital [9].
SLAs are agreements between a service provider and the parties receiving the service. SLAs comprise statements on both the quality and the quantity of the service as well as the compensations that must be enforced if the service properties are not matching the agreement. Smart contracts are computer programs that contain the content of a contract between parties. Smart contracts can define rules concerning the value exchange between the parties, rules on what compensations are needed if agreements are not fulfilled as well as automatic enforcement of the compensation [2].
In our work, we investigate if and how smart contracts could be used to support the trustworthiness of SLAs. In particular, we discuss the possibility of using smart contracts as support in different lifecycle stages of the SLA management.

2.2 Service Level Agreements (SLAs)

Service Level Agreements (SLAs) are documentations of agreements between the service provider and a customer. These agreements include the quality and the quantity of the service that the provider promises to deliver [5]. The description of these properties should be as detailed as possible so that it is possible to measure whether the agreement is being fulfilled or not. Beyond these descriptions of the service and its properties, an SLA also includes a description of how those properties can be ensured and what is the compensation method that must be enforced when one of the agreed properties is not fulfilled. Furthermore, it also includes exceptions from those compensation rules, which are usually external events such as natural disasters or terrorist attacks.
The service provider does not just provide an SLA or is demanded by the customer; it is formed through a negotiation between the involved parties. Examples of general service properties that can be documented are [11]:

- Availability
- Frequency
- Response Time
- Operation
- Quality/Performance
- Responsibilities
- Priorities of the party
- Tariffing and billing
- Service delivery

SLAs can be defined for different types of services. However, they are traditionally and most commonly used in network and IT-related fields. This paper focuses on Software as a Service (SaaS)-related SLAs. Typical service properties described in SaaS-related SLAs are:

- **Level of Service:** Level of Service can describe, among other properties, service availability, which is the duration that the service must be available to the client.
- **Quality of Service (QoS):** QoS is typically the bandwidth that the service provider wants to guarantee.
- **Capacity and capability of cloud service:** Capacity and capability of the service, for example, a cloud service, can include the maximum number of users that can access the cloud at one time and the potential ability of the provider to expand the service to more users.
- **Response time:** Response time defines the time that can be expected between placing a request and getting a response from the service provider, which is also called transaction processing time. Also, it defines the response time for responding to service outages.

2.2.1 SLA Management Process

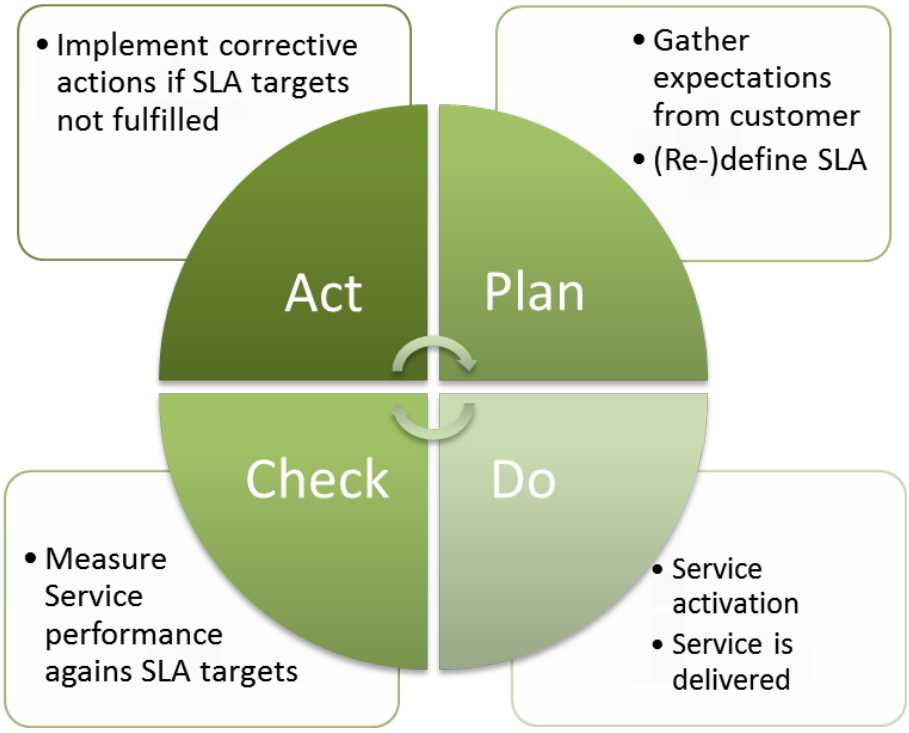


Figure 2.1: The SLA lifecycle [12]

There are four main stages in the management cycle of SLAs. The four stages are the negotiation, contract definition, monitoring, and enforcement[1]. Figure 2.1 depicts the SLA lifecycle in four main parts: act, plan, do and check. [12] on this lifecycle we map those management stages in each part. In the figure, contract negotiation and definition are comprised in the 'plan' part. The 'do' part does not contain any of the management stages mentioned because it relates to the management of the service itself, and not the management of the SLA. The service is delivered there which is the management of the service itself but not necessarily management of the service level agreement. During the delivery of the service, it is important to check if the service performs as agreed upon

during the 'plan' part. This is done in the 'check' part and comprises the monitoring management stage. Lastly, in the 'act' part of the SLA is enforced. As in any life cycle, the service level provider and the customer can learn from the last cycle and adjust their needs and offers.
More concretely: First the service provider and the customer(s) define the contents of the SLA together. The service provider's input is which services he/she can offer, and the customers' input is which service properties they need to be ensured to receive. During the monitoring phase, the service is monitored to detect any discrepancy between the service that is provided and the service that is agreed upon and described in the SLA. Finally, the enforcement stage is there to make sure the agreed upon compensations for violations of the SLA are paid [1].

2.2.2 Cloud Services SLA Examples

This section provides a description of two examples of SLAs from different cloud service providers: Amazon and Microsoft Azure.

2.2.2.1 Amazon Elastic Compute Cloud

The SLA for Amazon Elastic Compute Cloud promises an uptime of 99.99% which in case of failure is compensated with a service credit which is dollar credit. All the terms such as uptime and service credit, are described further in detail by Amazon to make sure that the service level agreement is clearly phrased and unambiguous. Exclusions from these rules are factors that go beyond their reasonable control, such as any force majeure events, problems related to Internet access or other problems that go beyond the responsibilities and capabilities of Amazon [13].

2.2.2.2 Microsoft Azure

Microsoft Azure has very similar SLAs to Amazon concerning uptime and compensation with service credits. To present an example of the level of detail that an SLA contains, one can refer to a quote from the main part of the Microsoft Azure SLA: "Maximum Available Minutes is the total accumulated minutes during a billing month for all roles that have two or more instances deployed in different Update Domains. Maximum Available Minutes is measured from when the Tenant has been deployed, and its associated roles have been started resultant from an action initiated by Customer to the time Customer has initiated an action that would result in stopping or deleting the Tenant" [14].

2.3 Smart Contracts

2.3.1 The general idea behind blockchain

A blockchain is a distributed database that stores all the different states a system passes through as well as the transactions that happened in between. The blockchain is distributed among all the participants of the network which means that every participant stores a copy of the database. The main feature of a blockchain is that it can be used to build trust between parties that otherwise have no reason to trust each other. Blockchains build this trust because nothing in the history of states can be altered.
Maher Alharby and Aad van Moorsel describes this functionality very well: "A blockchain is an ordered list of blocks, where its cryptographic hash identifies each block. Each block references the block that came before it, resulting in a chain of blocks. Each block consists of a set of transactions. Once a block is created and appended to the blockchain, the

transactions in that block cannot be changed or reverted. This is to ensure the integrity of the transactions [4]."
Classically, blockchains are known from cryptocurrencies implementations. However, different distributed applications beyond cryptocurrencies can be implemented using the blockchain technology. One of these applications is smart contracts.

2.3.2 The general idea of smart contracts

A smart contract is like an object in object-oriented programming, so it is basically a piece of code and it can for example also inherit from another smart contract. Smart contracts can define rules concerning the value exchange between the parties, rules on what compensations are needed if agreements are not fulfilled as well as automatic enforcement of the compensation. The smart contract code runs on a blockchain so that the trustworthiness and automatic enforcement is supported. The automatic enforcement of terms and conditions does not only support trust, but it also cost efficient since traditionally a third party would be needed to provide trustworthiness as well as enforcement and execution of conditions which is more costly [4].

2.3.2.1 Advantages of smart contracts

Smart contracts first and foremost are decentralized. This means that nobody has the power over the data. Thus, no centralized server could potentially be attacked or exploited and instead the smart contract is implemented on the augmentation safe blockchain architecture. Smart contracts use a global currency which is a benefit because payments can be made directly and without currency conversion. Smart contracts have high trustworthiness since nobody is allowed to change the contract code once it is appended in the blockchain. However, the author can include functions that only specific addresses can alter variables in the contract, but not the code itself. A smart contract is implemented on a blockchain and automatically triggers functions based on the contract terms, has no human bias and does not make mistakes(if properly implemented) which is an important and also a new advantage.
The monitoring, however, is not done automatically because the smart contract does not have access to external solutions. The monitoring has to be done outside the smart contract. Lastly, complex contracts are less of a challenge when implemented using smart contracts since the implementation and understanding has to be done only once and the following execution is done automatically and without human intervention except for the data input. In summary smart contracts in contrast to traditional contracts can be more secure, faster and cheaper [2].

2.4 Smart Contracts for SLAs

Why would we use Smart Contracts for the implementation of SLAs? Both are contracts; thus that suggests that there can be a degree of compatibility between them. However, it is important to highlight, that one major challenge with SLA management is the SLA monitoring. It is difficult to measure service, for example, a cloud while providing trust in the measured data. It is unclear who is responsible for measuring the service and how it can be ensured which measurements are trustworthy. In that case either the customers measure the service, the service provider or a third-party. If the customers measure the service - which they tend to do if they want to ensure that the service is delivered as promised - there will be a large number of compensation requests of customers to the cloud service provider. For the cloud provider is then very expensive and time consuming

to answer all the requests of customers that measured that an instance had violated an SLA.
However, if the service provider monitors the SLA, then there could be trust issues since it is not favorable for a service provider, for example, Amazon to report SLA breaches. It is not good for their public image, and they have to pay the compensations. Therefore, the customers have no reason to blindly trust the service provider and leave all the measuring to them. The last possibility is to allocate a third party to perform the measurement such as the one described further in the related work section.
Regardless of the choice of manner to perform the measuring, it is usually expensive to constantly and accurately measure the service. Smart contracts could not only define the rules and penalties around a Service Level Agreement in the same way that a traditional contract does, but also automatically enforce those obligations.

2.4.1 Probable advantages of using smart contracts for SLA management steps

The advantages of using smart contracts for SLA management steps are the advantages of using smart contracts in general. One particular advantage of implementing SLAs with smart contracts is that it solves the problem of finding a reliable party to enforce SLA violations. An automated enforcement that follows from the smart contract when violated saves efforts and increases trust.

2.4.2 Possible difficulties when using smart contracts for SLA management steps

An important aspect to consider for the concrete implementation of SLAs using smart contracts is that it requires a stable currency which is currently not available in the assortment cryptocurrencies. If the currency is not stable, the compensation is volatile. Therefore, it is not a valid reassurance that losses at the customer's side, caused by service outages, will be compensated properly. This is because as long as the currency is not stable there could be a dip in currency value before the compensation and therefore the compensation could be worth significantly less than appropriate or even nothing at all.
Another issue is that even when the measuring is automated, the measuring service still needs to be trusted. Also, like in any other computer program, it is possible to get stuck in a loop which would affect the correct operation of the smart contract, causing more losses.

2.4.3 Implementation of Smart Contracts

The actual implementation of a Smart Contract can be done with many different languages. One of the most widely used and probably also most suitable languages is Solidity [8]. Solidity is the language used by the Ethereum blockchain [7]. Ethereum is a decentralized publishing platform, and it is crowd-funded. The most special property of Solidity is that it is a Turing-complete language. Being a Turing-complete language means that it is possible to write programs (contracts) that can solve any reasonable computational problem. Looping, branching and local state storage are possible.
Turing-completeness is important for Smart Contracts because it makes it possible to implement sophisticated logic. To implement a complex contract with conditionals and special cases the availability of sophisticated logic in the programming language is crucial. Bitcoin, on the other hand, uses a stack-based bytecode scripting language, and the ability

to create a smart contract with rich logic using Bitcoin scripting language is very limited since it is not Turing-complete. Furthermore, Solidity is similar to Javascript and has a large developer community, which makes it easier for programmers to learn the language and help each other grow in the community.

2.5 Related Work

The Web Service Level Agreement (WSLA) framework [6] was developed because web services were not uniform enough and very expensive to maintain and enforce. In the WSLA framework, the measuring, condition evaluation, and management part of the SLA lifecycle can be delegated to a third party. This third party can have the ability to enforce consequences when conditions are not met. The monitoring steps and interaction with the WSLA framework are illustrated in Figure 2.2.

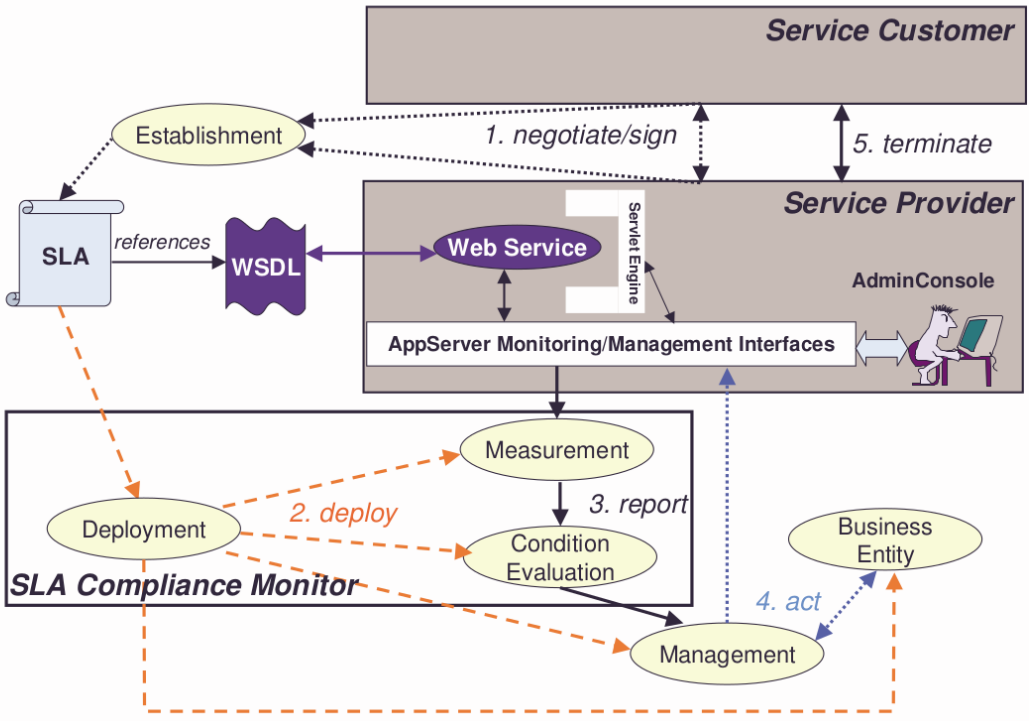


Figure 2.2: SLA monitoring by a third party through the WSLA framework [6]

2.6 Conclusion

In this paper, we reviewed the concepts of SLAs and smart contracts. Also, we conducted research trying to answer the question of how successfully smart contracts could be used in the implementation of SLAs. Based on the research and the arguments presented, SLAs could be translated into smart contracts. Generally, we found that using smart contracts for the implementation of SLAs to be a very promising idea. However, there are some limitations.

The main question that came up is how many additional regulations and what regulations exactly would have to be in place before the idea can work in everyday businesses. Regulations that we see a need for are for example legal regulations. They could come in the form of a smart contract template that is approved by lawyers so that it is made sure that smart contracts are legally valid.

Even though it would be possible to manage the full SLA lifecycle with smart contracts, with the current state of the art does not seem very feasible since there would be very many oracles needed to regulate availability, currency, server space, traffic, and so on, and the plausibility of a smart contract that is dependent on so many other systems is questionable. Therefore, we would suggest limiting the smart contract implementation of the SLA to the monitoring and enforcement stages of the management. Overall, it must be said that it is a very new technology and the usage of smart contracts for SLA implementation is only a proof of concept so far.

Bibliography

[1] Saad Mubeen, Sara Abbaspour Asadollah, Alessandro V. Papadopoulos, Mohammad Ashjaei, Hongyu Pei-Breivold, Moris Behnam: *Management of Service Level Agreements for Cloud Services in IoT: A Systematic Mapping Study*, 2017.

[2] Maher Alharby, Aad van Moorsel: *Blockchain-based Smart Contracts: A Systematic Mapping Study*, 2017.

[3] Alexander Keller, Heiko Ludwig: *The WSLA Framework: Specifying and Monitoring Service Level Agreements for Web Services*, March 2003.

[4] Maher Alharby, Aad van Moorsel: *A Systematic Mapping Study On Current Research Topics In Smart Contracts*, October 2017.

[5] G. Justy Mirobi, L. Arockiam: *Service Level Agreement in cloud computing: An overview*, December 2015. `https://ieeexplore.ieee.org/document/7475380/`

[6] Solidity Documentation `http://solidity.readthedocs.io/en/v0.4.24/`, last visited May 2018.

[7] Ethereum project `https://www.ethereum.org/`, last visited May 2018.

[8] Soldity Documentation `http://solidity.readthedocs.io/en/v0.4.24/`, last visited June 2018.

[9] Bettina Warburg: *Ted talk: How the blockchain will radically transform the economy*. `https://www.ted.com/talks/bettina_warburg_how_the_blockchain_will_radically_transform_the_economy`.

[10] Solidity in 2 Minutes `https://www.youtube.com/watch?v=3i203iTmcFc`, last visited May 2018.

[11] Margaret Rouse: *Definition: Service Level Agreement*. `http://searchitchannel.techtarget.com/definition/service-level-agreement`, last visited April 2018.

[12] blog.itil.org: *SERVICE LEVEL MANAGEMENT - PUT THE FOCUS ON THE CUSTOMERS EXPECTATIONS*. `https://blog.itil.org/2012/06/allgemein/service-level-agreements-fulfilled-customer-unhappy/`, last visited April 2018.

[13] Amazon: *Amazon Compute Service Level Agreement*, status of April 2018. `https://aws.amazon.com/ec2/sla/`.

[14] Microsoft Azure: *Microsoft Azure Service Level Agreement*, status of April 2018. `https://azure.microsoft.com/en-us/support/legal/sla/cloud-services/v1_5/`.

Chapter 3

Network Neutrality Laws: The Swiss Case Study

Cynthia Aludogbu, Kate Gadola

In December of 2017, the Federal Communications Commission of the United States decided to repeal their existing laws governing Network Neutrality. As a consequence, the topic was moved back to the forefront and is garnering a lot of attention in the media. In this paper, we aim to shed a light on what the underlying principles of Network Neutrality are and how its regulation has evolved. We discuss the different actors in the data delivery chain, how they may be able to influence Network Neutrality and what kind of influence regulation - or lack thereof - has on the end users and the local economy. With a focus on Switzerland as a case study, the arguments of the proponents and the opponents of regulation are taken into consideration. Furthermore, we compare the current situations regarding the law and the different providers in Switzerland, the United States and the European Union.

Contents

3.1 Introduction and Historical Background

The term "Net Neutrality" was first coined in 2003 by Tim Wu, a Columbia University, law professor. According to him, the main interest animating the advocacy of Net Neutrality is the idea of "preserving a Darwinian competition among every conceivable use of the Internet so that only the best survive" [1]. Although the term might be fairly new, the principles underlying Net Neutrality are anything but recent, predating even the Internet itself. Already in 1934, the Communications Act of 1934 was signed into law by US President Franklin D. Roosevelt. A new regulatory body, the Federal Communications Commission (FCC), was created and granted the power to regulate newly emerging technologies, such as telephony and broadcast TV [2].
One of the abilities appointed to the FCC was the power to label a communication organization as a common carrier. In general, a common carrier is an individual, a company or a public utility that transports people or goods in exchange for a fee, and it must do so in an agnostic manner [3]. This means that, for example, a railroad company must serve anyone who wishes to travel, regardless of age, gender, race or appearance, as long as there is space and the fee has been paid. The notion of a common carrier was not new, but with the Communications Act of 1934, it was applied, for the first time, to electronic communication.
The linchpin of the act was the wish to provide "universal service". The new act enforced this in two ways: FIrst, telecommunication companies would have to abide by regulations verifying that the rates they charged customers were fair and identical for everyone. Second, they were required to provide service to smaller rural areas, even though most telecommunication companies did not consider this to be profitable [2].
In the 1980s, when the Internet became publicly available, the common carrier laws were transferred de facto to the newly appearing Internet Service Providers (ISP). The first significant change of telecommunication law in over sixty years was implemented with the Telecommunications Act of 1996, whose main goal was to reduce regulatory barriers impeding entry and competition in the telecommunications sector [4]. This was supposed to open up the market, providing grounds for competition and innovation. However, based on a 2016 report from the FCC, 89% of households in the US only have zero or one choice of provider for Internet speeds above 100 Mbps [5]. A highly concentrated market such as in the communication industries can, on the one hand, lead to restrained competition, and on the other hand, it can undermine the interests of consumers [6]. This is the point where the debate about Net Neutrality began in earnest.
This paper aims to provide an overview of the topic of Network Neutrality, some varying opinions on what a neural network should encompass and how laws and regulations could be implemented to achieve this goal. Furthermore, it will discuss how neutrality principles can be bypassed while remaining within the boundaries of the law. Lastly, we will use the laws and regulations in Switzerland as a case study and compare them to different countries around the world, namely the United States of America and the European Union.

3.2 Network Neutrality

According to the Oxford Dictionary of English, Net Neutrality is "the principle that Internet service providers should enable access to all content and applications regardless of the source, and without favoring or blocking particular products or websites" [7]. This definition supports the "best-effort" principle, according to which the Internet has worked to date [8]. Conforming to this principle, all incoming data will be handled in the same way, provided that the full transmission capacity of the network has not yet been reached.

However, this interpretation of Net Neutrality may not suffice to offer a network that is indeed neutral, as the Internet value chain is not only restricted to ISPs and the internetwork level but also includes, among others, Content Delivery Networks (CDNs) and web portals, such as search engines. In this section, the different actors in the data delivery chain are presented, and the role that these actors can play in infringing upon the principles of Net Neutrality are discussed.

3.2.1 Actors in Data Delivery

The delivery chain starts with the Content Providers (CPs), that provide information and entertainment on the Internet. They are organizations or websites that produce online content, such as news reports, videos, movies, blogs or music. The content can either be accessed freely by everyone or only by members in exchange for payment. Some prominent examples in the entertainment sector are YouTube or Netflix. In the Swiss news media, examples are the SRF and newspapers, such as the TagesAnzeiger and the Neue Zürcher Zeitung.
These contents have to reach the consumers, which brings us to the next actor in the delivery chain, the ISPs. They are generally considered to be the main intermediaries in the data delivery chain and are therefore often the focal point of discussions about Net Neutrality [9]. The role of the ISPs is to provide Internet access to end users. To do this, they must connect, directly or indirectly, with other ISPs. These interconnections take place at Internet Exchange Points (IXPs) and can be grouped into two main types of interconnection agreements; transit and peering. In transit agreements, ISPs pay other networks to ensure access to every other sub-network of the Internet, often by traversing multiple sub-networks on the way. Peering is a direct connection between two sub-networks which are located physically close to each other and interconnect at an IXP. As opposed to transit, peering agreements are usually free of charge for both parties involved [8].
A further actor in the delivery chain is the CDN. CDNs are systems of distributed proxy servers (edge servers) which store cached content locally and deliver it to the end users depending on their geographical location [10]. This enables CDNs to guarantee CPs that their content will be delivered with high performance and reduced latency even during peak hours, as the physical distance between the end user and the server is reduced.
The last actors discussed in this paper are the search engines. They search documents or files for keywords and return the results in an ordered manner, beginning with the most important and relevant results, which are determined using ranking algorithms, e.g., PageRank.

3.2.2 Bypassing Network Neutrality Principles

The primary focus of regulatory bodies in the debate of Net Neutrality in Europe and the US is on the ISP and internetwork level [9]. As illustrated in the previous section, however, the data delivery chain also includes multiple other actors. These remaining actors, such as web portals (particularly search engines) and CDNs, are missing from the debate, even though there are numerous ways by which they can bypass Net Neutrality principles, all while remaining within the law. In this section we will discuss the methods that can be and - in some cases - are used by various actors in the delivery chain that infringe upon these principles.

3.2.2.1 ISPs

There are two main ways in which ISPs can differentiate Internet access and thus violate the Net Neutrality principles. The first method is quality differentiation, where ISPs can transport different data with different quality. The second method is commercial differentiation where, for example, some services of commercial partners of the ISP may be favored in certain user subscriptions [8]. These two methods are closely linked and often cannot be separated.
Over the course of the development of the Internet, new techniques have arisen, enabling ISPs to differentiate the data transported within their network. This means they can transport data in a fast, reliable manner or a slow and unreliable manner (higher delay, packet loss) [8][14]. There are a few incentives which might motivate network operators to influence the transportation of data to the end-users.
One such incentive would be if a network operator not only provides Internet access to its customers but also offers its services and content, for example, TV services [8]. This service would usually be transported via the same broadband connection that is used to transmit Internet data to its customers. The network operator would naturally be inclined to guarantee that their services are delivered in high quality and could thereby abuse its market power and protect itself against competitors offering a similar service [8][14]. The same principle can also be applied to services provided by commercial partners, e.g., affiliated CPs of the network operator.
Differentiation of data can furthermore be used to violate the Net Neutrality principle which states that access to all content should be provided to everyone, without discriminating based on the type of content. This can be achieved by offering different services to different demographic target groups. One such example would be to provide cheaper subscription plans which exclude the use of certain applications, e.g., WhatsApp or Skype [8]. The network operator could also charge higher prices for certain services, such as Voice over IP (VoIP). With this differentiation, ISPs would have the possibility of offering their own (vertically integrated) specialized services and could steer clients towards using them by blocking the competition. This would, in a similar fashion as the differentiation of quality, result in a great disadvantage for competing services. In addition, the customers would not have unrestricted access to all the content on the Internet.
Further use of data differentiation, with a similar outcome, is for ISPs to provide bad quality on certain Internet services intentionally so that their existing customers are inclined to purchase other services, preferably their own specialized services [8][14].

3.2.2.2 Search Engines

The most common way to discover and access content on the Internet is to use search engines as an intermediary. Hence, they can also greatly influence the number of views to any given CP by listing them at the top or the bottom of the suggested pages.
A common practice of search engines is to present their suggestions in one of two categories: sponsored results, from which the search engines profit when a user clicks on a corresponding link, and organic results, which should present the most relevant suggestions based on the input keywords [9]. Typically, the sponsored results are marked as such, and the user expects the organic results to be ordered according to pertinence. However, search engines might be tempted to include search results in the organic results that can, directly or indirectly, generate revenues. One such possible scenario would be in the case of a search engine owning a CP, which would, of course, incentivize the search engine to assign that content a higher rank [9].
There are two opposing forces to be considered in this scenario. The first is the short-term revenue, generated by users clicking on a link directing to the CP that is owned by the search engine. The second is the long-term motivation of the search engine to have a

high user satisfaction and thereby retaining the users, which also generates a long-term revenue. If the users are not satisfied with the search results, they may decide to switch to alternative search engines. However, even though search engines have an economic enticement to present results that are highly relevant and as such satisfactory to the end user, the negative effect of slightly biased results on the average relevance of the search results can be minimal. For CPs not owned by the search engine, these slight biases could, however, severely harm and potentially even threaten the survivability of those CPs [9].

3.2.2.3 Content Delivery Networks

CDNs can also engender differences concerning the average Quality of Experience (QoE) of CPs, which could be seen as another breach against Net Neutrality principles. One such scenario of a possible Net Neutrality breach is depicted in Figure 3.1.

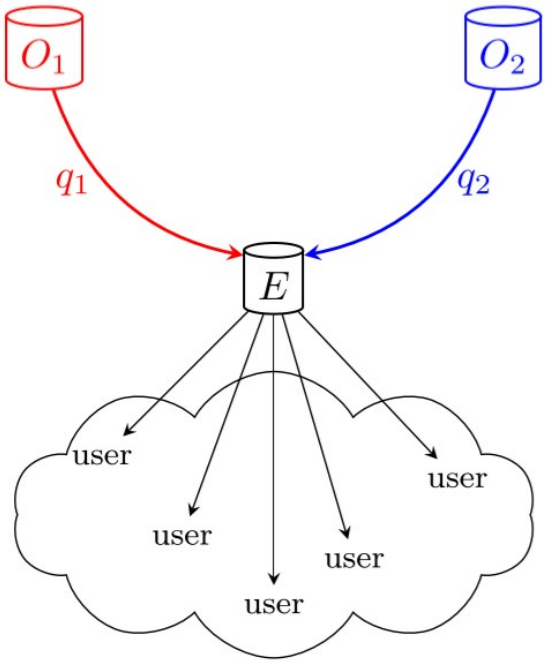


Figure 3.1: CDN with two rival CPs [9]

CDNs install edge servers, usually located near IXPs, to store the content as physically close as possible to the end users, which reduces latency and improves page load times [11]. For each request a CDN receives, it has two options: (1) It can get the content from the origin server O, or (2) it can get the content from an edge server E. Option 1 leads to high transit costs (unless the CDN also owns a transit network), as well as higher latency due to the geographical distance. Option 2 avoids transit costs and leads to higher QoE for the end users. Based on this, ideally, Option 2 should always be chosen. However, the storage/cache space at the edge servers are limited. For this reason, sometimes the CDN must resort to fetching the content from its origin server. To maximize profits, a CDN must find the optimal balance between the two Options, by deciding which content to cache at the edge servers. Additionally, it can also alter the number and/or the capacity of its edge servers [9].
The model in Figure 3.1 illustrates a scenario where one CDN offers its services to two competing Content Providers, both with their origin servers O1 and O2. These two CPs must share the storage resources provided by the CDN, which, in turn, will store the content generating the largest profit in its edge servers to maximize the revenue. Should the transit costs q1 and q2 be equal, the CDN will store the most popular content. If,

however, one CP has higher transit costs (for example CP1), then the CDN will be inclined to store more content from CP1, to reduce these transit costs. This will improve the QoE for CP1 customers and simultaneously reduce the QoE for CP2 customers. In summary, a CDN's internal costs can distort the competition [10].
Another situation, still based on Figure 3.1, can arise when two Content Providers pay the same price for the services of the CDN, but the content of one CP (say CP2) is more popular and higher in demand than CP1. The CDN will store more content from CP2 on the edge servers, meaning that even though both CPs pay the same fees, the dominant CP will be favored. This scenario is even further aggravated if the dominant CP2 pays a higher price, which CP1, possibly a newcomer to the market, cannot afford. The QoE gain for CP2 customers will be relatively small. However, the negative impact on QoE for CP1 customers will be more significant, leading to users switching to CP2 and reinforcing their dominant position in the market [9].

3.3 Network Neutrality in Switzerland

In Switzerland, there are currently no laws specific to Net Neutrality [8]. If network operators block or discriminate against data, neither consumers nor CPs have any legal grounds to battle against the offending network operators - even though, according to Article 16 of the Federal Constitution of the Swiss Confederation, "freedom of expression and information is guaranteed" [12].
Furthermore, in accordance with Article 49 of the Telecommunications Act, suppression of information, falsification, and inequalities in data transport are all legal, as long as the possibility of different treatment has been contractually stipulated by the network operators [8][13].

3.3.1 Current Situation

In 2012, the Body of European Regulators for Electronic Communications (BEREC) investigated the current traffic management practices. The results depicted in Figure 3.2 are based on 414 responses to a questionnaire sent out to telecommunication service providers in 32 European countries, Switzerland included. These providers have coverage of 90% of the market in their respective countries [8]. According to BEREC, their aim is "to promote end-users freedom to access and distribute content and run applications of their choice online, to promote competition and innovation" [15].
Figure 3.2 shows that for peer-to-peer traffic in Europe, 15.0% of fixed Internet access providers and 35.7% of mobile Internet access providers block or restrict the application for either some or for all of their subscribers. It also shows that 23.5% of mobile Internet access providers block or restrict the use of VoIP for their subscribers. Weighted according to the number of customers per providers, this means that more than half the European population with Internet access is either blocked or restricted from using VoIP [8]. BEREC states that this practice of differentiating traffic, which engenders constraints when accessing specified content or applications, is the most pertinent when it comes to the discussion of Net Neutrality and its regulation [15].

3.3.2 Market in Switzerland

There are a few services offered in the Swiss market which are subject to heated debate in the Net Neutrality discussion. In this section, some of these services are presented from the viewpoint of both the proponents and opponents of Net Neutrality regulation.

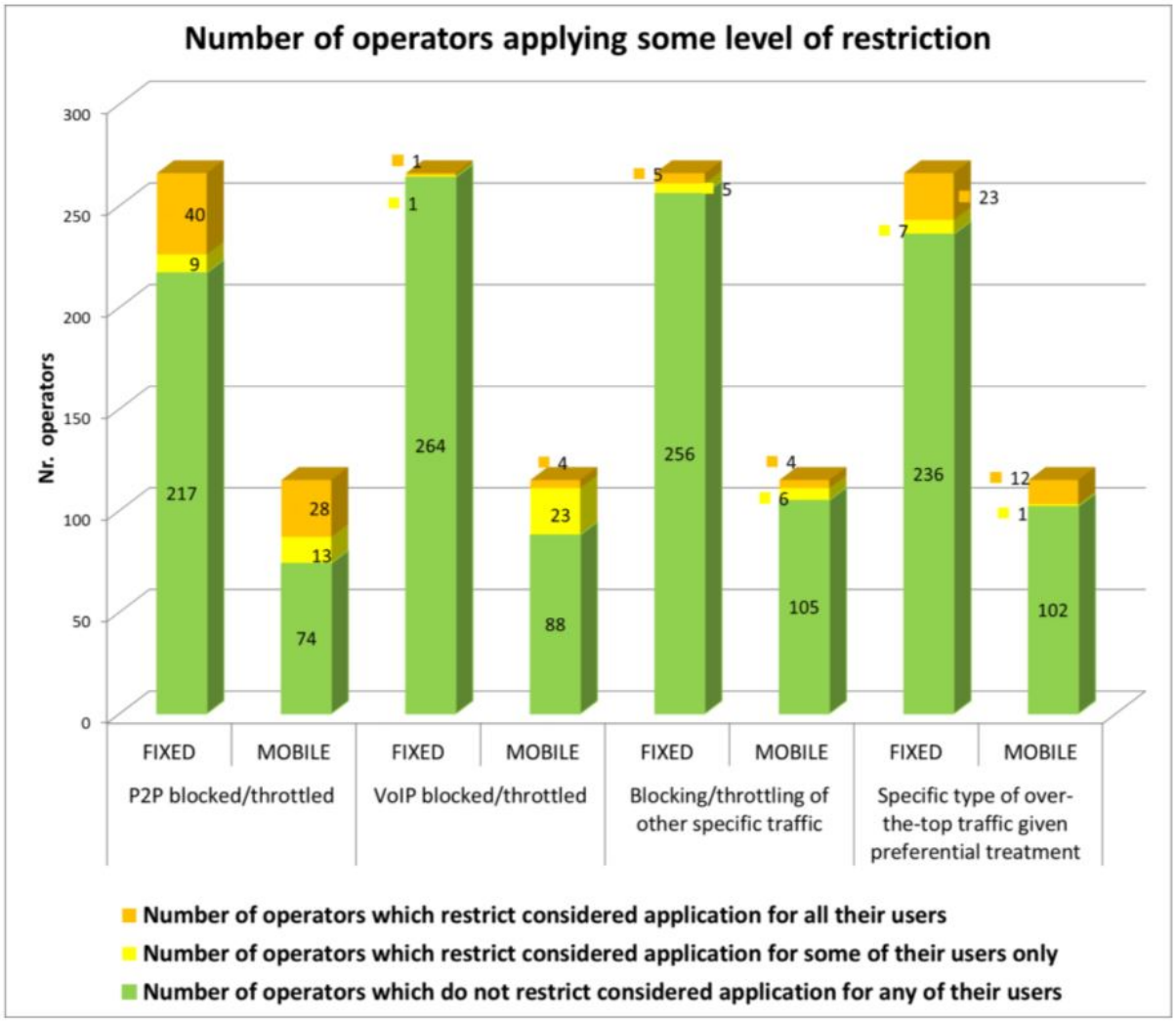


Figure 3.2: Number of providers restricting the usage of Internet services [16]

The opinions and examined practices are based on a report on Network Neutrality of the working group of the Swiss Federal Office of Communications (OFCOM) [8].
One such controversial behavior and the strongest type of interference [14] is, as was found to be a common practice in Europe by BEREC, the differentiation of traffic and blocking of certain services. Also in Switzerland, some network operators offer mobile contracts for which the use of VoIP (e.g., Skype) is excluded. This should motivate the consumers to use the service provider's telephone service instead. Net Neutrality opponents argue that these contracts are usually priced lower than those without the restrictions and that prohibiting these restricted contracts would limit their opportunities to design products, and thus weaken competition and innovation. Proponents claim that there is no reason why the cost of a contract would decrease in any significant manner when some services are excluded, and the only reason behind these types of contracts is to get customers to use their own services.
Another example that can also be found in Switzerland is the practice of implementing business models which bundle specialized services together with Internet access. One example is to place a cap on the amount of data allowed by a contract, but not include certain services to count towards reaching that cap (e.g., Spotify, WhatsApp). Net Neutrality opponents state that these contracts are unproblematic, as they are more expensive than those without the inclusive services. This means that customers deliberately decide to pay higher fees and get the additional services in return. Furthermore, they point out that competitors of Spotify and WhatsApp can also apply to be inclusive services, which would

mean that this practice does neither hinder competition nor innovation. Proponents, on the other hand, are of the opinion that innovative start-ups and smaller companies have a very small chance of being accepted as inclusive services next to or instead of the established companies, and that such practices cause disruptions to the level playing field of CPs.
Furthermore, as described in a previous section, some network providers also offer their own services and do so with guaranteed high quality. For certain services (e.g., television), this requires high bandwidth and can restrict Internet access on the same line, thus potentially disturbing the best-effort delivery in that network [15]. Opponents of Net Neutrality argue that such prioritization only occurs when the maximum capacity of the line has been reached and that it is necessary to prioritize in order for the customers to receive the service in the quality they have paid for. Proponents believe that the customers not only pay for the specialized service, but also for general access to the Internet, and therefore expect always to have that bandwidth available. They also make the point that such prioritization can be abused to create a two-tier Internet, where ISPs can require money from CPs in return for prioritizing their content. This would also favor large, established CPs and in the long run would hinder innovation and limit the customer's freedom of choice [14][15].

3.3.3 Arguments For and Against Regulation

As is the case with any controversial topic, there is an abundance of opinions on whether there should be regulations on Net Neutrality or not. The OFCOM working group has collected some of these opinions, both for and against regulation, in the Swiss market [**?**, 8] Based on these findings, this section will first provide some of the most common arguments proponents make in favor of regulation, and then the contentions of the opponents of Net Neutrality regulation.

3.3.3.1 Opponents

The main opponents of Net Neutrality regulation are the network operators, as they would be limited in their possibilities to compete in the market. They state that the Internet has successfully developed so far without any regulation and that it is therefore not necessary to introduce regulation now. They are also of the opinion that any regulation would be obsolete because the market would immediately punish any wrongdoings. Customers nowadays expect to be able to use services such as Google, Facebook, and Skype, and network operators, therefore, cannot afford to block or reduce the quality of certain services.
According to the opponents, controlling Internet traffic is necessary for technical and economic terms. Network expansion is not free, just as transport capacity is not infinite. They argue that it makes no sense to have networks that are sized to the maximum load they transmit at peak times, as that would result in largely increased cost and a considerable amount of unused capacity during all the other times. It is therefore sometimes important to be able to deviate from the "best-effort" principle to manage traffic and guarantee that quality-sensitive services can be successfully transmitted. They also point out that in case of an occurrence of network congestion, it is essential that some services, such as emergency calls, can be prioritized.

3.3.3.2 Proponents

The main demand made by proponents of regulation is that the fees for Internet access should be identical for everyone, regardless of how the user intends to use the Internet.

They state that as continuously more and more network operators offer their own or purchased content, the operators have not only the economic interest but also the means to favor their services or discriminate data.
Another point they make is that the Internet is a communication infrastructure which is of major significance to society, as it provides a platform that ensures freedom of information and diverse opinions [8]. ISPs have some measure of influence on the content offered to the end users, e.g., they can discriminate between data and content. This would threaten this platform and could be grievously detrimental to society, for example by impeding freedom of speech and cultural or political diversity [14][15].
As stated in the previous section, opponents believe that the expansion of the infrastructure is expensive and only economically reasonable to a certain extent, so they must be able to manage traffic. In answer to that argument, proponents contend that network operators would have no problem funding the necessary expansion with the revenue of their customers. These revenues can also be influenced if network operators use appropriate pricing plans for their customers. Another argument they make against traffic management is that ISPs could purposely not expand Internet access, such that CPs would be willing to pay higher fees to receive better transportation. Such a business model would only work if bottlenecks existed and the capacity was limited. Furthermore, if established CPs could pay higher fees in return for prioritization, smaller companies or newcomers could not compete in the market.

3.3.4 Approaches under Discussion for Network Neutrality Regulation

There are many different proposals regarding the actions that should be taken concerning Net Neutrality regulation in Switzerland. These proposals range from no interference by the state at all to demands for legislation prohibiting certain practices. A few of these proposed approaches will be discussed in this section.
In the EU, regulation of Net Neutrality already exists. Some of these regulations could also be adopted by the Swiss Confederation:

- Network operators must provide information on differentiation [17].
- Customers have the right to withdraw from a contract if a modification in the rules for differentiation has been made by the network operators [17].
- Network operators must provide a minimum quality of Internet access, which is stipulated by the national regulatory authorities [17].

Some further approaches which have been suggested are as follows:

- Prohibiting the practices of blocking data or intentionally transporting poor quality data [8].
- Only allow the term “Internet” to be applied to services that offer access to the entire Internet, without discrimination [8].
- Ensure that network infrastructure providers and content providers are separated [8].

Another common view is that it does not make sense to define in advance which traffic management practices are reasonable and legal [15]. The most effective counteractions to potential misconduct are transparency and competition [14]; Transparent network management practices would enable customers to make an informed choice of the ISP they

subscribe to. This, in turn, would lead to higher competition among the different ISPs of a region [14], ultimately benefiting the end user and preventing exploitation by the network operator. The network operators should furthermore be monitored by a regulatory body. In the case that misconduct does indeed occur, that case would then be reviewed on an individual basis.

3.4 Net Neutrality Around the World

At the earlier stage of the internet, it is saying that no one owns the internet, but with all the recent issues facing the internet, it since like the world is moving toward destroying the internet. The internet is a way to communicate globally easily. With free access to the internet businesses and transaction are carried out around the world. The repeal of net neutrality in the USA has left a lot of unanswered questions about internet freedom. Every country maintains their law on the internet differently. The U.S most recent law on the role of government overseeing and regulating internet move forward, it is important to view where other countries stand on net neutrality [18].
The federal communication commission (FCC) December 2017 decided to decontrol U.S internet. Net Neutrality is an open-access internet consumer protection, that is based on the idea that users should be free to advance their views and users have the full right to choose what service and content to consume on the internet without any discrimination for the internet services provider (ISP). Net neutrality law stands on the principle that no one, not lawmakers or ISP companies is granted the right to restrict, prevent or block content, applications or other internet services of the users [18].
As the United States repeal the net neutrality law and hope to control what their citizens and residents access to the internet which limits or remove the online freedom, most countries around the world are already doing so. While many countries are striking even stronger regulation the ones FCC did.

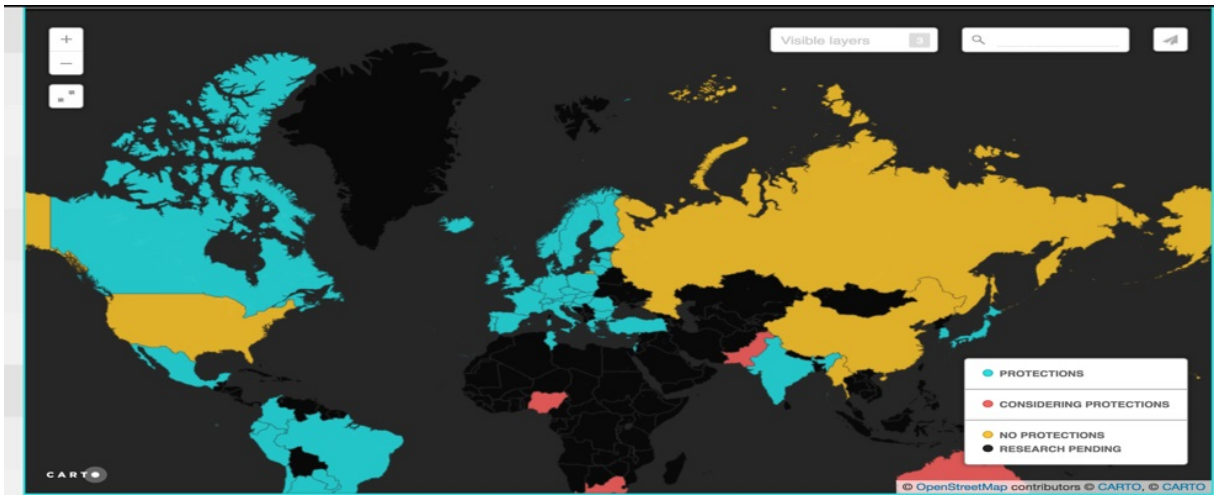


Figure 3.3: Status of net neutrality around the world

3.3 [19].

- Protection: these countries have laws or regulations in place protecting net neutrality. (E.g., Canada, Iceland, United Kingdom, India, Japan, South Korea and many more).

- Considering protection: these countries have not passed any laws or regulations, but they are working on one that will be considered by lawmakers or administers. (E.g., Australia, Pakistan, Nigeria, South Africa, Uruguay).

- No protection: these countries have no net neutrality laws or regulations. (E.g., Russian, China, United States).
- Research pending: there are countries that further research is being conducted on net neutrality in the country (there are many other countries that research on net neutrality is still ongoing).

3.4.1 The United states Net Neutrality

The united states since to be the law creator and lawbreaker, in the past ISPs in the U.S has restricted, prevent or block content from their users even when the net neutrality law is in place. In 2017, Comcast unlawfully blocked their users from sharing files with each other. In 2009 AT&T stop the user from connection to Skype and face time apps on their network. In 2011 Metro PCS stop their internet users form streaming Netflix and other online videos except not YouTube (due to some behind closed door negotiated deal). In 2012, Verizon disconnect apps that allow users to access internet on the computers from their mobile data service. There are many other ways that ISP in the U.S has violated the fundamental idea of net neutrality. Individual and lawmakers have tried to discipline these biased practices from ISPs for years with public debate and various court cases. In 2015, during the president Obama administration, the FCC reached a decision for open and free access to internet, the rule which eliminate the ISPs power to control, speed up or slow down traffic based on the content or paid prioritisation which offer "fast lanes" for big media sites and service providers like Facebook, Google and Netflix. The decision was not 100 percent perfect deal for individuals and small businesses, but it is a start to move forward [18]
In 2017, shortly after president Trump took office, Mr. Pai FCC chairman and other commentators rushed to undo the net neutrality rules in the sense that customers/users will receive far better services with a less regulated market, but since to ignore the fact that such rules are in place on the emerged of problems or the internet complaints[18]. Many countries around the world are dealing with a similar dilemma on how to manage current life digital realities, and they are slowly and individually contributing to a patchwork of law that differs from country to country. Several highly industrialized and in fact developing countries since to agree that regulations to protect the internet freedom is good for people and civil society.

3.4.1.1 Direct impact on The United States Residents

The United States vote to end the net neutrality law that protects open internet, the voted to dismantle the restriction that prevents ISPs from slowing down or blocking websites from distributing certain services. For many Americans, just like most people around the world want the right to choose what website to visit and what apps to use and so on. However, with this recent repeal on net neutrality, the ISPs in the U.S such as; Comcast, Verizon, and AT&T can affect the decisions based on which services and content U.S residents can access, download or get information [20]. The United States without the protection of the internet gives out a free path for ISPs to charge websites and services more to load content from a network subscriber. Also, this decision might create a fast lane and slow land, of which the fast can possible only be afforded by the rich and large companies. For small start-up businesses and lower-income individuals in the U.S that cannot afford "fast lane" internet will have to deal with slow or ever block of websites based on the content in some case [20].
The United States interest has always been under the net neutrality principles which mean that all Americans should have equal access to the internet and the ability to choose what kind of information there consume. Just like many people, we want to have that feeling

that we are in control of our life, what type of website and app will choose to access online should be the internet user choice without having ISPs and lawmakers limiting those choices. The internet freedom should users full right and not a privilege. The recent U.S decision gets rid of the net neutrality law in place and might ever restrict the FCC from putting rules into effect in future, even when the ISPs start acting very poorly [20]. The direct effect on people could be, for instance, ISP can go to Netflix demanding for an extra amount of fees per month in other for their contents to load for that ISPs subscribers. If Netflix could not find any other way out of the request, they will be forced to pay and whatever Netflix pay will be pushed to consumers that subscribe to Netflix. This will increase the price of what people do online, fewer free things will be available online, and fewer people will be visiting sites, the internet will become more consolidated. Startups and blogs that don't have extra money to pay for "fast lane" will not survive. For individuals getting access to some information they need will depend on how much money they have or earn [20].

3.4.1.2 Possible impact on U.S economy

The perception of net neutrality argues that everyone should have equal access to things on the internet, whether it is considered to be a small business owner or large company. It advocates the principle that every individual should be able to access and communicate freely online. With online access equality, and ability to get your business website and content in front of the same congregation as other, assure equal market competition for everyone from startup and freelancers to small business owners [21]. However, the decision to repeal net neutrality could eliminate open and free access to the internet for small businesses and consumers. Especially when the new regulations that could formerly not stop ISPs from charging the businesses more for "fast lane" access and institutions to get access to content consumers. Some small businesses would not be able to afford to budget high price for data prioritization as it could become expensive[21].
In a situation where small businesses and start-up cannot afford to pay the "fast lane" service, there will start losing access to the target audience online which is one of the best and most effective ways to reach the consumer. Old traditional marketing channels style does not really attract consumers as much as online business. Thus, is really not the best way to reach a larger audience. In an economic point of view, removal of net neutrality will create a serious problem for small businesses that have helped raise and grow the U.S economy. We also have to keep in mind that most of the U.S economy those are thought small business, as many of the big companies has outsourced and allocated their factories to China [21]. Plus, larger corporations especially media giants like Facebook will have more power over what content to share with few lucky people online. It will marginalize society /humanitarian that gain a voice through the ability to leverage the internet and raise awareness. The end of net neutrally could actually go beyond streaming content. It could have an impact on companies behind Internet-of-Things (IoT) devices as people will choose not to buy the products that need internet to work because that will generate more bills for them every month [21].

3.4.1.3 Obstacles of the decision in the United States

Repealing net neutrality is a huge battle that cable television and internet service providers want to win to remain relevant to the American consumers. It is important to understand the obstacles that will come with the repeal such as internet inequality; the end of net neutrality will be the beginning of the net inequality which means that ISPs will be charging start-ups, blogs and small businesses more for basic services and fast internet. The ISPs can choose which companies should have access to high-speed internet and at what

cost the companies should pay for it, which could be unfavorable for the streaming industry. Individual consumers will lose, the repeal will be more like old media wins, and new media loses, and final consumers like us will be the ones to pay the bills. In the past few years, many people have been dropping their TV packages mostly because they get daily news on their smartphone which allows companies like Hulu, Netflix, and Amazon to grow their membership bases. If broadband providers get their way to charge these companies more, they will, and the cost will be transferred to consumers. Finally attempting to stay relevant, a massive increase in people especially millennials use streaming to view TV and movies, cable TV is fighting hard to streaming, just like the print media and the online media. Unfortunately, the world is at that level where people, mostly young people will not control when it comes to the internet on a smartphone as we do everything with it. It is clear to say that the cable greatness days are over, but the recent repeal on the U.S net neutrality is in favors of the old media giants interest and will hurt other companies like Netflix [22].

3.4.1.4 The beneficiaries of the new rule

The decision to repeal net neutrality in the U.S will benefit and hurt a certain group of people, therefore is important to highlight those that will gain or lose under the new rules. The most important issue for supporters of net neutrality is the fact that ISPs could charge extra fees for transporting the same form of content at a fast speed through its network. I.e., if you want to get things done fast you should pay more. The ISPs in the U.S has promise American consumers that there will protect open internet, avoid blocking of legal content, less control over data speeds and no discrimination but ever mention anything about paid prioritization which since to be one of the areas they wish to benefit for the repeal [23].
Small business-like Start-ups could be affected in a negative way by this repeal could. Small start-ups that do not have the money or clout to pay for "fast lane" content delivery. United States net neutrality roll back will put small and medium-sized companies at a huge disadvantage over large companies. ISPs will be favoring certain e-businesses, website or platforms that they use to get new customers over others by placing the ones that paid in "fast lane" and slowing down or block other. Those are corporations that provide help dependent on fast services, like the ones whose perform remote health connected illness, are likely to benefit from the repeal, there are known as connection to sensitive services in the U.S. FCC also predict that the repeal will advance the development of new technologies such as autonomous vehicles, which need guaranteed internet connection [23].
Non-supporters of the repeal on net neutrality believe that consumer is the bigger losers under this new rule as they will be the ones that will end up paying more to stream certain content if they don't want to be frustrated by network traffic. This might lead to decrease in customer choices of internet service providers, and prices of broadband service will increase [23]. The principle of net neutrality is to keep the internet open for all and protect consumers access to websites and apps they wish to use, and not their internet service provider choices [23].

3.5 European Union

3.5.1 Net Neutrality in the EU

European union end-users have the full right and access to open internet without discrimination or prioritization of content and services that the users wish to access. The EU stands on a very strong net neutrality rules that traffic on the internet must be treated equally. On the hand, the EU net neutrality rules notice and states that some traffic

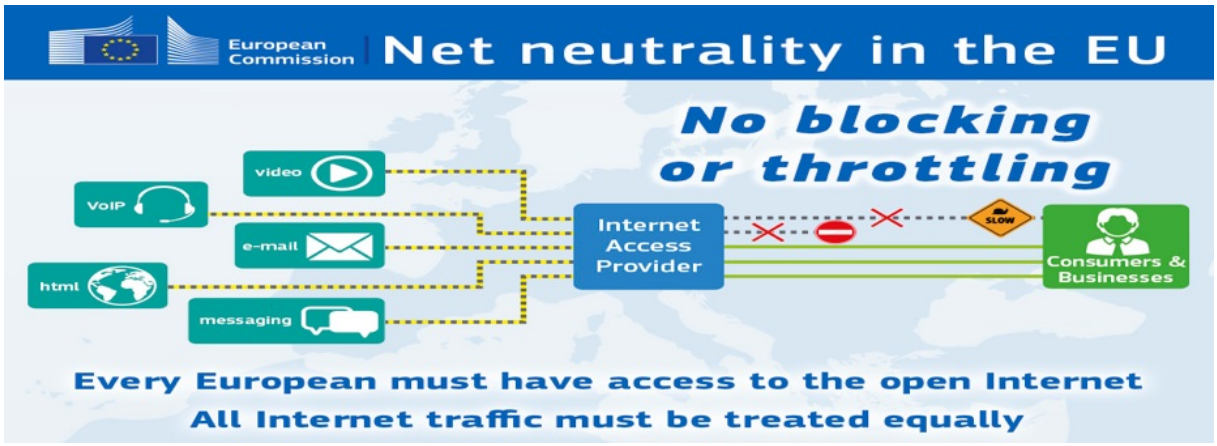


Figure 3.4: Net neutrality in the European union

with specialized services or services with specific quality level can be granted reasonable traffic management if necessary [24]. In 2015, European Union signed a strong rule demanding that telecommunication companies that provide internet access to manage all traffic equally and can only restrict traffic when network "equipment is operating at its maximum capacity" [24]. The rules also permit a little restriction in order to protect network security and manage emergency situations. In 2016, the European union electronic communications regulators notice a possible problem in the agreement and clarify that quality of service could differ, but no specific applications should be discriminated against. In 2017, the government notices some issues in the agreement that might result to a problem if the ISPs do not obey the rules; thus they start to monitoring the net neutrality agreement rather than waiting for violations to happen before reacting. European residents have better and stronger consumer protection than in the United States [18].
European Union regulation on net neutrality is a great accomplishment for the digital market. The rules give the final users the right to access and distribute their choice of content and services, which BEREC works on to ensure that these rules apply all over Europe. Internet service provider in Europe does not have the power to determine the success or failure of an individual, start-up and small businesses content and service distributed. [24].

3.5.1.1 The United states net neutrality repeal effect EU

The United States decision on net neutrality, do not have any effect on under the EU net neutrality law. European Union remains strongly committed to the free and open internet for citizens and residents. For many years, the united states of America have been known for setting and leading the world especially when it comes to a human right. That is one of the reasons why we may be interested in what other countries reaction might be with the FCC decision. Unfortunately, the FCC decision is just like one of those that have been made by trump administration and many countries are not in line with it [25]
Another important question is, what kind of net neutrality rule will the UK follow after the Brexit. Currently, the UK net neutrality is protected by EU policy support of the Digital Single Market. When the Brexit is finalized, UK government might choose to repeal the policy, which is more unlikely as it has been committed to universal service obligation [25]

3.6 Net Neutrality in Switzerland, USA vs the EU

There are apparent differences between the United States, European Union and Switzerland in the case of net neutrality. Switzerland does not have a law governing net neutrality, but in 2014, all the primary internet service provider (ISP) voluntary signed a code of conduct pledge to establish authority to monitor the code. The code of conduct states that ISPs cannot discriminate against content except for network management. Major ISPs like Swisscom, Sunrise, UPS cable-com, Orange, and the cable network companies' association Swiss-cable signed the voluntary code of conduct. Switzerland might not have the agreement called net neutrality agreement, but the code of conduct protect people right to access the internet freely, and it supports an open internet [19].
The European Union strongly support net neutrality and are monitoring the rules all over EU. The Body of European Regulators for Electronic Communications is involved in the EU net neutrality law to ensure that all (ISPs) in every EU countries obey the rule. Switzerland and European Union since to support open internet compare to the United States that recently vote to appeal a common-carriage legal rule to broadband internet access which disqualifies net neutrality protections for people in the United States. The new net neutrality in the USA allowed blocking throttling and paid prioritization, which since to make their case worst compare to the EU and Switzerland.

3.7 Conclusion

As seen in this paper, Net Neutrality is a controversial topic with strongly opposing viewpoints. In order to keep the Internet a level playing field, or - as Tim Wu phrased it - "'preserving a Darwinian competition"' [1], passing legislation would be the most effective method to achieve this. The argument of the opponents that regulation would be obsolete because the market would punish violations anyway seems nonsensical. This implies that they are already regulated, and any additional regulation would not affect them either way. So, why then would they oppose regulation in the first place? The control of network traffic due to technical and economic factors, on the other hand, might sometimes be hard to avoid. This could, however, also be considered when passing a new law protecting the Neutrality of the Internet. It is also imperative to take into consideration the fact that the internet is the main form of communication and primary platform to state one's opinion. Network operators have a certain amount of control over what reaches the consumers and what doesn't, and even though they might never abuse this power, appropriate laws could guarantee to keep this from happening.
It is safe to say that our world today will never function properly without internet. The world will not move backward but forward. Nothing good will come out of restricting the internet, although the U.S decision on net neutrality is still very new and no one knows what the coming years of the decision will be. But accoutring to many online articles implementing this new rule might a lot more difficult than expected. The decision might one of those rules are written but never actually go into practice. Switzerland might not have had any law called net neutrality, but there has a promise that can be count on. The ISPs signed a code of conduct pledge to establish authority to monitor the code in order to give the end users suitable open internet access. The European Union deeply believe that freedom of the internet is for everyone equally as EU residents and citizens enjoy open internet with discrimination or prioritization.

Bibliography

[1] Tim Wu: *Network Neutrality, Broadband Discrimination*; Journal of Telecommunications and High Technology Law, 2003, Vol. 2, p. 141

[2] Zsuzsa Detrekoi: *Net Neutrality: Current State of Affairs and Main Players*; `https://cmds.ceu.edu/article/2018-01-26/net-neutrality-current-state-affairs-and-main-players`, March, 2018

[3] The Free Dictionary; `https://legal-dictionary.thefreedictionary.com/common+carrier`, March 2018

[4] Nicholas Economides: *The Telecommunications Act of 1996 and its impact*; Japan and the World Economy, 1999, Vol. 11, No. 4, pp. 455-483

[5] Federal Communications Commission: *Internet Access Service: Status as of June 30, 2016*

[6] Hanlong Fu, Yi Mou, David Atkin: *The Impact of the Telecommunications Act of 1996 in the Broadband Age*; 2015

[7] Angus Stevenson: *Oxford Dictionary of English*; Oxford University Press, 3rd Ed., 2011

[8] Federal Office of Communications OFCOM: *Network Neutrality: Report of the working group*, 2014

[9] Patrick Maillé, Gwendal Simon, Bruno Tuffin: *Toward a net neutrality debate that conforms to the 2010s*; IEEE Communications Magazine, 2015, Vol. 54, No. 3, pp. 94-99

[10] Patrick Maillé, Karine Pires, Gwendal Simon, Bruno Tuffin: *How Neutral is a CDN? An economic approach*; Proceedings of the 10th International Conference on Network and Service Management, 2014, pp.336-339

[11] Cloudflare; `https://www.cloudflare.com/learning/cdn/glossary/edge-server/`, April 2018

[12] The Swiss Parliament: *Federal Constitution of the Swiss Confederation*; February 2017

[13] Die Bundesversammlung der Schweizerischen Eidgenossenschaft: *Fernmeldegesetz (FMG)*; March 2018

[14] Jan Kramer, Lukas Wiewiorra, Christof Weinhardt: *Net Neutrality: A Progress Report*; Telecommunications Policy, October 2013, Vol. 37, Issue 9, pp. 794-813

[15] Body of European Regulators for Electronic Communications (BEREC): *BEREC Annual Reports 2012*; BoR(13)67, June 2013

[16] Body of European Regulators for Electronic Communications (BEREC): *A view of traffic management and other practices resulting in restrictions to the open Internet in Europe*; BoR(12)30, May 2012

[17] The European Parliament: *Universal Service Directives*; Official Journal of the European Union, March 2002

[18] Meinrath and Foditsch, "How Other Countries Deal With Net Neutrality," 15 December 2017. Online. Available: https: www.smithsonianmag.com/innovation/how-other-countries-deal-net-neutrality-180967558/.

[19] Carto, "Status of net neutrality around the world," 2018. Online. Available: https://carto.com/gallery/net-neutrality/.

[20] Stanford, "What does the end of net neutrality mean for Americans and democracy online?", 18 December 2017. Online. Available: `https://medium.com/freeman-spogli-institute-for-international-studies/what-does-the-end-of-net-neutrality-mean-for-americans-and-internet-democracy-b4`

[21] Brown, "The Impact Of Net Neutrality Laws On Your Business," 8 December 2017. Online. Available: `https://www.forbes.com/sites/forbestechcouncil/2017/12/08/the-impact-of-net-neutrality-laws-on-your-business/#58c791da3662.`

[22] B. Kelly, "Net Neutrality Issue Again: Pros and Cons," 12 December 2017. Online. Available: https://www.investopedia.com/articles/markets/062014/what-you-need-know-about-net-neutrality.asp.

[23] S. Masunaga and P. Jim, "Here's who'll benefit and who might not if net neutrality is repealed as expected," 14 December 2017. Online. Available: http://www.latimes.com/business/la-fi-net-neutrality-20171213-htmlstory.html.

[24] Europa, "Open Internet," 09 September 2013. Online. Available: https://ec.europa.eu/digital-single-market/en/open-internet-net-neutrality.

[25] Bhatti, "Net neutrality may be dead in the US, but Europe is still strongly committed to open internet access," December 2017. Online. Available: https://theconversation.com/net-neutrality-may-be-dead-in-the-us-but-europe-is-still-strongly-committed-to-open-internet-access-89521.

[26] Masunaga and Puzzanghera, "Here's who'll benefit and who might not if net neutrality is repealed as expected," 13 December 2017. Online. Available: http://www.latimes.com/business/la-fi-net-neutrality-20171213-htmlstory.html.

Chapter 4

Advanced Message Queuing Protocol as a Communication Protocol Standard for IoT

Maciej Lebiedz

The Advanced Message Queuing Protocol (AMQP) is an open standard for passing business messages between applications or organizations. Its development began in 2006 and the design has been driven mostly by the finance community's technical needs. Focus was put to create a secure, compact, reliable transfer protocol to move messages between applications. AMQP now in version 1.0 is an international ISO/IEC standard. It is an asynchronous messaging protocol, not tied to any message source, model or topology. This paper explores in depth operation, use cases and pros and cons of AMQP and its possible impact and usage in Internet of Things.

Contents

4.1 Introduction

Advanced Message Queuing Protocol is a lightweight asynchronous M2M messaging protocol designed for reliability, security, provisioning and interoperability. While Various middleware standards exist for synchronous messaging, including Corba's Internet Inter-ORB Protocol (IIOP), Java Remote Method invocation (RMI), and Simple Object Access Protocol (SOAP), it wasn't the case for a long time in area of asynchronous messaging. Some proprietary products exist and use their own closed protocols, for example IBM Websphere MQ (formerly known as MQ Series) and Microsoft Message Queuing (MSMQ).

4.1.1 Motivation to develop AMQP

The lack of open asynchronous messaging protocol standards means messaging implementations don't interoperate. In June 2006 though, JPMorgan Chase (JPMC), Cisco Systems, Envoy Technologies, iMatix Corporation, IONA Technologies, Red Hat, TWIST Process Innovations, and 29West together announced the formation of the Advanced Message Queuing Protocol (AMQP) working group [2] which was supposed to create an open standard for an interoperable enterprise-scale asynchronous messaging protocol.
Current version of the protocol is 1.0. It has been developed iteratively, while taking feedback from developers and community into account. Most of the AMQP architecture has been driven by the finance community's technical needs. The focus is put on reliability, performance, throughput, scalability, and manageability. This report explains how Advanced Message Protocol works, mentions alternative asynchronous messaging protocols and discusses its use in Internet of Things (IoT) applications.

4.1.2 AMQP in Context of Internet of Things

Internet of Things is a term used to describe a network of physical devices such as sensors, everyday household objects such as fridges or watches that are able to exchange informations and communicate with each other without human interaction. These devices are usually small, with limited memory and processing power. To communicate over network, IoT devices use a variety of Internet protocols, some of which are regular and well known Internet protocols like IPv4, IPv6 or TCP and some of which that are emerging protocols designed to meet requirements of restrained IoT devices, for example 6LoWPAN or LPWAN. Internet of Things protocols can be grouped into infrastructure (6LowPAN, IPv4/IPv6), identification (Electronic Product Code), transport (Bluetooth, LPWAN), discovery (mDNS), data protocols (MQTT, CoAP, AMQP), device management (OMA Device Management), semantic (Semantic Sensor Net Ontology), multi-layer (IoTivity) and security (Open Trust Protocol) protocols [6].

4.2 Explaining AMQP

AMQP provides a layered model - there is frame transfer protocol and on top of that message transfer protocol. Containers, connections, channels, sessions are parts of frame transfer protocol, nodes and links are at message transfer layer. There are flow control mechanisms on both layers, that are useful for IoT devices with restricted memory and processing capabilities.

4.2.1 AMQP Model

AMQP model consists of ***containers*** - applications, that are connected between each other by ***connections***. Each connection can have multiple ***channels*** - unidirectional

paths through which ***frames*** can be send. Two channels can be bound together to form ***session*** which is a bidirectional, symmetric connection. Every container can have multiple ***nodes***. A node can be a consumer, producer, queue, relay or other structure. Nodes communicate with each other via ***links*** by exchanging ***messages***. Link is a transfer route in one way and acknowledge in other way. A session can have any number of concurrent links.

4.2.2 Containers and Nodes

Containers are applications in AMQP terms, nodes exist within a container and each container may hold many nodes. Examples of containers are brokers and client applications. Nodes are named, addressable entities within the application responsible for the safe storage and/or delivery of messages. Messages can originate from, terminate at, or be relayed by nodes. Nodes can be organized in any way - flat, hierarchical, or as a graph. Node can be a queue or topic or relay or event store or other structures. There is no requirement or recommendation of what node must look like. From the point of view of the AMQP it is a message source or sink, the details about design or implementation are not relevant for the protocol. Examples of AMQP nodes are producers, consumers, and queues. Producers and consumers are the elements within an application that generate and process messages. Queues are entities that store and forward messages [1].

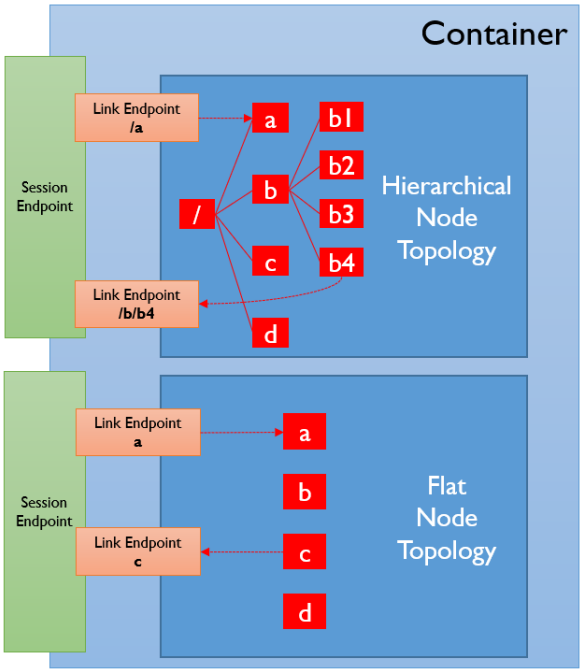


Figure 4.1: Container and Nodes [7]

4.2.3 Connections and Channels

Connections exist between two containers. An AMQP connection is layered over a foundational transport stream, usually TCP is used. TCP is not required though, it could be any protocol that provides a reliable consistent stream of data, so SCTP could be an alternative. Connection at AMQP level provides reliable ordered sequence of frames and negotiates maximum frame size. The management of transfer capacity is very important for constrained devices that are very often used in IoT applications. A maximum frame size - payload size that container is willing to support - is negotiated so that payload does not exceed buffer capacity of devices. Creating AMQP connections is expensive, so the usage of connections needs to be maximized.
Connections also manage maximum channel number. Channel is an independent path through which messages can be send. Channels are used through sessions. Sessions bind two channels together. Client has outbound channel, server has outbound channel. Establishing a session takes two of those channels and binds them together into a bidirectional connection, that is why AMQP is classified as a bidirectional symmetric communication protocol.

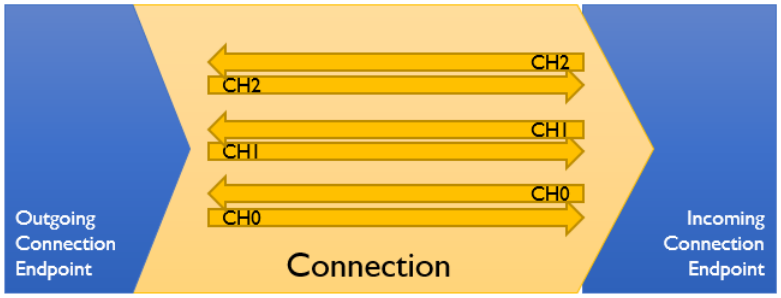


Figure 4.2: Connection and Channels [7]

4.2.4 Sessions

Session exists within a connection and between two containers. It consists of two unidirectional channels bounded together. Session provides a window-based flow control model, i.e. incoming and outgoing window on either side of session that sets limits on how many frames can be handled by the sides. Creating multiple sessions between containers is possible and it allows to have multiple independent passages for frames with different throttling, for example one for regular data and another for high priority data or alerts.

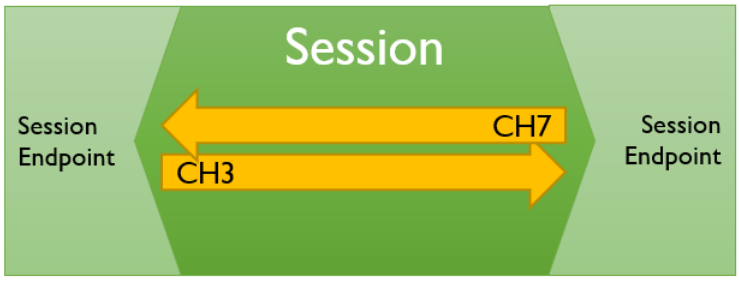


Figure 4.3: Session [7]

4.2.5 Links

Links are used for reliable messaging. They exist between nodes and are formed over sessions. Links are unidirectional for data traffic and bidirectional for flow control data and information about what happens with messages. A session can have any number of concurrent links, links can be initiated in either direction by either peer. Links can outlive collapsed sessions. When a session collapses and new connection is created afterwards, links can be restored and delivery state between those two parties can be recovered.

4.2.6 Frames and Frame Transfer

An AMQP connection consists of a full-duplex, reliably ordered sequence of frames. A frame is the unit of work carried on the wire. Connections have a negotiated maximum frame size allowing byte streams to be easily defragmented into complete frame bodies representing the independently parsable units. The precise requirement for a connection is that if the n-th frame arrives, all frames prior to n must also have arrived. It is assumed connections are transient and can fail for a variety of reasons resulting in the loss of an unknown number of frames, but they are still subject to the aforementioned ordered reliability criteria. This is similar to the guarantee that TCP or SCTP provides for byte streams, and the specification defines a framing system used to parse a byte stream into

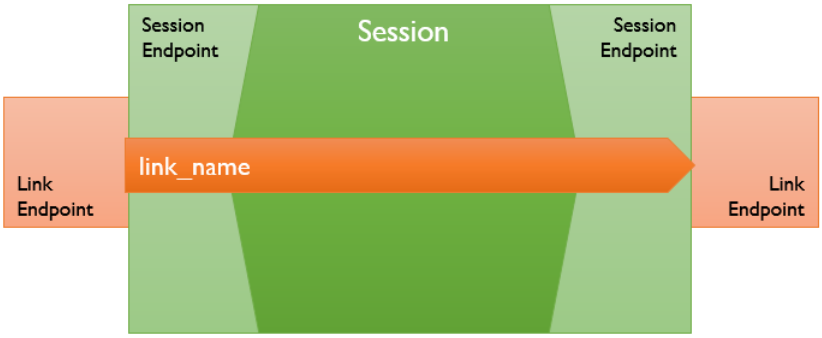


Figure 4.4: Link [7]

a sequence of frames for use in establishing an AMQP connection. An AMQP connection is divided into a negotiated number of independent unidirectional channels. Each frame is marked with the channel number indicating its parent channel, and the frame sequence for each channel is multiplexed into a single frame sequence for the connection. An AMQP session correlates two unidirectional channels to form a bidirectional, sequential conversation between two containers. Sessions provide a flow control scheme based on the number of transfer frames transmitted. Since frames have a maximum size for a given connection, this provides flow control based on the number of bytes transmitted and can be used to optimize performance [1].

4.2.7 Messages and Message Transfer

A single connection may have multiple independent sessions active simultaneously, up to the negotiated channel limit. Both connections and sessions are modeled by each peer as endpoints that store local and last known remote state regarding the connection or session in question. In order to transfer messages between nodes a link needs to be established between the nodes. A link is a unidirectional route between two nodes. A link attaches to a node at a terminus. There are two kinds of terminus: sources and targets. A terminus is responsible for tracking the state of a particular stream of incoming or outgoing messages. Sources track outgoing messages and targets track incoming messages. Messages only travel along a link if they meet the entry criteria at the source. Links provide a credit-based flow control scheme based on the number of messages transmitted, allowing applications to control which nodes to receive messages from at a given point. Sessions provide the context for communication between sources and targets. A link endpoint associates a terminus with a session endpoint. Within a session, the link protocol is used to establish links between sources and targets and to transfer messages across them. A single session can be simultaneously associated with any number of links. Links are named, and the state at the termini can live longer than the connection on which they were established. The retained state at the termini can be used to reestablish the link on a new connection (and session) with precise control over delivery guarantees (e.g., ensuring ”exactly once” delivery) [1].

4.3 Usage of AMQP

AMQP is an asynchronous messaging protocol and provides support for both publish/subscribe and request/response models of communication.

4.3.1 AMQP Use Cases

Simplest use case, where AMQP can be used would be any web service that receives many requests every second, where no request can get lost and all requests need to be processed by a process that is time consuming. If the web service needs to be highly available and ready to receive new request instead of being locked by the processing of previous received requests it is a classic scenario where a queue between the web service and the processing service can be put. The two processes will be decoupled from each other and will not need to wait for each other. The queue will persist requests if their number becomes really huge. Using middleware messaging protocol allows also for easy scaling - all that is needed to be done is to add more workers to work off the queues faster.
In addition to providing a buffer between a web service and another processing service, message queues can be used for more advanced scenarios. The message broker can be configured to route and distribute messages according to different rules and different processes. Messages can be added to different queues depending on how the messages should be handled. The processing systems can then process them at their leisure.

4.3.2 Applications as Middleware

AMQP as a middleware provides a queue for applications to send messages to and to read the messages from. AMQP allows the specification of what messages can be received and how trade-offs are performed with respect to security, reliability, and performance.

4.4 Evaluation of AMQP and Alternatives

Depending on nature of IoT application and its requirements, there are advantages and disadvantages to working with a particular protocol. There are other data protocols that can be used in Internet of Things projects, for example MQTT, CoAP or HTML. Because none of them is able to support all messaging requirements of all types of IoT systems, trade-offs have to be made when selecting appropriate protocol for IoT solution.

4.4.1 Pros and Cons of AMQP

Pros of AMQP A non-exhaustive list of pros of the Advanced Message Queuing Protocol

- AMQP is flexible - it can operate in client/broker or client/server architectures.
- Supports publish/subscribe or request/response abstractions of message exchange.
- It is a very secure protocol, TLS/SSL, IPSec, SASL are supported.
- AMQP provides reliability and allows the user not to worry about the message delivery at all

Cons of AMQP A non-exhaustive list of cons of the Advanced Message Queuing Protocol

- Because of AMQP's support for security, reliability, provisioning and interoperability there is overhead resulting in larger message size.
- Adding middleware layer to projects increases complexity, protocol itself is also very complex.
- AMQP doesn't have significant community, open source projects or contributors.

4.4.2 Available Alternatives

4.4.2.1 MQTT - Message Queuing Telemetry Transport

MQTT is one of the oldest M2M communication protocols, which was introduced in 1999. It is a publish/subscribe messaging protocol designed for lightweight M2M communication in constrained networks. MQTT client publishes messages to an MQTT broker, which are subscribed by other clients or may be retained for the future subscription. Every message is published to an address, known as a topic. Clients can subscribe to multiple topics and receives every message published to the each topic. MQTT is a binary protocol and normally requires fixed header of 2-bytes with small message payloads up to maximum size of 256 MB. It uses TCP as a transport protocol and TLS/SSL for security. Thus, communication between client and broker is a connection oriented. MQTT has three levels of Quality of Service for reliable delivery of messages. It is most suitable for large networks of small devices that need to be monitored or controlled from a back-end server on the Internet. It is neither designed for device-to-device transfer nor for multicast data to many receivers. MQTT supports only publish/subscribe model of communication in comparison to AMQP, which can operate in both publish/subscribe and request/response mode. Thanks to simplicity of MQTT, its message overhead is lower than overhead of AMQP. [5].

4.4.2.2 CoAP - Constrained Application Protocol

CoAP is a lightweight M2M protocol from the IETF CoRE (Constrained RESTful Environments) Working Group. CoAP supports both request/response and resource/observe (a variant of publish/subscribe) architecture. CoAP is mainly developed to interoperate with HTTP and the RESTful Web through simple proxies. CoAP uses Universal Resource Identifiers (URI) instead of topics. Publisher publishes data to the URI and subscriber subscribes to a particular resource indicated by the URI. When a publisher publishes new data to the URI, then all the subscribers are notified about the new value as indicated by the URI. CoAP is a binary protocol and normally requires fixed header of 4-bytes with small message payloads up to maximum size dependent on the web server or the programming technology. CoAP uses UDP as a transport protocol, what causes significantly lower message overhead when compared to AMQP with TCP. As a trade-off, clients and servers communicate through connectionless datagrams with less reliability. However, it uses ”confirmable” or ”non-confirmable” messages to provide two different levels of QoS. Where, confirmable messages must be acknowledged by the receiver with an ACK packet and non-confirmable messages are not. AMQP is more reliable and secure than CoAP, but CoAP uses less bandwidth and less processing power than AMQP, which is important in context of IoT. [5].

4.5 Conclusion

This paper has presented Advanced Message Queuing Protocol in context of usage in Internet of Things. AMQP is an asynchronous messaging protocol, designed to be reliable, secure and configurable. A few other open source data protocols for asynchronous messaging with possible use cases in Internet of Things are available. Choosing one of these protocols for a particular use case should be done while keeping in mind trade-offs that come with the choice. When only energy usage and low overhead for sending messages is relevant, MQTT or CoAP protocols are appropriate choices, but when focus is put on security and reliability, AMQP is a viable choice, providing these features at cost of a slightly bigger message overhead.

Bibliography

[1] OASIS Advanced Message Queuing Protocol (AMQP) Version 1.0 http://docs.oasis-open.org/amqp/core/v1.0/amqp-core-complete-v1.0.pdf

[2] S. Vinoski. *Advanced Message Queuing Protocol* http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4012603

[3] Joel L. Fernandes, Ivo C. Lopes, Joel J. P. C. Rodrigues, Sana Ullah *Performance evaluation of RESTful web services and AMQP protocol* http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6614932

[4] Jorge E. Luzuriaga, Miguel Perez, Pablo Boronat, Juan Carlos Cano, Carlos Calafate, Pietro Manzoni *A comparative evaluation of AMQP and MQTT protocols over unstable and mobile networks* http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7158101

[5] Nitin Naik *Choice of Effective Messaging Protocols for IoT Systems: MQTT, CoAP, AMQP and HTTP* http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8088251

[6] *IoT Standards and Protocols (retrieved 21.05.2018)* https://www.postscapes.com/internet-of-things-protocols/

[7] *Introduction to AMQP 1.0 (retrieved 24.05.2018)* https://onedrive.live.com/view.aspx?resid=123CCD2A7AB10107!732068&ithint=file%2cpptx&lor=shortUrl&app=PowerPoint

Chapter 5

An Introduction to IoT Use Cases With an Evaluation of Integration Possibilities with Blockchains

Anna Götz and Cyrill Halter

Can blockchain technology be used to solve some of the problems present in internet of things (IoT) applications? We approach this question by analyzing specific IoT use cases in the industries supply chain management, agriculture, healthcare and energy. Based on these insights, the benefits of IoT systems are summarized as intelligent monitoring and automated control, which manifest themselves in different ways in each of the exemplary industries. Despite the profits gained from the IoT, certain challenges persist or are newly introduced. We then examine how to solve these problems using blockchain technology. The main finding is that blockchain's greatest asset, the introduction of decentralized trust, can be harvested to improve many IoT applications and solve most of the problems previously identified.

Contents

5.1 Introduction

The Internet of Things (IoT) and Blockchain industries have been growing rapidly over recent years and have become some of the most prominent buzzwords in the information technology (IT) sector. The size of the IoT is estimated to grow to 28 billion installed devices with global market revenue growing to 7.1 trillion USD in 2020 according to an International Data Corporation (IDC) market analysis from 2014 [1]. The IoT is changing large parts of the world we live in, penetrating various industries and finding its way into our homes, our cars and even our bodies. It can be expected that in a few years, every aspect of our lives will be influenced heavily by smart devices. This predicted omnipresence has raised concerns about the security of the IoT. And the threat is real: Past investigations have revealed vulnerabilities in smart devices, such as baby monitors [2] or smart cars [3], that could allow hackers to access the most private data or to manipulate the devices' functionality with dire consequences. The exploitation of security flaws in pacemakers to deliver deadly shocks to its user [4] is perhaps the most striking example for the implications of IoT vulnerabilities. On a wider scale, the Mirai Botnet [5] has shown that IoT security is not only important for individuals, but may be vital for the proper functioning of the entire internet.

While the notion of a cryptographically secured chain of blocks was originally conceptualized in 1992 by Stuart Haber and Scott Stornetta [6], the first blockchain implementation was created in 2008 by an unknown author who goes by the name Satoshi Nakamoto as the public ledger for Bitcoin, a peer-to-peer electronic cash system [7]. Bitcoin has managed to foster a great deal of public attention and, until recently, the number of transactions per month has been growing steadily since its publication [8]. The popularity of Bitcoin has sparked widespread interest in cryptocurrencies and blockchain technology. Modern blockchain systems, such as *Ethereum* or *Hyperledger*, that pave the way for applications that go past the simple exchange of digital currency, continue to be one of the most prominent topics of the IT sector today. Blockchain is viewed as a fundamental technology that will revolutionize many aspects of our lives, such as business, law or government, and is even compared by some to the likes of TCP/IP (transmission control protocol/internet protocol) [9]. While blockchain certainly has revolutionary potential, many are still struggling to identify actual use cases where this new technology is able to facilitate innovation and improvement of the status quo.

This paper will investigate integration possibilities of blockchain into existing IoT use cases and determine its potential to remedy the challenges posed by the unique characteristics of the IoT. In a first step, the IoT industry as well as the latest developments and challenges in the IoT realm will be introduced. Recent IoT use cases will be selected in four different exemplary industries and explained in detail. In a second step the potential of blockchain will be explained and specific challenges for the application of blockchain to the IoT domain will be mentioned. This second step will further consist of an evaluation of the aforementioned IoT use cases regarding the potential for blockchain integration and the elaboration of benefits and drawbacks. A final part will summarize the conclusions that can be drawn from the investigation and will mention areas of interest for future research.

5.2 Terminology

The following section will define the basic terminology and explain the concepts used throughout this paper.

5.2.1 Internet of Things

Various definitions of the *internet of things* (IoT) have been made over the years with varying degrees of abstraction. For the purposes of this paper, we will define the IoT according to [10] as *"[...] a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies."* Figure 5.1 shows the new dimension, *AnyTHING communication*, added to the information and communication technologies by the IoT.

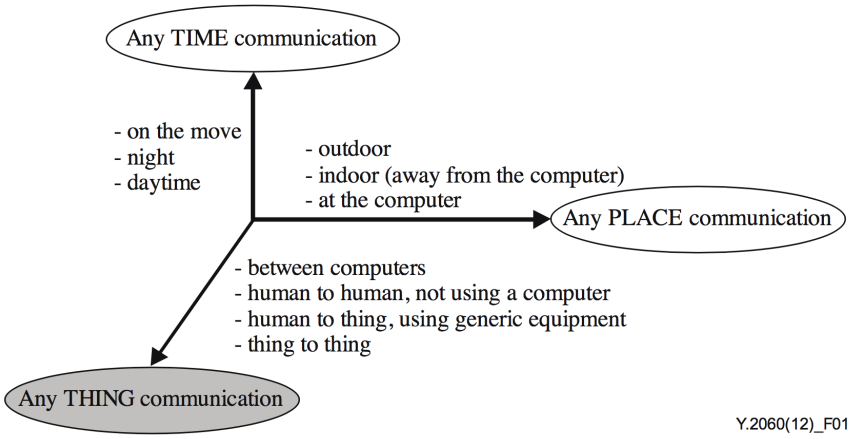


Figure 5.1: The new dimension added to the information and communication technologies by the IoT [10]

5.2.2 Blockchain

The term *blockchain* refers to a distributed ledger technology that through its extraordinary architecture is able to provide decentralization, persistency, pseudonymity and auditability [52]. In blockchains, all transactions are stored in a sequence of blocks. Each block consists of a block header, that includes a reference to the previous block in the form of a parent block hash, and a block body containing a list of transactions (see Figure 5.2). In this distributed system, every user can obtain a copy of the complete blockchain. The state of the blockchain is verifiable at any time thanks to the consecutive hashing of parent blocks.

A user who wishes to include a transaction into the blockchain can submit it into a transaction pool. The blockchain then determines who will process the transaction using a distributed consensus algorithm, such as *Proof of Work* or *Proof of Stake*, that varies with the blockchain implementation, and distributes the processed block to the entire network. Once a few blocks have been added to the blockchain on top of the one containing the transaction, it is immutably persisted with a very high probability [52].

There are further differences between different blockchains apart from the algorithm used for consensus determination [52]. In *public* blockchains, each node in the network may take part in the consensus process and the entire blockchain is accessible to everyone. *Consortium* blockchains are partially centralized (controlled by a set of organizations)

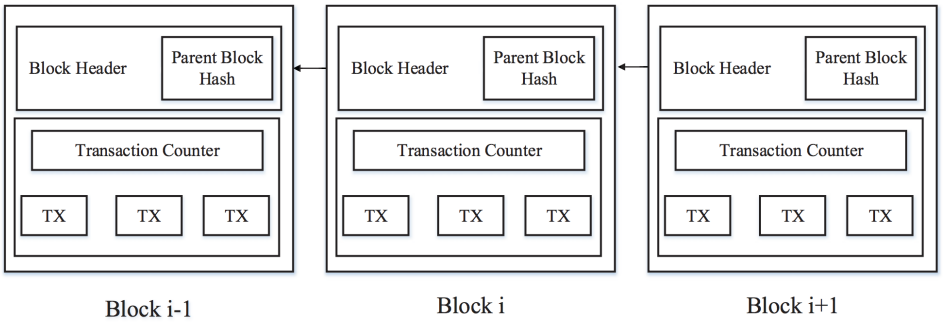
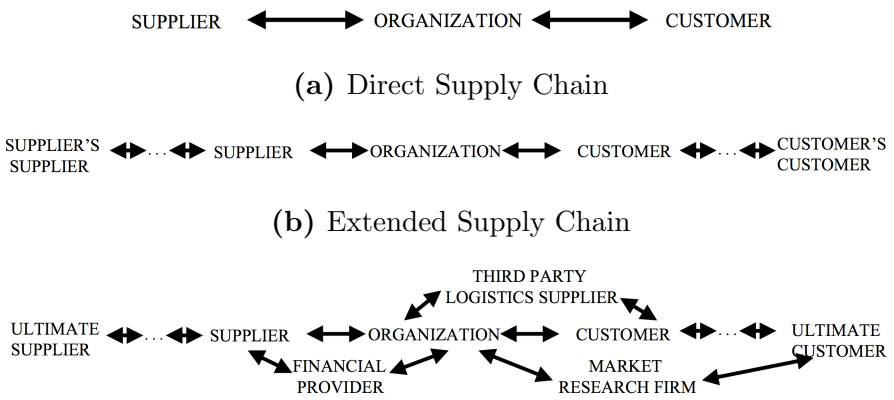


Figure 5.2: A blockchain consisting of a sequence of blocks [52]

and limit consensus determination to a selected set of nodes. While this impairs the immutability of the processed blocks, it is computationally much more efficient than the public approach. They may also have restrictions on the access to the data contained in the blockchains. Finally, *private* blockchains are fully controlled by a single entity. They can theoretically be tampered with easily and very active discussions are being held today whether they bring any advantages over conventional database solutions.
Blockchains differ further in their ability to process complex computational tasks. While the original *Bitcoin* blockchain was intended purely to process transactions of digital currency, more recent systems like *Ethereum* include Turing complete scripting languages that allow users to attach logic to their transactions. These programs called *smart contracts* may, for example, withhold a payment until some condition is met. The applications are endless.

5.2.3 Supply Chain Management

The term *supply chain management* is ambiguously defined in literature. For the purposes of this paper, we will refer to the separate definitions for *supply chain* and for *supply chain mangement* given in [11]. A **supply chain** is therefore defined as "*a set of three or more entities (organizations or individuals) directly involved in the upstream and downstream flows of products, services, finances, and/or information from a source to a customer.*"
The three entities mentioned in this most basic case of a *direct supply chain* are an organization, a supplier and a customer. It should be mentioned, however, that supply chains can become far more complex. Mentzer et al. coin the terms *extended supply chain* and *ultimate supply chain* to describe more sophisticated versions of a supply chain that include extended and intermediate customers and suppliers (see Figure 5.3). Supply chains exist in all businesses, whether they are managed or not.
The term *supply chain management* involves various different dimensions and perspectives. Mentzer et al. evaluate these points of view in [11] and come to the conclusion that **supply chain management** is "*the systemic, strategic coordination of the traditional business functions and the tactics across these business functions within a particular company and across businesses within the supply chain, for the purposes of improving the long-term performance of the individual companies and the supply chain as a whole.*"
Supply chain management is therefore a process that involves several different entities from different corporations and different parts of corporations that manages goods along the supply chain with the ultimate goal of customer satisfaction, value, profitability or a competitive advantage.



(a) Direct Supply Chain

(b) Extended Supply Chain

(c) Ultimate Supply Chain

Figure 5.3: Types of Supply Chains [11]

5.2.4 Agriculture

According to the United States Department of Agriculture, agriculture is defined as the *science or practice of farming, including growing crops and raising animals for the production of food, fiber, fuel and other products.* Nowadays, farming has become increasingly complex, and it is useful to have a closer look at some specific concerns of today's agricultural research [12] [13]:

- *Selection of Crops and Animals*: Different species flourish in different conditions. Selecting the one suitable for the local climate and conditions is crucial for maximizing the output.
- *Equipment*: With an increasing world population that needs to be fed every day, producing a large amount of food is crucial. Farms tend to get bigger and require equipment that is able to operate on a large scale. With the right equipment, human labor can also be reduced.
- *Soil*: The branch of agricultural science concerned with the soil is mostly interested in its fertility properties as well as how it influences plants and animals. The reduction of pests is another important factor in this branch of agricultural science.
- Food Lifecycle: Once the food has been collected from the farm, the biggest concern is to prepare it for and get it to the consumers as soon as possible (processing, packaging, delivering).

5.2.5 Healthcare

Healthcare is *a summarizing expression that refers to all products and services related to health and medical care.* The healthcare sector, therefore, includes a number of separate industries, a few of which shall be mentioned here [14]:

- *Pharmaceuticals*: The pharmaceutical industry includes pharmaceutical manufacturers, as well as biotechnology firms that engage in research for and development of new pharmaceuticals.
- *Medical Equipment*: Medical equipment manufacturers distribute a wide range of medical devices, ranging from simple products, such as scalpels or stethoscopes, to highly complex machinery, such as MRI machines or surgical robots.

- *Managed Healthcare*: The managed healthcare industry mainly includes insurance companies that provide insurance for health related costs to its customers.
- *Healthcare Facilities*: Healthcare facilities include hospitals, clinics, labs and nursing homes. They may be separate corporations or may be operated by overarching healthcare facility firms. This sector includes the medical services that can be received in said facilities.

5.2.6 Energy

The energy sector concerns itself with producing and supplying energy [15]. It is usually categorized by energy sources. The main ones are the following [16]:

- *Coal*: While the production of coal has declined drastically in recent years, it continues to supply a large amount of the world's energy.
- *Oil and Gas*: The industry also still heavily relies on oil and gas, the other two main fossil energy sources.
- *Nuclear Reactions*: Despite major protests, especially Asian and Middle Eastern countries are increasing their nuclear power output.
- *Renewables*: Wind, sun, water and others are the energy sources of the future, not least because of their steadily decreasing cost.

5.3 IoT Use Cases

The following section will explain real world use cases of the IoT. The importance of the IoT will first be mentioned and some challenges hindering the further development of the IoT will be described. Practical IoT use cases will then be illustrated in the four exemplary industries supply chain management, agriculture, healthcare and energy. Further, opportunities and challenges will be listed for each industry.
While the number of connected IoT devices has not been increasing as rapidly as suggested by early estimations, growth has nevertheless been the main trend in the IoT industry over recent years. 2017 marked the first year where the number of connected IoT devices surpassed that of PCs, laptops, tablets and smartphones. At the same time, the interest in the IoT has remained stable and high throughout 2017. IoT startups continue to raise massive amounts of funding, most significantly Uptake, who closed two funding rounds in 2017 for a total investment of 207 million USD [17]. These numbers make clear that the IoT has gained global relevance and that it is slowly moving from hype to reality.
There are still some questions that remain to be answered for the IoT to experience the explosive growth that was originally predicted for it in early estimations, such as 2011's Ericsson report [18]. The following is a list of challenges that the IoT faces to reach widespread adoption and acceptance [19]:

- *Data Management and Mining*: IoT sensors and devices are already generating immense amounts of data and will produce even larger data volumes with the growing amount of hardware in use. The storage and processing of this data may overstrain existing data centers. In addition to this, IoT data may be unstructured and consequently hard to understand. Its analysis and the extraction of useful information will pose a challenge for big data analysts for years to come [19].

- *Security and Privacy*: Security is a topic that has been neglected for a long time during the early days of the IoT. The growing number of connected devices and the advancement of the IoT into every aspect of our lives has exacerbated the threat posed by an insecure IoT. The topic is complicated by its unique characteristics: Devices have limited resources and operate in an unattended, often wireless environment. Security must therefore be addressed carefully for every part of a thing's lifecycle. Furthermore, the fact that IoT hardware may be used to control physical infrastructure increases the potential for harm. So far, there has been no agreement on standards or regulations in the IoT industry, making security decisions difficult for both consumers and developers [19].
  Privacy concerns have been sparked by the vast amounts of personal data that can be recorded by the IoT. This does not only concern the theft of data by malicious actors but also the sale of data by IoT device manufacturers. A solution to this problem is difficult to find since the sale of data is at the core of many IoT companies' business model [19].

- *Chaos*: The development of the IoT is happening at a much higher pace than the typical consumer product innovation cycle. This has led to the rollout of many often poorly tested products that do not satisfy the standards have been established in other industries. The challenges mentioned above can be attributed in part to this issue. In a hyper-connected world, a small error in a subsystem may lead to widespread chaos through a chain reaction. The solution to this problem demands high effort to reduce the complexity of IoT systems, to enhance the standardization and to guarantee the security and privacy of users at any time [19].

5.3.1 Supply Chain Management

The emergence of the internet has changed the way that supply chains operate in today's economy. The developments that it provoked can be summarized in the following key expressions [20]:

- *Globalization and Outsourcing*: Companies are no longer independent entities. Instead, they operate in a network of businesses on a global scale in a collaborative effort to create value.
- *Stock Keeping Unit (SKU) Proliferation*: Companies no longer sell just a single pre-configured product but offer an immense range of options and customizations to their clients in order to meed their individual needs as closely as possible.
- *Shorter Product Lifecycles*: The lifetime of the products offered by companies to their clients is getting steadily shorter as businesses try to meet an increasingly volatile demand and increase their profit margins.

These developments have led to new requirements for speed and flexibility. The IoT promises to help businesses meet these requirements by improving the efficiency and effectiveness of today's supply chain, providing up to 15% increase in productivity in delivery and supply chain performance [21].
[22] lists some of the key trends of the supply chain industry in 2017, two of which are closely related to the IoT: Warehouse robotics are steadily driving forward the automation of the warehouse and are converting it into a purely digital system with only minimal human interaction. Chinese e-commerce giant Ali Baba has recently managed to reduce the human workforce in one of its storage facilities by 70% through the use of smart carts that are able to move shelves through the warehouse and bring them to human packagers. Autonomous road transportation has been a popular topic for a while and is already a reality in some isolated industries, such as Western Australia's mining industry. While still struggling with legal and social issues, this development has already advanced fairly far from a technical standpoint, and will drastically reduce transportation costs in the future.
IoT integration opportunities into supply chain management applications can be categorized based on [23]:

- *Purchasing*: Once fully developed, the IoT is able to provide ubiquitous information about any part of a supply chain. This enables companies to gauge the state of any object to be purchased and, therefore, make better procurement decisions.
- *Fabrication*: Real-time monitoring of production through smart sensors in fabrication facilities can allow businesses to optimize their manufacturing procedures and to recognize defects early on resulting in a more efficient and more reliable fabrication process.
- *Transportation*: Smart trackers and sensors can provide a wide range of information about objects in transit including the location of products, as well as ambient conditions, such as temperature or pressure. This leads to greater transparency, controllability and predictability of the supply chain.
- *Storage*: Smart tags and sensors on stored objects, as well as robotic assistants for human warehouse employees can help to increase efficiency as well as warehouse capacity. In addition to this, the storage conditions of the stored products can be tracked and their quality can be assured.

Even with well-thought-out solutions in place, there remain some challenges for IoT-assisted supply chain management systems. These relate mostly to the *Security and Privacy* and the *Data Management and Mining* problems for the IoT mentioned earlier in this section [24]:

- *Trust*: For different enterprises to be able to collaborate in a shared supply chain, each on of them must be able to trust in the truthfulness of the information shared by another. The data must be assumed to be correct and untampered with. Today, this may happen on a bilateral or on a legal basis.

- *Reconciliation*: For many of today's systems, it is difficult to achieve true end-to-end integration. This is due mostly to the fact that there are only very limited standards in place. To exploit the true potential of the IoT in the absence of standards, custom tailored solutions have to be built, which is very costly.

- *Effectiveness of the Lowest Common Denominator*: The effectiveness of the end-to-end supply chain information flow is limited by the effectiveness of the weakest link in the IoT solution implemented to support it. Given that not all contributors to said information flow may be trustworthy, this could also be called the most "wicked" link. One node in the network not correctly recording, processing or passing on information may be enough to severely impair the operation of the entire system.

5.3.2 Agriculture

The agricultural sector has seen tremendous changes in recent years, many of which are related to the emergence of new technologies. About 40 years ago, farms tended to be quite homogeneous in terms of size. Nowadays, we can observe a number of small, local farms who emphasize their focus on high quality products, but we also see mass production in ever-growing large-scale farms [25]. Naturally, the maintenance of large farms comes with a certain overhead. This overhead has created opportunities for technological improvements to establish themselves in the agricultural sector.
[49] has identified two main applications of IoT applications in agriculture:

- *Intelligent Monitoring*: Intelligent or distant monitoring relies on sensors installed throughout the farm. Numerous aspects that influence the wellbeing of the plants or animals can be recorded and transmitted to the farmer, who gets access to the data through a (smartphone) application. Graphs can show trends over time, and the user can be alerted if a certain pre-defined threshold of some value is reached.

- *Automatic Control*: As was established before, the number of large-scale farms has increased. As a consequence, the number of potential observations from the Intelligent Monitoring increased as well. This introduces a challenge for the farmer who has to monitor all aspects. Automatic control takes some of this burden off the farmer's shoulders by acting autonomously. Instead of just sending a notification if a certain threshold is reached (e.g., the soil moisture is too low), the system can follow through with an appropriate action (e.g., watering the plants).

Diving deeper into how Intelligent Monitoring can be applied in agriculture, consider the following use cases:

- *Temperature, Humidity and Illumination Monitoring*: The most basic factors that influence plant growth are temperature, humidity and illumination. It is essential to find the right balance between these factors. Naturally, they are a good starting point for any IoT system in agriculture in order to uncover inefficiencies and

maximize productivity and profitability [28]. With the appropriate sensors, many more aspects can be monitored, for example the nutrient content of the soil or the amount of wind the plants are exposed to.

- *Pest Detection*: Advanced sensors combined with cameras and image processing allows the farmer of today to detect weeds as well as harmful insects that might damage plants. This is extremely beneficial as pests are the most destructive force when it comes to plant survival [29].

- *Animal Monitoring*: Just like the bodily functions of humans can be monitored, which is the basis of many fitness applications that have emerged in recent years, health data of animals can be recorded as well. This allows faster identification of diseases in livestock and the potential to fight them before they spread [27].

- *Vehicle and Equipment Tracking*: Via GPS sensors, the location of farm vehicles and equipment can be tracked. This is especially powerful when combined with autonomous vehicles such as drones. It can ensure precise coverage of a field during ploughing, planting, watering, fertilizing etc. [26].

In order to make use of the data collected during the *Intelligent Monitoring* phase, they have to be transmitted to the person in charge, usually the farmer. The transmission occurs via a wireless network with the destination of a central base station responsible for data collection [28]. The farmer can then access the data via a desktop or smartphone application. Due to the fact that sensors record a huge amount of data over time, data processing is necessary to provide the data in a presentable format, for example graphs. In a first step of IoT implementation into the agricultural sector, the farmer would then use the collected and transmitted information to plan her actions, for example fertilizing the crops or examining the sick animal. With a more advanced IoT system, the effort required from the farmer in this phase is reduced by *Automatic Control*. Instead of physically being present in the location where the task is to be carried out, the farmer can initiate actions directly through the (smartphone) application. In practice, the following use cases can be envisioned:

- *Substance Distribution*: Once a dry area or a part of the field lacking nutrients has been discovered, water or fertilizer can be applied automatically to the affected area. First, this practice saves the farmer valuable time. Second, it can aid in decreasing the energy consumption involved in the process by activating a drone to carry out the task rather than requiring the farmer to take the tractor to the respective location.

- *Pest Elimination*: With the data from the *Pest Detection* and the help of drones or stationary equipment, weeds can be removed automatically. The machines are sophisticated enough to only attack weeds and to do so in a way that does not damage the crops, for example by pulling too hard or removing plants from a too large area.

- *Environment Manipulation*: This general area includes aspects such as opening stable windows or doors, turning on or off various devices or manipulating the state of any other physical object. The triggers for such changes are as diverse as the manipulations themselves, ranging from changed animal health data to weather changes that make the use of a heating system redundant.

Despite these valuable advancements in both *Intelligent Monitoring* and *Automated Control* with IoT technology, some issues the agricultural sector is facing are beyond the capabilities of IoT technology or at least the current implementations of it. Other challenges

were only introduced with the use of IoT technology. The following list is a summary of both categories of problems:

- *Food Waste*: With the agricultural sector having to provide food for roughly 9.6 billion people in 2050 [30], it is essential to keep food waste to a minimum. [30] has identified the major areas of food waste and has found that it greatly differs between developing and developed countries. In the former, shortcomings in on-farm practices, transport and processing account for around 80% of the wasted food. This includes pest infestation, the lack of proper storage facilities and the absence of a thought-out food chain.
  On the other hand, the main reason for food waste in developed countries is careless behavior of the consumers and its effects on retailers. The majority of consumers only buy spotless fruits and vegetables, which leads to the fact that retailers dispose of food before the consumers even get a chance to buy the less than perfect products. Because food is quite cheap in developed countries, people's inhibitions to throwing away food are rather low, so products that are suddenly unwanted because the people "just don't feel like eating them" at the moment or food items that have barely surpassed their "best before" date but are still edible end up in the trash. Local, small-scale farming could be the solution but is unfortunately often hindered by too high costs compared to big retailers who benefit from economies of scale or problems with payment terms [31].

- *Trust in Certification Compliance*: Food certifications were established to prove to the consumer that the food is truly bio, organic, local, vegan, halal etc. While farmers and other food processing organizations have to fulfill strict requirements in order to get certified and are also regularly tested in order to stay certified, it is infeasible to test every single fruit, vegetable and piece of meat. While IoT devices are capable of capturing nutrient, temperature and processing data that could give insight to the consumers about whether an agricultural product complies with the regulations of a certain qualification, such systems are complex and there currently exists, to the best of our knowledge, no platform to provide such data to the consumers. Additionally, even if such a system existed, it would be prone to data falsification.

- *Restrictions on UAVs*: Unmanned aerial vehicles (UAVs), also known as drones, can play a huge role in farm automation as mentioned in the use cases of *Automatic Control*. However, as described in the *Chaos* section, IoT devices that do not adhere to common standards have flooded the market. Consequential complaints about UAVs related to privacy concerns have led the US Congress to release the Federal Aviation Administration Modernization and Reform Act (FMRA) in 2012 [32]. Because a solution to the privacy problem needed to be found fast and probably also because of a lack of expertise on the different applications of drones on the side of the lawmakers, the FMRA is quite restrictive when it comes to commercial uses of UAVs. For example, it prohibits the commercial use of UAVs during nighttime without regard to the fact that certain agricultural operations are better carried out at night (e.g., watering) or are even only useful at night (e.g., deterring nocturnal animals from destroying the crops).

5.3.3 Healthcare

The healthcare industry of the future is facing a number of issues. The world's population is aging rapidly. Predictions show that by 2050, one out of five people may be of age 60 or older [33]. Since age is directly correlated with a higher occurrence of health problems,

the healthcare industry is confronted with the problem of sustainability in the future. The younger population, on the other hand, sees itself dealing with increasingly busy work schedules and is thus reluctant to address health problems and to concentrate on a healthy lifestyle. With these issues among others, the healthcare industry has been looking for ways to increase its efficiency and effectiveness. The IoT is credited with great potential to provide solutions for some of these problems, promising lower expenses, better treatment results and disease control, reduction of mistakes and more [34]. In this context, it is not surprising that the global IoT healthcare market is estimated to grow by around 400% from 2015 to 2020 [35].
Recent years have seen growing acceptance towards IoT applications in healthcare. In 2015, Swiss health insurance provider CSS launched a program for premium reduction based on the number of steps recorded using a wearable step counter, following an international trend in the insurance industry [36]. The approval of the first smart pill, an ingestible device containing sensors and wireless communication equipment, by the American Food and Drug Administration (FDA) in late 2017 marks another milestone in the integration of the IoT into healthcare [37].
A wide range of use cases exist for the IoT in the healthcare industry. They will be categorized here based on [33]:

- *Personal Health Monitoring*: Wearables provide promising opportunities for the monitoring of personal activity, as well as other health related data, that could benefit healthcare practitioners significantly in their ability to make accurate diagnoses and to discover the root cause of medical problems. The fact that this potential is recognized by both the healthcare industry, as well as the IT industry is illustrated best by the publication of Apple's HealthKit [38] and ResearchKit [39] frameworks with the release of the Apple Watch. These two frameworks enable developers to create applications for medical monitoring and research using data from the Apple Watch's sensors. The extensive data that can be captured with wearables offers many new possibilities for telemedicine (the remote treatment of patients), the detection of medical emergencies, preventive diagnostics and more [33].

- *Drug Prescriptions*: Medical mistakes can be fatal. A large part of the errors that happen in the medical industry are due to faulty drug prescriptions. The IoT could help mitigate this issue through the usage of RFID tags on pharmaceuticals. The electronic representation of a pharmaceutical could then be connected to a unique electronic identity of a patient. Like this, the handing out of the wrong medicine in a pharmacy could be avoided [33]. Other prescriptions that are connected to the patient ID could also be checked automatically for interferences. On the patient side, problems exist mostly with drug adherence. Patients may forget to take a drug or take too much of it. Here the IoT could help, for example, with smart pill boxes that automatically dispense the correct amount of medicine and remind the patient to take a prescribed pill [40].

- *Support for People with Disabilities or Health Problems*: The IoT has the ability to assist and support disabled or impaired people to achieve a higher quality of life. A smart navigation device, for instance, could help a blind person find his way through a city when his known route is blocked. A smart wheelchair may be able to detect low battery levels and automatically search for a charging station in the user's proximity.

- *Assistance for Emergency Situations*: In medical emergency situations, rapid response is critical. The IoT has the ability to reduce the time until a patient experiencing some sort of emergency is helped and medical experts arrive at the scene.

Some systems in this area are already broadly deployed. Numerous elderly people that live alone wear a bracelet that enables them to contact family or friends should they fall down without the ability to get back up by themselves [41]. Smart defibrillators that guide helpers through the process of reanimation and automatically contact emergency medical services are another example that is in use today.

- *Medical Device Sharing*: Medical equipment is notoriously expensive and contributes a significant part to high healthcare costs. Equipping devices with RFID tags and using smart logistics algorithms could help hospitals reduce the amount of devices in circulation and consequently reduce the cost of treatments.

- *Medical Supply Chain*: The medical supply chain is especially sensitive. Pharmaceuticals often have to be transported in temperature controlled environments. Problems with fraud are also frequent in certain areas. The application of sensors and RFID tags can help to deal with these issues. The topic of supply chain monitoring is discussed further in Section 5.3.1.

Smart medical devices have already found their way into our daily lives. Implanted devices like pacemakers can form wireless connections for administration purposes and automated insulin pumps provide relief for diabetics across the world. For the IoT to justify its presence and to unleash its full potential in the healthcare industry, however, there remain some concerns that need to be addressed relating mostly to the *Security and Privacy* problems mentioned at the beginning of this chapter [42]:

- *Security*: IoT applications in healthcare must above all be secure. The discovery and exploitation of vulnerabilities by a malicious actor seldom has more drastic consequences, potentially leading to the death of numerous patients. This may be the case, for example, if an implanted pacemaker is hacked and modified to misbehave. This poses great technical challenges to IoT architects and, since no solution is ever completely secure, a moral dilemma. So far, security issues have been ignored to a large degree.

- *Loss of Privacy*: The information used by the healthcare industry is perhaps some of the most private that people ever give away. The protection of that privacy is therefore essential for the acceptance of IoT applications in healthcare. In many countries, the protection of patient data is even mandated by law (doctor-patient confidentiality) and is thus a prerequisite for the deployment of any IoT solutions for healthcare.

- *Trust*: Trust is a delicate issue in two areas. First of all, the integrity of the data delivered by IoT devices must be trustworthy. Corruption of or tampering with said data during recording or transmission may be disastrous since it may be used as a basis for life and death decisions. Second of all, the implementation of IoT solutions for healthcare may also be hindered by the lack of interpersonal trust that exists between patient and doctors, nurses or other medical personnel.

5.3.4 Energy

As already defined above, the energy sector has two main tasks – producing and supplying energy. Until recently, these tasks were accomplished with a simple electric grid. It is defined as "a network of transmission lines, substations, transformers and more that deliver electricity from the power plant to your home or business" [43]. While "simple" might be a misleading attribute for such a complex system, it is, in fact, much simpler than the newest development in the energy sector – the smart grid. What makes a grid smart

is the "two-way communication between the utility and its customers" as well as sensors integrated in the process of energy transmission [43].
This is where IoT technology comes in. All our devices – heaters, fridges, lights, TVs, computers, kitchen and bathroom appliances and so on – rely on energy. Another aspect that all these devices have in common is that they can be equipped with different kinds of sensors and actuators, either for measuring energy use or for controlling their behavior. While this example only highlights the opportunities of smart grids in energy consumption, the benefits already start much earlier at the stage of electricity generation [45].
We identified the following IoT use cases in the energy sector across all stages of the energy lifecycle:

- *Remote Monitoring and Control*: Energy generation is usually a quite scattered endeavor, whether it is offshore oil pumping or solar panels and wind turbines spreading across vast pieces of land. Therefore, monitoring and maintaining these facilities is often challenging. With IoT technology, all data is gathered in a control center as [44] describes for the oilfield industry. Incoming data from sensors capturing temperature, pressure, flow rate, equipment load and other measures are automatically monitored and used as input for automated maintenance.

- *Detection of Disturbances*: As a result of the previous use case, IoT enables timely detection of disturbances in a thing's operation. Starting from the energy generation stage, malfunctioning of a wind turbine, for example, can be detected by monitoring the amount of energy produced by each turbine and comparing the data. If the value is significantly lower for a certain turbine, it is likely that it is malfunctioning. Changes in productivity might happen continuously over time, making it hard to detect for a human. Big data processing of the collected sensor data is one step ahead and can alert the operators in case of a downward trend.
  The same method is feasible in the energy consumption stage. A refrigerator that slowly consumes more and more energy might need to be de-iced or cleaned. Continuous monitoring of energy consumption combined with early alerts can therefore even help save energy and consequently drive down costs.

- *Smart Pricing*: In a very limited sense, smart pricing has been in place for many years – energy providers charge more for the same amount of energy during the day as compared to during the night. However, as in all fields, the price should be determined by supply and demand if one strives to achieve an economic equilibrium. Simple day-and-night distinction might be a good approximation in many cases, but it is certainly not optimal. In a smart grid where the energy consumption of all households is monitored, new opportunities arise. If the real-time consumption is known at all times, the energy price can be optimized in terms of supply and demand. Whether this model is indeed optimal, all things considered, and what legal restrictions there might be is a whole different topic that needs to be addressed before implementing such a system.
  With a smart pricing model, there is also the potential of saving cost on the side of the energy consumers. One has to distinguish between deferrable and non-deferrable electrical appliances [46]. Non-deferrable appliances must have access to energy either at all times (refrigerator, heater) or at least at any time the consumer desires (lighting devices, stoves). Deferrable appliances, on the other hand, can defer their operation. Washing machines and (robotic) vacuum cleaners fall into this category – their functioning is usually not time-critical. This is where the cost saving potential comes in. If the deferrable appliances are programmed in a way to run only when energy prices are low, the costs are minimized.

- *Environment-Informed Behavior*: Energy waste is huge – so huge that it costs U.S. businesses and households an estimated $130 billion per year [47], let alone the unquantifiable negative impact on environmental health. IoT technologies are a powerful weapon in fighting this energy waste. Ideally, devices only operate when they are needed based on the current state of the environment. Different types of sensors such as those sensing lighting, temperature, motion and many other aspects of the environment can identify when certain devices are needed. In an ideal setting, air conditioning units stop once the outside air cools down naturally and the windows are opened instead; lights dim as it gets lighter outside, or they switch off completely if the respective room is empty; TVs, radios and other devices turn off if nobody is attending to them.
  One important aspect to consider when designing these environment-informed systems is that they must not consume a lot of energy themselves. Otherwise, the energy savings on the side of the regular household systems are quickly counteracted by the energy consumption on the monitoring and control side.

Despite the many benefits IoT technology can bring to the energy sector, some challenges remain.

- *Single Point of Failure*: Modern societies rely heavily on the electrical grid. From heating to water purification to food cooling – many aspects of modern life people take for granted require energy. When introducing the smart grid, one therefore has to be extremely cautious not to introduce any vulnerabilities with it. However, no matter the caution, a smart grid is a central, internet-based system by nature and therefore a single point of failure [60].

- *Mismatch of Energy Production and Consumption*: In an ideal world, energy is always produced right when and where it is needed. Clearly, this scenario is utopian. For this reason, energy storage systems have long been in place. However, current energy storage solutions are costly and not flexible enough for the present and future power network situation [48].

- *Lack of Consumer Choice*: Since the global electricity market is controlled by a few big players [50], energy consumers' options are limited. A person who wants to rely on clean energy, for example, must either put a lot of effort in the search for a suitable energy provider or will never even find a provider that completely satisfies her expectations.

5.4 Blockchain Integration Possibilities

This section will highlight the most promising aspects of blockchain technology. Focusing on the IoT, we will examine how blockchain architectures can be optimized in this area and what the related challenges are. Specifically, this section will focus on the sectors supply chain management, agriculture, healthcare and energy and address the current challenges in these industries presented in the chapter *IoT Use Cases*. The goal is to investigate in which of these use cases blockchain can provide a benefit.
The revolutionary idea behind blockchain technology is that of decentralized trust. In the past, a commonly trusted intermediary, like a bank, had to be included in any transaction. With a blockchain, mutual trust can be established without an intermediary. The reason for this lies in the immutable nature of a blockchain – information stored within is tamper-proof [52]. This does not mean that it is impossible to alter the data. In fact, each node has to be able to make changes to propose a new transaction. However, all changes are validated by the other nodes before they are added to the blockchain. Manipulated data will never be accepted; therefore, a potential fraud would quickly be discovered and the discredited, manipulated information would not be distributed to the other parties. In this brief summary as well as throughout the entire paper, public blockchains are considered unless mentioned otherwise.
While blockchains can be applied to many different fields and have some common benefits as well as challenges in each of these, some are also specific to the respective field. For the IoT as a very broad field, the advantages blockchain technology may yield can be summarized as such:

- *Secure Records*: Whether it be physical items whose presence is detected or more abstract information collected by sensors or actuators, all steps along the way are recorded. More than that, they are recorded in a secure manner because the individual pieces of information corresponding to the observed states are stored in a tamper-proof blockchain.

- *Trust in Devices*: Before a secure record is even useful, it needs to be ensured that the data submitted by the device to the blockchain actually depicts reality. Otherwise, the data is not worth anything. This, in turn, can be ensured by blockchain technology. The device configuration is stored in a blockchain as it is released by the manufacturer. Any alterations to the software or settings are recorded, in which case the IoT device is not allowed to contribute its recorded data anymore [53].

- *Increased Autonomy*: To this point, IoT devices have mostly been used for simple recording and acting in non-critical situations. However, with smart contracts based on blockchain technology, devices could gain more autonomy even in critical situations [51].

- *Eliminated Single Point of Failure*: The fact that IoT devices generally rely on a centralized cloud makes them extremely vulnerable. The malware Mirai exploited a related vulnerability with the consequence of affecting numerous devices, even those beyond the IoT. A decentralized, blockchain-based system could mitigate this problem [53].

While blockchain technology gained popularity with Bitcoin, there are many different blockchains available by now – Ethereum, Hyperledger, Ripple, Quorum – just to mention a few. Although they share a basic concept, they focus on different areas. Without going too much into detail, we would like to point out that the choice of blockchain can have a big impact on the success of an implementation. For applications related to the IoT, it is crucial to choose a blockchain that is less resource-intensive than common blockchains

because the IoT devices are limited in their capacities [54]. The industry has already picked up this need as we see, for example, in the implementation of the IoT Chain (iotchain.org). Even beyond IoT, it is important to tailor the blockchain architecture to each specific use case.

5.4.1 Supply Chain Management

The following will address the challenges mentioned in Section 5.3.1 and detail the potential of blockchains to provide solutions.

- *Trust*: The trust concerns in IoT SCM systems can be addressed by storing data recorded by smart sensors in a blockchain. The distributed nature and the cryptographic hashing algorithms of a blockchain ensure that the records are tamper-proof and proves their authenticity and provenance [53]. The storage of device configurations in the blockchain, as described in [58] or [53], can provide additional assurances for the trustworthiness of supplied information. Using these methods, both the method of recording data, as well as the data recorded are public information shared between all entities involved and cannot be changed or manipulated by any single actor.

- *Effectiveness of the Lowest Common Denominator*: Other than conventional centralized database solutions, blockchains are distributed by nature. The usage of blockchains as a data backend eliminates a single point of failure in an SCM system since both the stored data as well as the nodes running the blockchain are highly redundant, making a failure very improbable [53].

- *Reconciliation*: End-to-end integration requires a common data backend. A public blockchain has the benefit of already being universally accessible for anyone with an internet connection and distributed over thousands of devices while conventional database solutions have to be set up and managed accordingly, a labor intensive task. In addition to this, they provide other advantages, as is described earlier in this section makes them a viable candidate to fulfil this task[53].

SCM often serves as a prime example for both IoT and blockchain use cases and it can also serve as one for the integration of both. The requirement for trust in the multi-party, multi-step supply chain process, that remains unsolved even with well thought out IoT systems in place, can be addressed well using a blockchain solution. Large parts of the information shared in SCM, such as the provenance of items or the manufacturing data, is already public today (or should be public). Privacy, blockchain systems' main shortcoming, is therefore less of an issue than in other industries. If the shared information must be protected, a supply chain would allow for the application of a semi-private blockchain which is operated by a consortium of all the multiple parties involved and not controlled by a single entity [55].

5.4.2 Agriculture

This chapter will revisit the challenges presented in Section 5.3.2 and show how blockchain applications can mitigate some of them.

- *Food Waste*: Although the reasons for food waste in developing and developed countries are quite different as we identified before, blockchain offers a solution that is beneficial in a variety of problematic situations. The way this is achieved is by establishing a decentralized food marketplace that allows consumers to buy directly from the producers. Blockchain facilitates this marketplace because it provides

decentralized trust and secure records as discussed above. As [57] and [59] showed for decentralized marketplaces in general, the blockchain approach results in reduced processing time, lower cost of goods and no transaction fees. In a food marketplace, especially the lower processing time is crucial. Developing countries benefit because of the reduced need for storage facilities. In developed countries, reduced processing time has the effect of less imperfections of the food that may be caused by long transportation paths. This, in turn, could help fight food waste.

- *Trust in Certification Compliance*: Before the rise of blockchain technology, certification agencies had to be trusted by consumers to award certifications in a rightful manner and regularly control adherence to the standards they represent. This is no longer necessary. As BcAgriFood demonstrated with the example of grapes that travel from South Africa to Europe, certification standards can be tracked and stored in a secure blockchain.
  Additionally, as we showed earlier in this section, blockchain can facilitate trust in IoT devices. This further adds to the trustworthiness of certifications if certification criteria are measured by such devices. For example, trusted IoT sensors can measure the type and amount of fertilizer that is applied to plants or the amount of hormones added to animal food. This information is then stored in a blockchain and used to evaluate whether certification criteria are met.

- *Restrictions on UAVs*: It can be envisioned that blockchain applications keep track of what exactly the cameras on UAVs used for agricultural purposes record. However, this does not solve the privacy concerns of the lawmakers; in fact, it might even be contrary to their goals as such a solution would mean that private data are stored in the blockchain forever, visible to anyone. Therefore, blockchain technology offers no solution to this challenge.

Blockchain technology provides (part of) the infrastructure necessary for efficient technology-supported agriculture [56]. This was also shown by examining the blockchain solutions to common problems with IoT systems in the agricultural sector in the points above. However, not all issues can be solved with blockchain, especially those related to privacy. As already mentioned in the previous section, this is the main shortcoming of blockchain systems. However, the agricultural sector is by far not the industry with the highest privacy standards, and blockchain applications certainly solve more problems in this industry than they leave unsolved.

5.4.3 Healthcare

The following will address the challenges mentioned in Section 5.3.3 and detail the potential of blockchains to provide a solution.

- *Security*: The security challenges in IoT systems for healthcare may be addressed by the storage of device configurations in a blockchain. This would enable an IoT device to ensure at all times that it is configured as is intended by the developers while still allowing the developers to modify the configuration after deployment using a smart contract. In addition to this, the handling of access to the data collected by the IoT device could be achieved through a smart contract, ensuring the authenticity of the access control configuration [58][53].

- *Loss of Privacy*: While there exist blockchain implementations that have privacy mechanisms in place, the blockchain concept as such does not provide privacy. It can even be stated that the public nature of a blockchain inherently conflicts with the establishment of privacy.

- *Trust*: The trust concerns in IoT healthcare systems can be addressed by storing data recorded by smart sensors in a blockchain. The distributed nature and the cryptographic hashing algorithms of a blockchain ensure that the records are tamper-proof and proves their authenticity and provenance. This could provide medical professionals with more confidence in the truthfulness data, allowing it to be used in the decision making process. The storage of device configurations in the blockchain further trust in the mode of operation of a healthcare IoT devices and can, therefore, further contribute to the aforementioned benefit.

The points mentioned above show that there exists potential for blockchain systems to improve healthcare related IoT systems, especially through the storage of device configurations and health data in a distributed ledger. The establishment of privacy, however, may not be achieved using blockchains and may even contradict the sensible application of a blockchain solution altogether since the privacy of health data is often protected by law. While private blockchains do address this issue, they neutralize many of the benefits enabled by public blockchain technology in the first place, such as distributed trust. In order to unlock the blockchain's potential for healthcare IoT systems, these issues must be addressed in the future both on a technological and a legal level.

5.4.4 Energy

This section will look at the concerns for IoT systems in the energy sector raised in Section 5.3.4 through the lens of blockchain technology and suggest appropriate solutions.

- *Single Point of Failure*: As we have established earlier, an IoT-supported smart grid is, by nature, centralized and therefore constitutes a single point of failure. Moving away from the smart grid concept while still harvesting its benefits, [59] suggest the creation of local energy markets (LEM), in which energy producers and consumers can "virtually trade energy within their community." This promising new marketplace is enabled by smart contracts using blockchain technology [59] [60]. In such a decentralized system, the single point of failure is eliminated. However, [59] also admits that, with current implementations, a blockchain-based LEM is not yet scalable. This problem has to be solved before we can rely on such an approach.

- *Mismatch of Energy Production and Consumption*: In part, this challenge is also addressed by the creation of LEM. The reason is that, with a decentralized production of energy, more energy producers enter the market. If we assume that a higher number of producers leads to a more diverse range of energy sources, the chances that at least some of them can provide consumers with energy at any time is increased. However, it is also clear that this assumption does not hold in extreme situations like exceptionally high energy demand during less productive times. Energy storage systems will therefore remain a crucial part of the (blockchain-enhanced) smart grid.

- *Lack of Consumer Choice*: The challenge regarding lack of consumer choice is twofold, as we saw earlier. Neither are IoT-based smart grids very transparent (and trustworthy so) nor do energy consumers really have a choice, even if they were aware of the specifics of the energy they purchase. Both of these aspects can be solved with a blockchain approach. With a plurality of energy vendors, consumers can choose what type of energy to purchase and from whom. Additionally, information about the origin of the energy recorded by the smart grid can be securely stored in a blockchain, therefore reassuring the user that it is correct.

Overall, we found that a decentralized energy marketplace with many small energy producers can solve most of the problems inherent to a smart grid. These LEM are now feasible

with the existence of blockchains and their various benefits, such as the immutability of data and the facilitation of smart contracts. In addition to the mentioned benefits, we can also expect lower energy cost as a result of "minimizing expensive grid transactions" [59]. On the other hand, one must be mindful of the energy consumption of the decentralized marketplace as such [60] because the cost savings could be outweighed by the additional energy costs for operating the system. Another drawback of current implementations of LEM that [60] pointed out is that there is no support of energy credits because senders cannot "transact the assets they do not own." This is, however, possible in traditional markets. Therefore, a solution to this challenge has to be found before blockchain-supported LEM will be accepted by those who value this feature in existing energy markets.

5.5 Conclusion

To sum up our findings, we have explored how the industries supply chain management, agriculture, healthcare and energy can benefit from the implementation of the IoT. Possible use cases are as diverse as these industries, but they all relate to the concepts of intelligent monitoring and, thereafter, automatic control based on the data collected while monitoring. On the other hand, we have also uncovered some of the limitations of IoT-based systems in the exemplary industries.
The second part of the paper aimed at finding solutions to these challenges by using blockchain technology. The result was positive: Blockchain can indeed mitigate many of the problems introduced by IoT applications. This can be attributed to blockchain technology's greatest asset – decentralized trust. Yet, some challenges persist. Mainly, the introduction of a blockchain into a system cannot solve the lack of privacy. In fact, as we have shown, the concept of blockchain can be argued to be contrary to that of privacy. Therefore, applications containing sensitive data will have to enhance their system beyond the implementation of blockchain technology.

Bibliography

[1] Denise Lund & Carrie MacGillivray & Vernon Turner & Mario Morales *Worldwide and Regional Internet of Things (IoT) 2014-2020 Forecast: A Virtuous Circle of Proven Value and Demand*, IDC Market Analysis, IDC, Framingham, USA, May, 2014, pp 1–29. https://www.business.att.com/content/article/IoT-worldwide_regional_2014-2020-forecast.pdf

[2] *9 baby monitors wide open to hacks that expose users' most private moments*; https://arstechnica.com/information-technology/2015/09/9-baby-monitors-wide-open-to-hacks-that-expose-users-most-private-moments/, March, 2018

[3] *Hackers can now hitch a ride on car computers*; http://www.latimes.com/business/autos/la-fi-hy-car-hacking-20150914-story.html, March, 2018

[4] *Hacked terminals capable of causing pacemaker deaths*; https://www.itnews.com.au/news/hacked-terminals-capable-of-causing-pacemaker-mass-murder-319508, March, 2018

[5] *Dyn Analysis Summary Of Friday October 21 Attack*; https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/, March, 2018

[6] Stuart Haber & Scott Stornetta: *How to time-stamp a digital document*; Journal of Cryptology, Vol. 3, No. 2, Springer, New York City, USA, January, 1991, pp. 99–111, https://link.springer.com/content/pdf/10.1007%2FBF00196791.pdf

[7] Satoshi Nakamoto: *Bitcoin: A Peer-to-Peer Electronic Cash System*; Bitcoin, October, 2008, https://bitcoin.org/bitcoin.pdf

[8] *Confirmed Bitcoin Transactions Per Day*; Blockchain.info, https://blockchain.info/charts/n-transactions?timespan=all, April, 2018

[9] Marco Iansity & Karim R. Lakhani: *The Truth About Blockchain*; Harvard Business Review, January-February 2017 Issue, Harvard Business School Publishing, Boston, MA, USA, February, 2017, https://hbr.org/2017/01/the-truth-about-blockchain

[10] *Overview of the Internet of things*; Recommendation ITU-T Y.2060, International Telecommunications Union, Geneva, CH, June, 2012, http://handle.itu.int/11.1002/1000/11559

[11] John T. Mentzer & William DeWitt & James S. Keebler & Soonhong Min & Nancy W. Nix & Carlo D. Smith & Zach G. Zacharia: *Defining Supply Chain Management*; Journal Of Business Logistics, Vol. 22, No. 2, Wiley-Blackwell, Hoboken, New Jersey, USA, 2001, pp. 1–25, https://www.biblioteca.fundacionicbc.edu.ar/images/e/e4/Conexion_y_logistica_2.pdf

[12] *Agriculture*, United States Department of Agriculture; https://agclass.nal.usda.gov/dne/search.shtml, accessed April 24, 2017

[13] Jude Boucher: *Agricultural Science and Management*. callistoreference, 2018.

[14] *Healthcare Sector*; Investopedia, https://www.investopedia.com/terms/h/health_care_sector.asp, April, 2018

[15] *Energy Sector*; Investopedia, https://www.investopedia.com/terms/e/energy_sector.asp, accessed April 24, 2018

[16] Julian Turner: *The energy industry outlook, from 2017 to 2018*. Power Technology, January 17, 2018, https://www.power-technology.com/features/energy-industry-outlook-2017-2018/, accessed April 24, 2018

[17] Knud Lasse Lueth: *IoT 2017 in Review: The 10 Most Relevant IoT Developments of the Year*; IoT Analytics, https://iot-analytics.com/iot-2017-in-review/, April, 2018

[18] *More Than 50 Billion Connected Devices*, Ericsson White Paper, Ericsson AB, Stockholm, Sweden, February 2011, pp 1–12. http://www.akos-rs.si/files/Telekomunikacije/Digitalna_agenda/Internetni_protokol_Ipv6/More-than-50-billion-connected-devices.pdf

[19] In Lee & Kyoochun Lee: *The Internet of Things (IoT): Applications, investments, and challenges for enterprises*; Business Horizons, Vol. 58, No. 4, Elsevier B.V., Amsterdam, NL, August, 2015, pp. 431–440, https://ac.els-cdn.com/S0007681315000373/1-s2.0-S0007681315000373-main.pdf?_tid=12fe9035-a01b-4c2f-aa3f-4a85c09966af&acdnat=1522136463_964880c9a42394a11d5b676752b564e5

[20] Duncan McFarlane & Yossi Sheffi: *The Impact of Automatic Identification on Supply Chain Operations*; The International Journal of Logistics Management, Vol. 14 No. 1, Emerald, Bingley, UK, 2003, pp. 1–17, https://doi.org/10.1108/09574090310806503

[21] Victoria Greene: *What's Ahead for IoT and Logistics in 2018*; IoTForAll, https://www.iotforall.com/logistics-and-iot-trends-2018/, March, 2018

[22] Rob O'Byrne: *6 Key Supply Chain and Logistics Trends to Watch in 2017*; Logistics Bureau, https://www.logisticsbureau.com/6-key-supply-chain-and-logistics-trends-to-watch-in-2017/, April, 2018

[23] Ping Lou & Quan Liu & Zude Zhou & Huaiqing Wang: *Agile Supply Chain Management over the Internet of Things*; 2011 International Conference on Management and Service Science, IEEE Computer Society, Washington, DC, USA, August, 2011, pp. 1–4, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5998314&isnumber=5997898

[24] *Continuous interconnected supply chain - Using Blockchain & Internet-of-Things in supply chain traceability*, Deloitte White Paper, Deloitte, London, UK, November, 2017, pp. 1–24, https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/technology/lu-blockchain-internet-things-supply-chain-traceability.pdf

[25] Alfons Weersink: *The Growing Heterogeneity in the Farm Sector and Its Implications*; Canadian Journal of Agricultural Economics, Vol. 66 (2018), pp. 27–41

[26] Christopher Brewster & Ioanna Roussaki & Nikos Kalatzis & Kevin Doolin & Keith Ellis: *IoT in Agriculture: Designing a Europe-Wide Large-Scale Pilot*

[27] Karina Popova: *IoT as a solution for precision farming*; TechTarget, February 23, 2017 `https://internetofthingsagenda.techtarget.com/blog/IoT-Agenda/IoT-as-a-solution-for-precision-farming`, accessed April 26, 2018

[28] Mare Srbinovska, Cvetan Gavrovski, Vladimir Dimcev, Aleksandra Krkoleva and Vesna Borozan: *Environmental parameters monitoring in precision agriculture using wireless sensor networks*; Journal of Cleaner Production, Vol. 88, 2015, pp.297–307

[29] Tanja Folnovic: *Yield Losses Due to Pests*; agrivi, March 26, 2016 `https://blog.agrivi.com/en/post/yield-losses-due-to-pests`, accessed April 26, 2018

[30] H. Charles J. Godfray, John R. Beddington, Ian R. Crute, Lawrence Haddad, David Lawrence, James F. Muir, Jules Pretty, Sherman Robinson, Sandy M. Thomas and Camilla Toulmin: *Food Security: The Challenge of Feeding 9 Billion People*, Science Vol. 327 (2010), pp. 812–818

[31] Julian Parfitt, Mark Barthel and Sarah Macnaughton: *Food waste within food supply chains: quantification and potential for change to 2050*, Phil. Trans. R. Soc. B (2010), Vol. 365, pp. 3065–3081

[32] Peggy K. Hall and Rusty Rumley: *Legal Challenges Facing Unmanned Aerial Systems and Commerical Agriculture*, 39 U. Ark. Little Rock L., Vol. 389 (2017)

[33] Ekaterina Balandina & Sergey Balandin & Yevgeni Koucheryavy & Dmitry Mouromtsev: *IoT Use Cases in Healthcare and Tourism*; 2015 IEEE 17th Conference on Business Informatics, Vol. 2, IEEE Computer Society, Washington, DC, USA, July, 2015, pp. 37–44, `http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7264765`

[34] *Iot In Healthcare: How It Gives A Second Wind To Your Medical Software*; Cleveroad, `https://www.cleveroad.com/blog/iot-in-healthcare-industry--see-why-it-has-a-promising-future`, March, 2018

[35] Justin Gesso: *Healthcare business trends*; IBM IoT Blog, `https://www.ibm.com/blogs/internet-of-things/iot-healthcare-business-trends/`, March, 2018

[36] Viktoria Weber: *Apple Watch, Fitness-Tracker & Co.: Schweizer Krankenkassen wollen ihren Kunden bald auf Schritt und Tritt folgen*; Watson, `https://www.watson.ch/Schweiz/Digital/673540201-Apple-Watch--Fitness-Tracker---Co---Schweizer-Krankenkassen-wollen-ihr`, March, 2018

[37] Rich Haridy: *FDA approves first smart pill that tracks drug regimen compliance from the inside*; New Atlas, `https://newatlas.com/smart-digital-pill-fda-approval/52187/`, April, 2018

[38] *HealthKit*; Apple, `https://developer.apple.com/healthkit/`, April, 2018

[39] *ResearchKit*; Apple, `http://researchkit.org`, April, 2018

[40] *The missing link in healthcare: Addressing the silent killer of non-adherence*; Vodafone White Paper, Vodafone Ltd., Berkshire, UK September, 2017, pp. 1–5, `http://www.vodafone.com/business/news-and-insights/white-paper/the-missing-link-in-healthcare`

[41] *Digitaler Schutzengel fÃ¼rs Handgelenk*, Swisscom Magazin, https://magazin.swisscom.ch/digitalisierung-im-alltag/digitaler-schutzengel-fuers-handgelenk/, May, 2018

[42] Phillip A. Laplante & Nancy Laplante: *The Internet of Things in Healthcare – Potential Applications and Challenges*; IT Professional, Vol. 18, No. 3, IEEE Computer Society, Washington, DC, USA, May, 2016, pp. 2–4, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7478533

[43] *What is the Smart Grid?*; https://www.smartgrid.gov/the_smart_grid/smart_grid.html

[44] YaFang Lou & ZhiJun Yuan & ShuJun Zhou: *The study on wireless internet of things (IOT) technology in the digitizing oilfield construction*

[45] Wen-Long Chin & Wan Li & Hsiao-Hwa Chen: *Energy Big Data Security Threats in IoT-Based Smart Grid Communications*

[46] Xin Li & Quiyuan Huang & Dapeng Wu: *Distributed Large-Scale Co-Simulation for IoT-Aided Smart Grid Control*

[47] *America: The Worldwide Leader In Wasting Energy*; Forbes, https://www.forbes.com/sites/ciocentral/2013/02/22/america-the-worldwide-leader-in-wasting-energy/#6b8b5e231985, accessed April 29, 2018

[48] Alaa Mohd, Egon Ortjohann, Andreas Schmelter, Nedzad Hamsic & Danny Morton: *Challenges in integrating distributed Energy storage systems into future smart grid*; Industrial Electronics (2008)

[49] intel: *Intel INSIDE, energy efficiency OUTSIDE*, https://www.intel.com/content/www/us/en/internet-of-things/solution-briefs/smart-city-lighting-brief.html

[50] *How Blockchain Technology Will Disrupt the Energy Sector*; Capdax, https://medium.com/capdax-exchange/how-blockchain-technology-will-disrupt-the-energy-sector-59207f453f40, accessed May 21, 2018

[51] Cognizant: *Blockchain in Banking: A Measured Approach*, https://www.cognizant.com/whitepapers/Blockchain-in-Banking-A-Measured-Approach-codex1809.pdf, accessed April 22, 2017.

[52] Zibin Zheng & Shaoan Xie & Hongning Dai & Xiangping Chen & Huaimin Wang: *An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends*; 2017 IEEE 6th International Congress on Big Data, IEEE Computer Society, Washington, DC, USA, June, 2017, pp. 557–564, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8029379

[53] Nir Kshetri: *Can Blockchain Strengthen the Internet of Things?*; IT Professional, Vol. 19, No. 4, IEEE Computer Society, Washington, DC, USA, August, 2017, pp. 68–72, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8012302

[54] Ali Dorri & Salil S. Kanhere & Raja Jurdak: *Blockchain in internet of things: Challenges and Solutions*; ArXiv e-prints, Cornell University, Ithaca, NY, USA, August, 2016, pp. 1–13, https://arxiv.org/pdf/1608.05187.pdf

[55] Amit Ganeriwalla& Michael Casey& Prema Shrikrishna& Jan Philipp Bender & Stefan Gstettner: *Does Your Supply Chain Need a Blockchain?*; Boston Consulting Group, `https://www.bcg.com/publications/2018/does-your-supply-chain-need-blockchain.aspx`, May, 2018

[56] Yu-Pin Lin & Roy R. Petway & Johnathen Anthony & Hussnain Mukhtar & Shih-Wei Liao & Cheng-Fu Chou & Yi-Fong Ho: *Blockchain: The Evolutionary Next Step for ICT E-Agriculture*

[57] Jonathan Biggs, Sheri R. Hinish, Michael A. Natale & Matt Patronick: *Blockchain: Revolutionizing the Global Supply Chain by Building Trust and Transparency*

[58] Seyoung Huh & Sangrae Cho & Soohyung Kim: *Managing IoT Devices using Blockchain Platform*, 2017 19th International Conference on Advanced Communication Technology (ICACT), IEEE Computer Society, Washington, DC, USA, February, 2017, pp. 464–467, `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7890132`

[59] Esther Mengelkamp & Benedikt Notheisen & Carolin Beer & David Dauer & Christof Weinhardt: *A blockchain-based smart grid: towards sustainable local energy markets*

[60] Nurzhan Zhumabekuly Aitzhan & Davor Svetinovic: *Security and Provacy in Decentralized Energy Trading through Multi-Signatures, Blockchain and Anonymous Messaging Streams*

Chapter 6

An Overview of Emerging Wireless Communication Systems in 5G

Ananya Pandya, Bhargav Bhatt

This paper gives an introduction to fifth generation wireless communication systems. Followed by the emerging technology of 5G communications such as Light-Fidelity, LoRa and mmWave. Each technology is further explained in details along with it's challenges and use cases. Further, the paper describes the real time scenarios of this new technology. At the moment, it's not yet clear which technologies will do the most for 5G in the long run, but a few early favorites have emerged. Moreover, 5G is still in the planning stages, and companies and industry groups are working together to figure out exactly what it will be. But they all agree on one matter: As the number of mobile users and their demand for data rises, 5G must handle far more traffic at much higher speeds than the base stations that make up today's cellular networks.

Contents

6.1 Introduction

Wireless data traffic has been increasing at a rate of over 50 % per year per subscriber, and this trend is expected to accelerate over the next decade with the continual use of video and the rise of the Internet-of-Things (IoT). To address this demand, the wireless industry is moving to its fifth generation (5G) of cellular technology that will use millimeter wave (mmWave) frequencies to offer unprecedented spectrum and multi-Gigabit-per-second (Gbps) data rates to a mobile device. Mobile devices such as cell phones are typically referred to as user equipment (UE). A simple analysis illustrated that 1 GHz wide channels at 28 or 73 GHz could offer several Gbps of data rate to UE with modest phased array antennas at the mobile handset, and early work showed 15 Gbps peak rates are possible with 4 times 4 phased arrays antenna at the UE and 200 m spacing between base stations (BSs).
With global mobile data traffic expected to grow eight times by the end of 2023, there is a need for a more efficient technology, higher data rates and spectrum utilization. New applications such as 4K/8K video streaming, virtual and augmented reality and emerging industrial use cases will also require higher bandwidth, greater capacity, security, and lower latency. Equipped with these capabilities, 5G will bring new opportunities for people, society, and businesses.

6.1.1 Features of 5G technology

- **High Speed** Practically possible to avail the super speed i.e. 1 to 10 Gbps.
- **Low Latency** Latency will be 1 millisecond (peer to peer).
- **High Bandwidth** 1000 times more bandwidth will be available per unit area.
- **More Connected Device** Feasibility to connect 10 to 100 number of devices.
- **Worldwide Coverage**
- **Energy Efficient** There will be about 90% reduction in network energy usage. More over it will also be efficient enough to increase the battery life of the devices

6.2 Emerging Technologies

This section presents the emerging technologies that are going to integrate with 5G implementation and their framework. Li-Fi, LoRa and Milimeter Waves are each described in their own subsection. The last subsection gives a brief introduction to 5G technologies like Massive MIMO and Beamforming.

6.2.1 LiFi

Li-Fi can be thought of as a light-based Wi-Fi. It uses light instead of radio waves to transmit information.
Instead of Wi-Fi modems, Li-Fi would use transceiver-fitted LED lamps that can light a room as well as transmit and receive information.
Since, simple light bulbs are used, there can be any number of access points.
Light bulbs devices are normally used for illumination only by applying a constant current. The implementation of Li-Fi is using LED light bulbs at the downlink transmitter. Due to fast and subtle variations of the current, the optical output can be made to vary at extremely high speeds.

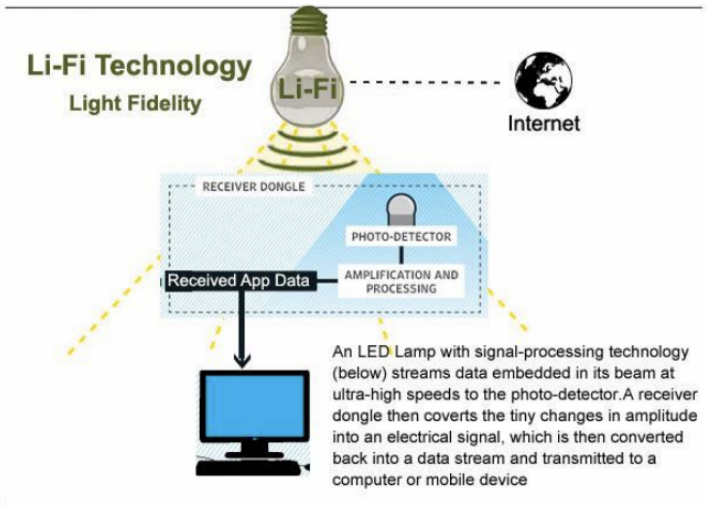


Figure 6.1: Li-Fi Technology

The property of optical current is used in Li-Fi setup. The operational procedure is very simple, if the LED is on, you transmit a digital 1, if its off you transmit a 0. The LEDs gives nice opportunities for transmitting data, which can be switched on and off very quickly. This leads to very small amount of requirement of LEDs and a controller that code data into those LEDs. Only one thing need to be taken care of, is to vary the rate at which the LEDs flicker depending upon the data we want to encode.
There are some different types of enhancements, that can be made, like using an array of LEDs for parallel data transmission, or using mixtures of RGB LEDs to alter the lights frequency with each frequency encoding a different data channel. These kind of advancements promise a theoretical speed of 10 Gbps meaning one can download a full high-definition film in just 30 seconds [1].

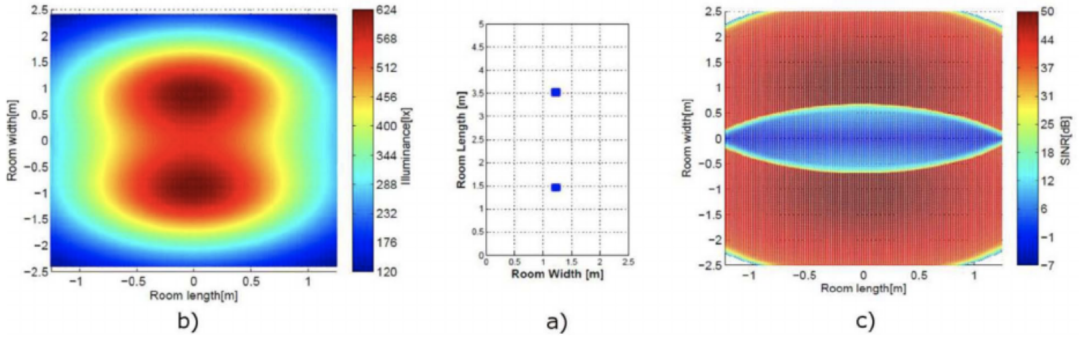


Figure 6.2

A unique feature of LiFi is that it combines illumination and data communication by using the same device to transmit data and to provide lighting. Fig. 6.2(a) depicts a simple room scenario with two lights. Fig. 6.2(b) shows the resulting illuminance at desk level of 0.75 m. In the particular example, the lights are placed such that within the plane at desk height, 90 % of the area achieves an illuminance of 400 lx based on a given illumination requirement. Figure 6.2 depicts the resulting signal-to-interference-plus-noise ratio(SINR). The region where the light cones overlap is subject to strong CCI, and the SINR drops significantly. It is interesting to note that the SINR can vary by about 30 dB within a few centimeters. This example also highlights that the peak SINR can be in region of 50 dB which is two to three orders of magnitude higher than the peak SINR in RF based wireless systems. The achievable data rate strongly depends on the location of the receiver and also on the field of view (FoV) of the receiver.

Interference mitigation techniques are required to ensure that within the region of strong CCI, a mobile station can also achieve high SINR, and this is a non-trivial problem which involves signal processing such as successive interference cancellation [2].

1. **Applications of Lifi:**

   The applications of Li-Fi are categorized to be very diversified due to its key features, such as energy efficient, beam lighting,security, high data rate capability and many more. Each light fixture in the application environment turns into separate type of data channel. These channels can supply different data into each separate pool of light, which then can be delivered at the full speed download for the channel.

   Security: In office, particularly in closed room environment, the access area of each channel is the width of the light pool, and can be accessed by multiple users. Each user can receive higher data rates than would be the case for an equivalent Wi-Fi channel. In the Wi-Fi case, each user or group of users directly competes for access to bandwidth. The net result is that the more connections there are, the slower the download speeds are for all. By contrast, in the case of Li-Fi, with its greater number of available access points, each pool of light provides full channel data rates with fewer simultaneous users. The overall net benefit to each user is up to 1000 times greater speeds. In addition, and in contrast to radio waves, the light does not pass through the walls. Therefore, with minimal precautions to avoid leakage from windows, etc., security is fundamentally enhanced as compared with Wi-Fi.

   Dense urban environments: Dense urban environments by their nature tend to have complete artificial lighting coverage. This lighting infrastructure can provide always available high data rate access for users as they move through that environment. For example, along a hotel corridor or reception hall a number of users can receive high data rate downloads at any point. Moreover, high speed wireless communication would be available in every room since the light waves do not propagate through walls. This results in interference-free wireless communication, and spectrum does not have to be shared among a large number of users in the rooms.

   Cellular communication: In external urban environments, the use of Li-Fi enabled street lamps would provide a network of internet access points. In cellular communication, the distance between radio base stations has come down to about 200-500 metres. So, instead of deploying new radio base stations in our cities, street lamps could provide both, illumination during night, and high speed data communication 24/7. Surprisingly, even when the lights are off as perceived by the eye, full data communication rates are still possible. There is also an additional cost benefit as installing new radio base stations usually comes with large cost for installation and site lease.

   EMI sensitive environments: On aircraft, Li-Fi enabled lighting will allow high data rate connectivity for each passenger. It will allow connectivity at all times, without creating electromagnetic interference (EMI) with sensitive radio equipment on the flight deck. The reduction in cabling requirement also means a lighter aircraft.

   Intelligent transportation systems: Car headlights and tail lights are steadily being replaced with LED versions. This offers the prospect of car-to-car communication over Li-Fi, allowing development of anti-collision systems and exchange of information on driving conditions between vehicles. Traffic lights already use LED lighting, so that there is also the prospect offered of city wide traffic management systems. This would enable car systems to download information from the network and have real time information on optimal routes to take, and update the network regarding conditions recently experienced by individual vehicles.

Indoor navigation: By identifying each light (for example, through the use of the widely used MAC codes used by data routers and computers) it is possible to provide a smart means of navigating through urban environments. The identification of each code would be linked to a specific location. For example, light received from the closest fixture can indicate to a mobile user their exact position as they travel along a corridor [3].

2. **Products:**

LiFi-XC: The LiFi-XC provides lightweight, highspeed secure and fully networked wireless communications via light. The LiFi-XC is a certified plug and play system that works with USB devices and is small enough to be integrated into your next laptop, tablet or smart appliance [4].

Babcock: Babcock has established a smart Connected Facility test bed at its Devonport Dockyard in Plymouth. The purpose of this facility is to test and evaluate a number of leading technologies that will allow it to develop new operating models based on the use of digital data. The Connected Facility is being used to demonstrate how smart wireless sensoring and condition based monitoring systems might provide benefit to its maintenance programme and drive benefit into the business both in terms of cost savings and increased asset availability. Currently, the use of wireless sensors using radio frequency (RF) enabled sensors can represent a challenge as RF transmission can be subject to interference, security risks and can be unreliable. In order to understand its options for future wireless communications that are reliable, secure and non-interfering , Babcock is evaluating the application of new wireless opportunities to ensure that Babcock and ultimately its customers can ride the technology wave while operating under safe and secure conditions required in this sensitive environment. Light fidelity (LiFi) technology is a natural fit for such critical use case [5].

BT Defence: The LiFi installation allowed for BT to test and prove unique use cases of LiFi for the defence sector. Applications such secure communications through light due to the intrinsically safe nature of containing light were established. Additional consideration was given to the ability to apply different security levels to individual lights or a group of lights allowing for very sophisticated geofencing [6].

3. **LiFi Misconceptions:**
There are many misconceptions in relation to LiFi:

LiFi is a LoS technology: This perhaps is the greatest misconception. By using an orthogonal frequency division multiplexing(OFDM)-type intensity modulation (IM)/direct detection (DD) modulation scheme, the data rate scales with the achieved signal-to-noise-ratio (SNR). In a typical office room environment where the minimum level of illumination for reading purposes is 500 lx,the SNR at table height is between 40 dB and 60 dB [25]. This means higher order digital modulation schemes can be used in conjunction with OFDM to harness the available channel capacity. By using adaptive modulation and coding (AMC) it is possible to transmit data at SNRs as low as -6 dB. Therefore, there is no direct LoS component reaching the receiver at the front, but the video is successfully received. Obviously, if the wall would be dark, more light would be absorbed which would compromise the SNR at the receiver. If the SNR drops below the -6 dB threshold,an error-free communication link would not be possible. However, in low-light conditions single photon avalanche diodes may be used at the receiver which enhance the receiver

sensitivity by at least an order of magnitude.

LiFi does not work in sunlight conditions: Sunlight constitutes a constant interfering signal outside the bandwidth used for data modulation. LiFi operates at frequencies typically greater than 1 MHz. Therefore, constant sunlight can be removed using electrical filters. An additional effect of sunlight is enhanced shot noise, which cannot easily be eliminated by optical filters. In one of the study, the impact of shot noise was investigated qualitatively, and it was found that data rate is compromised by 1.5 % and 4.5 % assuming a 0.19 mm2 detector, and 2 mm2 detector respectively. Saturation can be avoided by using automatic gain control algorithms in combination with optical filters. In fact, we argue that sunlight is hugely beneficial as it enables solar cell based LiFi receivers where the solar cell acts as data receiver device, and at the same time harvests sunlight as energy

Lights cannot be dimmed: There are advanced modulation techniques such as eU-OFDM which enable the operation of LiFi close to the turn-on voltage (ToV) of the LED which means that the lights can be operated at very low light output levels while maintaining high data rates.

The lights flicker: The lowest frequency at which the lights are modulated is in the region of 1 MHz. The refresh rate of a computer screen is about 100 Hz. This means the flicker-rate of a LiFi light bulb is 10,000 higher than that of a computer screen.Therefore, there is no perceived flicker.

This is for downlink only: A key advantage is that LiFi can be combined with LED illumination. This, however, does not mean that both functions always have to be used together. Both functions can easily be separated (see the comment on dimming). As a result, LiFi can also be very effectively used for uplink communication where lighting is not required. The infrared spectrum,therefore, lends itself perfectly for the uplink. We have conducted an experiment where we sent data at a speed of 1.1 Gbps over a distance of 10 m with an LED of only 4.5 mW optical output power [2].

6.2.2 LoRa

LoRa (Long Range) is a long-range wireless technology which refers to the spread spectrum modulation technique. It is specifically designed for long-range IoT applications that are used over a Low Power Wide Area Network (LPWAN), with the help of low power battery operated devices to transfer data at a low bit rate over a long range. LoRa is the physical layer that is required to establish communication [8]. LoRa devices provide the optimal efficient level of service in terms of device battery life, network capacity and manufacturing as well as operating cost. LoRa Technology is making the world a Smart Planet by integrating this wireless radio frequency technology into smart cars, illuminating smart lights, machines, manufacturing equipment, home appliances, wearable devices.

LoRa Alliance

The LoRa Alliance a non-profit association, currently more than 500 member companies and organization committed to contributing large-scale deployment of LPWAN IoT by means of development and promotion of the LoRaWAN open standard. Members benefit from a vibrant ecosystem of active contributors offering solutions, products, and services, which create new and sustainable business opportunities [7]. The Alliance has members throughout major continents of the world such as North America, Europe, Africa and Asia including telecommunication companies, original equipment manufacturers (OEM), system integrators, sensor and semiconductor manufacturers. Founding members of the LoRa Alliance include IBM, MicroChip, Cisco, Semtech, Bouygues Telecom, Singtel, KPN,

Swisscom, Fastnet and Belgacom [7]. The LoRa Alliance provides the interoperability, that is, communication among different devices, needed for LPWAN to scale, making LoRaWAN the premier solution for global LPWAN deployments through standardization and certification schemes.

LoRa Technology

Lora technology is a union of long-range, efficiency through low power consumption and secure data transmission. It is a Semtech innovation. Both, public and private networks using this technology can provide coverage which is greater in distance than that of existing cellular networks. It can easily integrate with existing infrastructure and provides a solution to serve battery-operated IoT devices. Semtech builds LoRa Technology enabled chipsets which are built into the products offered by the large network of IoT associates and further blends into LPWANs from mobile network operators worldwide [8].

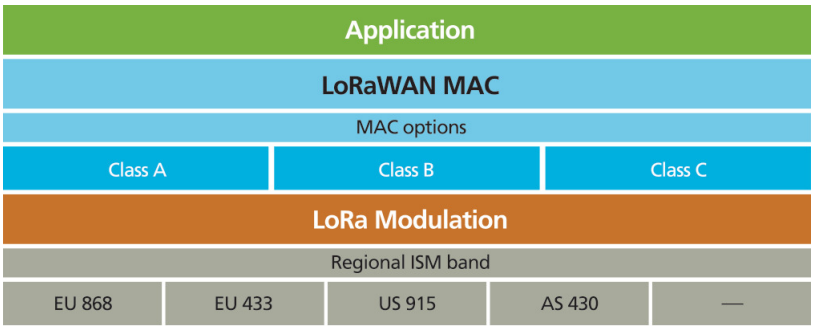


Figure 6.3: LoRa Layers

LoRaWAN

LoRaWAN is multiple access protocol which is designed to reduce the node collisions. It is implemented om server side. A server application is required to run the MAC functions over a network connection. It is a protocol specification built on top of the LoRa technology developed by the LoRa Alliance. LoRa uses unlicensed radio spectrum, also known as the ISM band or the Industrial, Scientific and Medical bands. It means that anyone can use this band and don't need a specific kind of license from government to use it. For instance, like Wifi. This bands enables low power wide area communication among remote sensors and gateways connected to the network.Public or Private IoT network can be established using hardware and software through standards-base approach to build a LPWAN. Such system is bi-directionally secure, interpolatable and mobile and provides accurate localization. As an open source, the specification is available for free to download from the LoRa Alliance website. LoRaWAN network architecture is a star-of-stars topology in which gateways are a transparent bridge relaying messages between end-devices and a central network server in the back-end [8].

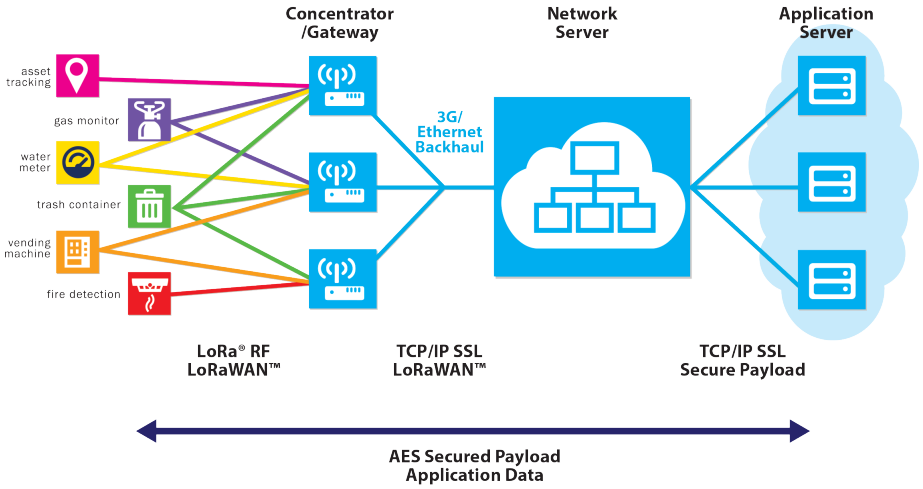


Figure 6.4: LoRa Networks

LoRa Key Features

- **Geolocation** Enables GPS-free, low power tracking applications.
- **Low Cost** Reduces costs three ways: infrastructure investment, operating expenses and end-node sensors.
- **Standardized** Improved global interoperability speeds adoption and roll out of LoRaWAN-based networks and IoT applications.
- **Low Power** Protocol designed specifically for low power consumption extending battery lifetime up to 20 years.
- **Long Range** Single base station provides deep penetration in dense urban/indoor regions, plus connects rural areas up to 30 miles away.
- **Secure** Embedded end-to-end AES128 encryption.
- **High Capacity** Supports millions of messages per base station, ideal for public network operators serving many customers.

Challenges

The biggest drawback of LoRa is that they do not exist everywhere. Therefore, they are appropriate only for solutions sold in a defined geographic area. Companies wanting to deploy IoT solutions quickly in a variety of locations may have to wait on the buildout of network coverage. These networks also have some work to do to make device provisioning and identity easy. Without a SIM card-like concept, keys and unique ID numbers for each endpoint need to move between network operators and device manufacturers [9].

6.2.3 Milimeter Waves

Millimeter wave generally corresponds to the radio spectrum between 30 GHz to 300 GHz, with wavelength between one and ten millimeters. However, in the context of wireless communication. Milimeter Waves corresponds to a few bands of spectrum ranging from 38 to 94 GHz, and more E-band between 70 GHz and 90 GHz , which is allocated for the purpose of wireless communication in the public domain [10].

The key advantage of mm wave communication technology is the huge amount of availability of spectral bandwidth. The range of spectral bandwidth is between 70 GHz and 80 GHz bands, a total of 10 GHz, which is more than total of all other licensed spectrum

available for wireless communication. With such wide bandwidth available, millimeter wave wireless links can achieve capacities as high as 10 Gbps full duplex, which is unlikely to be matched by any lower frequency RF wireless technologies.
Due to the availability of this extraordinary amount of bandwidth enables the capability to scale the capacity of mm wave wireless links as demanded by market needs. Typical mm wave products commonly available today operate with spectral efficiency close to 0.5 bits/Hz. Whenever the demand arises for higher capacity links, mm wave technology will be able to meet the higher demand by using more efficient modulation schemes.

Challenges

These are the technical challenges that Milimeter wave faces [11].

- **Free space loss** The free space loss in dB is calculated with: L(Transmission loss) = 92.4 + 20log(f) + 20log(R).
- **Atmospheric absorption** The atmosphere absorbs millimeter waves, thus restricting their transmission range. Rain, fog, and moisture in the air make the signal attenuation very high. Oxygen absorption is especially high at 60 GHz.
- **Mechanical resonance** The mechanical resonance frequencies of gaseous molecules also coincide with the millimeter wave signal. For current technology, the important absorption peaks occur at 24 and 60 GHz.
- **Scattering** Millimeter wave propagation is also affected by rain. Raindrops are roughly the same size as the radio wavelengths and therefore cause scattering of the signal.
- **Non-line of sight issues** When a line-of-sight path between transmitter and receiver isn't present, the travelling signal still has alternative ways to reach the receiver, be it through diffraction, reflection or bending. Diffraction in millimeter waves is scarce due to the short wavelengths.
- **Brightness temperature** When millimeter waves are subjected to absorption by water vapor, oxygen and rain, these molecules absorb high frequency electromagnetic radiation. This absorption subsequently leads the molecules to emit higher frequency EM radiation. This energy emission, when received by a receiver antenna, is called brightness temperature and it degrades system performance. Any Earth-based antenna aimed at a satellite with a high elevation angle, for example, will suffer signal degradation caused by picking up brightness temperature emanating from atmospheric constituents.

Use Case - MiwaveS

MiWaveS is a European collaborative project developing millimeter-wave wireless communication technologies for 5G heterogeneous cellular mobile networks. It focuses on how low-cost or advanced millimetre-wave (mmW) technologies can provide multi-Gigabits per second access to mobile users and contribute to sustain the traffic growth. Hence, spectrum flexibility and the exploitation of the available mmW spectrum will be key strategies to build high-throughput and low-latency infrastructures for next generation heterogeneous mobile networks [12].
It will investigate and demonstrate key enabling technologies and functionalities supporting the integration of mmW small-cells in future heterogeneous networks, particularly at the level of networking functions and algorithms integrated radio and antenna technologies.It is also an industry-driven large-scale integrating project bringing together world-leading European industries and researchers in the domain of wireless communications. It intends to help European ICT industry to be at the forefront of innovation and R&D on

key enabling technologies for future broadband mobile networks and secure a competitive position on this strategic market [13].

6.2.4 Cellular Networks in 5G

Massive MIMO is the currently most compelling sub-6 GHz physical-layer technology for future wireless access. The main concept is to use large antenna arrays at base stations to simultaneously serve many autonomous terminals, as illustrated in Fig. 6.5 [14].

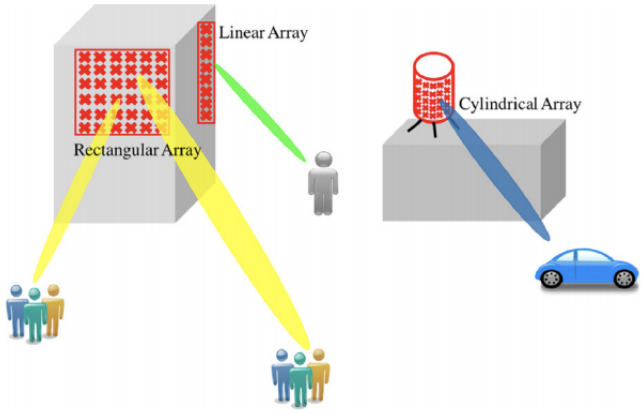


Figure 6.5: Three types of layout of massive MIMO base station antenna array: linear,rectangular, and cylindrical arrays.

- **Excellent spectral efficiency :** achieved by spatial multiplexing of many terminals in the same time-frequency resource. Efficient multiplexing requires channels to different terminals to be sufficiently different, which has been shown to hold, theoretically and experimentally, in diverse propagation environments. Specifically, it is known that Massive MIMO works as well in line-of-sight as in rich scattering [14].

- **Superior energy efficiency :** by virtue of the array gain, that permits a reduction of radiated power. Moreover, the ability to achieve excellent performance while operating with low-accuracy signals and linear processing further enables considerable savings [14].

Beamforming antenna arrays will play an important role in 5G implementations since even handsets can accommodate a larger number of antenna elements at mm-wave frequencies. Aside from a higher directive gain, these antenna types offer complex beamforming capabilities. This allows to increase the capacity of cellular networks by improving the signal to interference ratio (SIR) through direct targeting of user groups. The narrow transmit beams simultaneously lower the amount of interference in the radio environment and make it possible to maintain sufficient signal power at the receiver terminal at larger distances in rural areas [15].

- **Analog Beamforming :** The architecture is used in mm-wave systems as diverse as radar and short-range systems. If there is a case of implementation a multi-stream transmission with analog beamforming is a highly complex task [15].

- **Digital Beamforming :** While analog beamforming is generally restricted to one RF chain even when using largenumber antenna arrays, digital beamforming in theory supports as many RF chains as there are antenna elements. If suitable precoding is done in the digital baseband, this yields higher flexibility regarding

the transmission and reception. The additional degree of freedom can be leveraged to perform advanced techniques like multi-beam MIMO. These advantages result in the highest theoretical performance possible compared to other beamforming architectures [15].

6.3 Applications of 5G Technologies

The following sections describe a number of service scenarios that are the real time applications of 5G technology. These illustrate various scenarios which can take advantage of 5G technology to either increase performance or to utilize the unique capabilities offered by Mobile Edge Computing(MEC) platforms such as proximity to the user and network edge, serving a highly localized area.

6.3.1 Internet of Things

The Internet of Things (IoT) has reshaped the power of computing with various applications built among various types of sensors. An enormous development is seen in IoT based product line and its activity will grow in up coming year. Currently, IoT projects fits in the low data rate solutions that they require to function, along with the low costs which represents the success of non-cellular A Low-Power Wide-Area Network (LPWAN) technologies in various areas and of current cellular IoT solutions. In emerging Iot paradigm in years and decades to come, machine to machine communication plays an important role. Because of IoT-5G scenario, there is boost in sensor based IoT capabilities to robots, actuators and drones for distributed coordination and low-latency reliable execution of tasks at hand. However, with the vast scope and growth in IoT and potential specifications of 5G technologies, IoT can use 5G technologies to push it's limits to next level in terms of growth and development.
By year 2020, up to 40 billion devices will be connected to the Internet as part of the IoT. This can cause bottleneck for existing communication infrastructure which requires transfer of enormous data volumes for efficient IoT[16].
IoT is helpful in establishing efficient city infrastructure by using big data technologies to process information about traffic flow. Then, it is possible to inform users of the recommended transportation and the estimated arrival time according to traffic conditions. However, a network with low latency is a prerequisite or an otherwise serious problems in traffic safety might take place. The massive increase in network connected devices will soon exhaust the International Mobile Subscriber Identity (IMSI) and IPv4. In future IoT scenarios, a tremendous amount of connected devices will be present compared to current 4G network scenarios. Therefore, 5G technologies for transmission and networks have to be able to maintain multiple network connections with many devices using limited resources. Currently, the pricing policy of mobile services is applied per terminal or connection. The number of terminals is expected to increase exponentially; therefore, a new criteria of billing is required [17].

6.3.2 Augmented Reality/Virtual Reality

The Augmented and Virtual Reality technology still lacks in deploying high-quality systems with flexibility and rich user experience which is necessary to integrate and get adopted into the market. These remarkable systems have more potential than video gaming industry, scattered new and unusual experience, and fancy eye-catching applications. Especially if the deployed upon existing infrastructure networks. As per the specifications

Figure 6.6: Smart personal, building and city services with IoT

and features, 5G shares high potential to provide a paradigm shift in the network technology and deliver a higher level of innovation. Thus the network requirement of emerging technologies should be identified to step increase in network capabilities. The projected latency and bandwidth/data rate requirements of the various use cases in terms of 5G are depicted in figure 6.7.

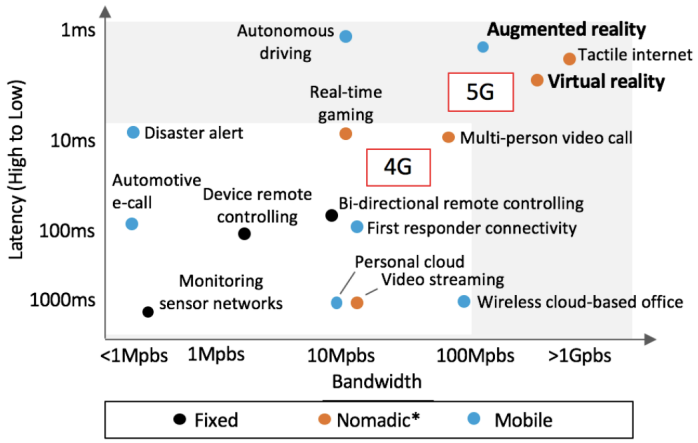


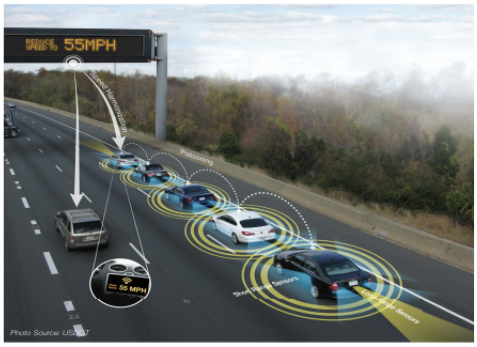
Figure 6.7: Projected network demands of emerging technologies

To deliver next generation of lightweight, ultra-low-latency and compute-intensive technology that will enable inescapable AR/VR adoption. Cloud providers have already begun to invest in edge clouds with a distributed presence that is, placing cloud servers geographically closer to the end user. With the same pace, 5G will have to develop rapidly not only with the efficiency and capacity of the network infrastructure but also by directly integrating computing resources into communication system [18].

6.3.3 Smart Vehicles and Transport

The movement towards 5G means massive Machine Type Communications (mMTC) will allow cities, transportation and infrastructure to transmit real-time data for improved maintence and greater operational efficiency.
When transportation and vehicles are equipped with 5G connectivity, it will revolutionize the way we travel. Vehicle-to-vehicle and vehicle-to-infrastructure communication will make roads safer and more environmentally friendly, while allowing buses and public transportation to run more efficiently. New services and business models can be supported considering sensors embedded in roads, railways and airfields to communicate to each other and/or with smart vehicles [19].
Autonomous-driving cars have the intelligence to recognize, decide and control accordingly.Enhanced V2X communications and autonomous functions are designed to avoid accidents caused by human error. The concept of vehicle platooning refers to vehicles traveling together by following a lead vehicle. This leads to increased safety and comfort, reduced traffic congestion and efficiency improvement. Vehicle platooning can be easily implemented through communication with 5G base stations and vehicle-to-vehicle communications. 5G base-stations can figure out the location and speed information of vehicles in real time through 5G with low latency and can support maintaining the minimum distance between cars. Traffic safety and control include all the services to ensure maximum safety in any type of situation. These applications include large-file and real-time data exchange and, in the case of passenger terminals, real-time information, entertainment systems and video advertising. V2X and some other intelligent transportation systems (ITS) applications require very low latency; much lower than the one provided by current technologies.

Self driving car



Platooning

Smart traffic control

Figure 6.8: Smart Transportation Services

In addition, driverless and next-generation driver-assisted cars will need real-time safety systems that can exchange data with other vehicles and a fixed infrastructure around them. These types of cars need to process at least 1 Gbps of data rate to make smart decisions. However, current technologies cannot support the simultaneous transmission and reception at such a high data rate among thousands of cars within a small area. Therefore, 5G technology is essential for providing real-time services in future vehicles, and baking low latency into the design of 5G networks will open up the potentially large market

of smart transportation for wireless operators. Localization is also one of the significant requirements for autonomous-driving vehicles to acquire the accurate information around the vehicles [17].
5G technology brings the following benefits in the domain of transportation:

- Sustainability
- Safety
- Fleet monitoring
- Navigation and augmented reality
- Eco-system scalability

6.3.4 User Centric Computing

The user receives content after recognizing, interpreting and inferring on big data-based situational information collected through various sensors. Figure 6.9 shows examples of such services. Intelligent health services, such as personal health care, psychotherapy, de-stressing, business coaching, etc., are based on the big data analysis of life-logs. The networks in the future are expected to be more congested due to the increasing number of devices and data traffic. This increases network delay and would occur to create a threat regarding the connectivity to cloud computing servers. Moreover, it is also useful for mobile services like smart cars, smart health care, industrial automobiles, augmented reality and gaming. Mobile edge computing and accurate big data analysis of data coming from sensors are essential to provide prompt and timely response in the case of any disaster. They are also helpful to counteract climate change and industrial accidents.

Figure 6.9: User-centric computing services

The increasing demand of data traffic requires future 5G technology to increase the data rate and decrease latency. Energy efficient actuators and sensors are necessary to support green communication. Moreover, low-power telecommunication technology is another desirable 5G feature. In short, 5G must provide efficient big data processing and rapid big data transmission with minimum latency. Additionally, accurate localization of mobile terminals is required to provide these services in a timely manner [17].

6.4 Conclusion

By analyzing the emerging technologies like Li-Fi, LoRa and megatrends of future mobile services, the concept of 5G services, which emphasize the realistic experience of end-users, has been established. The next generation of wireless networks-5G-promises to deliver that, and much more. With 5G, users should be able to download a high-definition film in under a second (a task that could take 10 minutes on 4G LTE). And wireless engineers say these networks will boost the development of other new technologies, too, such as autonomous vehicles, virtual reality, and the Internet of Things.
At the moment, it's not yet clear which technologies will do the most for 5G in the long run, but a few early favorites have emerged. Moreover, 5G is still in the planning stages, and companies and industry groups are working together to figure out exactly what it will be. But they all agree on one matter: As the number of mobile users and their demand for data rises, 5G must handle far more traffic at much higher speeds than the base stations that make up today's cellular networks.

Bibliography

[1] Harnit Saini: *LI-FI (LIGHT FIDELITY)-THE FUTURE TECHNOLOGY IN WIRELESS COMMUNICATION*, June, 2016

[2] Harald Haas: *LiFi is a paradigm-shifting 5G technology*, 2017

[3] Lifi-Centre; `https://www.lifi-centre.com/about-li-fi/applications/`, *accessed May 2, 2018*

[4] Products, Pure-Lifi; `https://purelifi.com/lifi-products/`, *accessed May 1, 2018*

[5] Case Studies, Pure-Lifi; `https://purelifi.com/case-study/babcock-powered-by-purelifi/`, *accessed May 1, 2018*

[6] Case Studies, Pure-Lifi; `https://purelifi.com/case-study/transforming-internet-at-bt-2/`, *accessed May 1, 2018*

[7] LoRa-Alliance; `https://lora-alliance.org/`, *accessed May 02, 2018*

[8] Semtech; `https://www.semtech.com`, *accessed May 02, 2018*

[9] Link Labs: *selecting a wireless technology for New Industrial Internet of Things Products*; `https://www.link-labs.com/lora`, *accessed May 02, 2018*

[10] Prasanna Adhikar: *Understanding Millimeter Wave Wireless Communication*; `http://www.loeacom.com/`, *accessed May 02, 2018*

[11] Belcher, Rober: *EXTREMELY HIGH FREQUENCY (EHF) LOW PROBABILITY OF INTERCEPT (LPI) COMMUNICATION APPLICATIONS.* MS Thesis. Naval Postgraduate School, 1990. PDF file

[12] MiWaveS White Paper 1: *Heterogeneous Wireless Network with mmWave Small Cell Access and Backhauling*; `http://www.miwaves.eu`, *accessed May 02, 2018*

[13] MiWaveS White Paper 2: *Heterogeneous Wireless Network with mmWave Small Cell Access and Backhauling*; `http://www.miwaves.eu`, *accessed May 02, 2018*

[14] Erik G. Larsson: *Massive MIMO for 5G* LinkÃ¶ping University, LinkÃ¶ping, Sweden and Liesbet Van der Perre, KU Leuven, Leuven, Belgium, March, 2017

[15] Rohde and Shwarz White Paper : *Millimeter-Wave Beamforming: Antenna Array Design Choices and Characterization*; `https://www.mtt.org/sites/default/files/whitepapers/beamform_mmw_antarr.pdf`, *accessed May 02, 2018*

[16] WALEED EJAZ, ALAGAN ANPALAGAN, MUHAMMAD ALI IMRAN, MINHO JO, MUHAMMAD NAEEM, SAAD BIN QAISAR, WEI WANG: *Internet of Things (IoT) in 5G Wireless Communications* , January, 2016

[17] Heejung Yu, Howon Lee, Hongbeom Jeon: *What is 5G? Emerging 5G Mobile Services and Network Requirements* , October, 2017

[18] Alisha Seam, Amy Poll, Remound Wright, Dr. Julius Mueller, Faraz Hoodbhoy: *Enabling Mobile Augmented and Virtual Reality with 5G Networks* , January, 2017

[19] Smart vehicles and transport, Ericsson-5G; `https://www.ericsson.com/en/5g/use-cases/smart-vehicles-and-transport`, *accessed May 3, 2018*

Chapter 7

An Overview of Blockchain Interoperability

Vasileios Koukoutsas, Te Tan

Blockchain technology has experienced a fast development over past years driving its usage in many application areas beyond FinTech (Financial Technology). Different areas has different requirements and thus, different blockchain usage scenarios are being developed. Cross-chain interoperability becomes the key to answer questions like How to do transactions cross different blockchains and how to overcome the scalability problem of blockchains. In this paper, a summary of the current and potential approaches to cross-chain interoperability is presented. Then, challenges towards interoperability implementation will be discussed. Finally, we will talk about some use cases of interoperability.

Contents

7.1 Introduction

Since Satoshi Nakamoto proposed Bitcoin in 2008 [1], there has been a surprising growth of cryptocurrencies powered by blockchain technology. According to coinmarketcap, there are more than 1500 types of cryptocurrencies available in the market [2]. More than just cryptocurrencies, blockchain technology has experienced a thriving development. For example, Ethereum acts as a successful platform which enables convenient development and execution of Smart Contracts [3].
Different organizations and various use cases have lead to many blockchain implementations. Hence it becomes more and more important that these individual blockchains can "*talk*" to each other. Taking Supply Chain for instance, the adoption of blockchain solution could help improve the efficiency and transparency of products' flow. However, many organizations which are related to a specific supply chain may implement their own blockchain respectively. Hence, there comes the need for information sharing between these blockchains across the supply chain flow. Another problem that cross-chain interoperability can mitigate is scalability. The data storage capability of blockchain is limited by the time needed to create a block and the block size. One possible method is to store the data in multiple blockchains in parallel, with the help of interoperability. Cross-chain interoperability has been identified by Underwood as one of the key challenges to blockchain technology [4].
This report summarizes approaches aiming at solving the cross-chain interoperability problem. Then, use cases in which cross-chain interoperability plays an important role are discussed to overview different approaches towards interoperability.

7.2 Approaches to interoperability

In this section, we summarize the approaches which already have or could potentially enable cross-chain interoperability.

7.2.1 Notary

Technically speaking, the *Notary* is the simplest way to facilitate cross-chain interoperability [5]. In this mechanism, one trusted or a set of trusted entities is used to claim whether an event happened on a blockchain. In order to explain this mechanism more intuitively, we introduce the Interledger, which is an advanced implementation of Notary mechanism [6]. *Interledger* is a protocol which enables interledger transactions with the help of the nodes which have accounts on both ledgers (blockchains). There are three kinds of roles in Interledger: *sender*, *receiver* and *connector*. A sender is someone who wants to initiate a cross-ledger transaction with the receiver. A connector is a node who facilitates the transaction by coordinating the asset transfer on multiple ledgers.
Figure 7.1 shows how Interledger makes cross-ledger transaction possible. Figure 7.1 *a* shows connector's functionality: to transfer the asset from A to B, A can first transfer it to C on one ledger, and then C transfer it to B on another ledger. This can be extended to the case which involves an arbitrary number of connectors as shown in picture *c* (so-called payment chain). However, in picture *a* nothing prevents C from misbehavior like stealing the money. So Interledger protocol introduces *escrow* and *notaries*. At the beginning of the transaction, the sender will select his trusted notaries, whose role is to coordinate and synchronize the transaction. Escrow is an intermediate between participants. All the participants only transfer their assets to their respective escrows, who will only execute to transfer the asset to the next participant when they received the *Execute Message* from (most) notaries. Taking picture *c* in Figure 7.1 for instance, after P_{n-1} has transferred

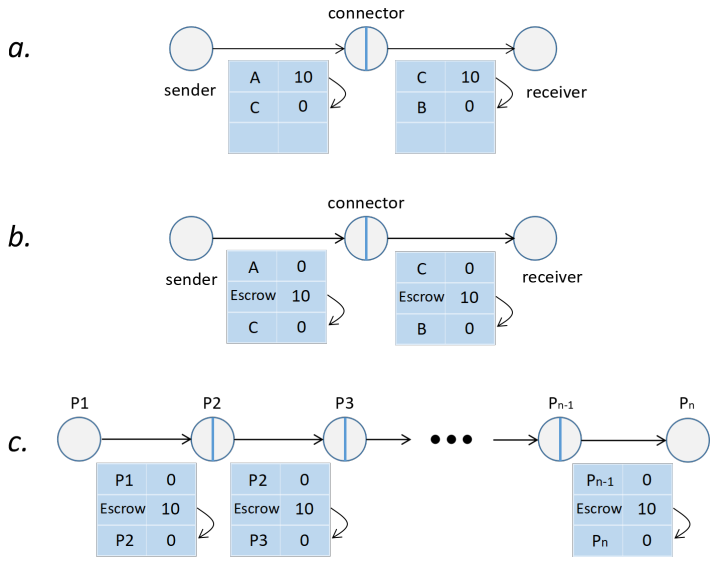


Figure 7.1: Cross-ledger transactions enabled by Interledger protocol

the asset into its escrow, P_n has to sign a receipt and send it to all notaries. The notaries will decide whether they receive the receipt in time. If they do whey will sign a Message of *Execute* and send it to all participants. Finally, the transaction will execute, and every participant claims their assets.

7.2.2 Sidechain/Relay

Sidechain(or Relay) approach is proposed by Adam Back et al. which aims to enable bitcoins and other ledger assets to be transferred between multiple blockchains [7]. A sidechain is a blockchain that validates data from other blockchains. Instead of relying on intermediaries as Notary does, blockchains do information validation by themselves. The blockchain from which the sidechain verifies data is called as the main chain or parent chain.
The sidechain will use the standard verification procedure to verify the block header from the main chain. To explain how it works, we take the blockchain with proof-of-work as the consensus algorithm as our example. We will first explain how a sidechain validate a transaction happened in the main chain. Then based on that, we introduce how to enable asset portability with the help of sidechain.

7.2.2.1 Verify a transaction in another chain

Suppose a blockchain A is going to verify whether a transaction TX took place in blockchain B. In this case, chain A is the sidechain and chain B is the main chain. Two steps are needed: first A will verify the block header containing TX has been finalized, then A will verify the specific TX against the block header.
Validate the block header: chain A uses the same consensus algorithm as chain B which is proof-of-work, which works as follow:

1. *verify proof-of-work:* chain A fetches the block header from chain B which contains the targeted transaction. The information contained in the block header is shown in Table 7.1. To generate a block in the proof-of-work based blockchain, a certain amount of computational efforts should be invested. Validators must solve a hashing problem in which a solution named Nonce(as shown in Table 7.1) should be found. The difficulty of this hashing problem is constrained by Difficulty target. The inherent characteristic of hashing problem ensures that the exploitation of solution

is hard while the verification of the solution is easy. Only Blocks with the correct Nonce are regarded as valid. What chain A does is verifying whether this Nonce is the correct answer to the hashing problem. If it is, chain A thinks the block is valid.

2. *wait until the block is finalized:* a valid block is not enough to confirm the transactions in the blockchain. To mitigate the risk of reorganization, chain A has to wait until a few more blocks have been generated on chain B. Reorganization occurs when more than one block has formed and added to the blockchain simultaneously, which lead to the formation of forks. Then further blocks will be added on these forks. In proof-of-work based blockchain, only the longest fork, which represents the fork with the most computational efforts invested, will be kept and all other forks will be discarded. Hence chain A need to wait for a few more blocks to be generated to ensure the target block is finalized.

Table 7.1: Information contained in the block header

Field	Description
Version	The version number of blockchain
Previous block hash	the hash code of previous block
Merkle root	the hash code of the root of the Merkle tree
Timestamp	the timestamp of the block
Difficulty target	the difficulty target for the formation of the block
Nonce	the counter used by validators to generate a block

Verify the target transaction: after the validation of block header, chain A will then verify the target transaction. As shown in Table 7.1, there is a field named Merkle root within the block header. Merkle root is the root hash code of the Merkle Tree, which is a layered tree structure of the hash code. The leaves of the Merkle Tree are the hash codes of each transaction stored in the block. Every non-leaf node is the hash code of its child nodes. The root hash code of this tree is included in the block header. An example of Merkle Tree is shown in Figure 7.2.
With the help of Merkle Tree, chain A can verify a particular transaction by downloading a single branch of Merkle Tree, instead of downloading the whole block. For instance, if chain A wants to verify transaction *L4* in Figure 7.2, chain B will give him following nodes: *Hash 1-0* and *Hash 0*. Chain A will then compute *Hash 1* from hash code of *L4* and *Hash 1-0*, and next he will compute *Top Hash*(Merkle root) from *Hash 1* and *Hash 0*. If the computed *Top Hash* is the same as the Merkle root he got from block header, the transaction *L4* is valid.

7.2.2.2 Asset portability enabled by sidechain

Above we explained how the sidechain validates a transaction in the main chain, the same approach can be used to enable the asset portability between sidechain and the main chain. Figure 7.3 explains how the asset of user A on the main chain can be transferred to user B on the sidechain. The first user A launches a transaction, sending his asset to a special address on the main chain which will lock this asset. Then the sidechain will rely on the validation procedure described in the last subsection to verify this transaction on the main chain: A has sent the asset to the special address. Note that once the asset has been sent to the special address successfully, it can only be unlocked by the sidechain, who will use its consensus algorithm to confirm that A's asset has not been spent elsewhere. After the confirmation of A's transaction, the sidechain will create a new asset on itself, which

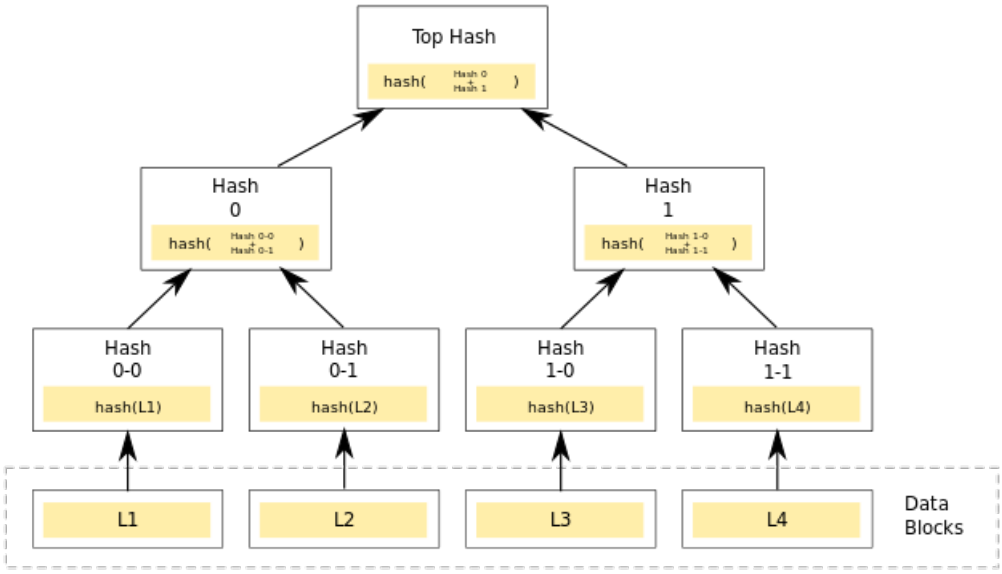


Figure 7.2: An example of the Merkle Tree structure [8]

A can use for further transactions on the sidechain without constraints. For example, A can transfer it to B as shown in Figure 7.3.

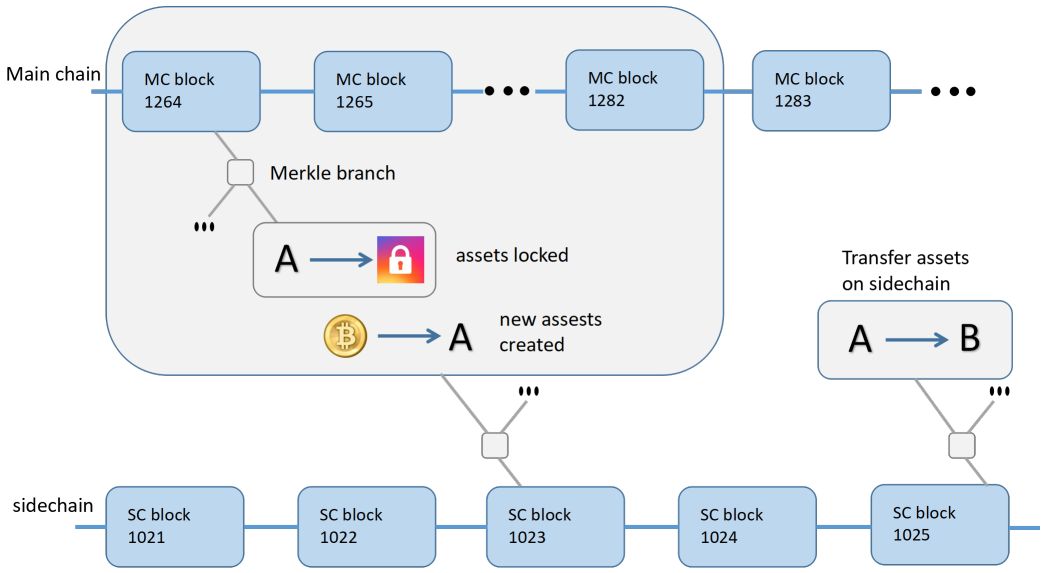


Figure 7.3: Asset transfer enabled by sidechain

7.2.3 Hash-locking

Hash-locking is another well-known technique to achieve cross-chain assets exchange[5]. One of the biggest advantages of Hash-locking is that it requires no notary or sidechain. Its limitation is also obvious: it can only use for atomic operations, not for asset portability. Figure 7.4 shows how this mechanism works. In this case, A wants to exchange assets with B. Firstly A generates a random secret s, computing its hash h and sending it to B. Secondly A locks his asset into a smart contract, B also locks his counterpart asset into a smart contract after he verifies A did so. Then it comes to the stage of claiming assets. If B receives the correct secret s from A within X seconds, B's asset will be transferred to A. Similarly, if A receives secret s from B within $2X$ seconds, A's asset will be transferred

to B. Note that in order to claim the asset from B, A must reveal the secret s within X seconds, which ensures B has at least X seconds time window to claim the asset from A because A has to wait for $2X$ seconds according to the mechanism.

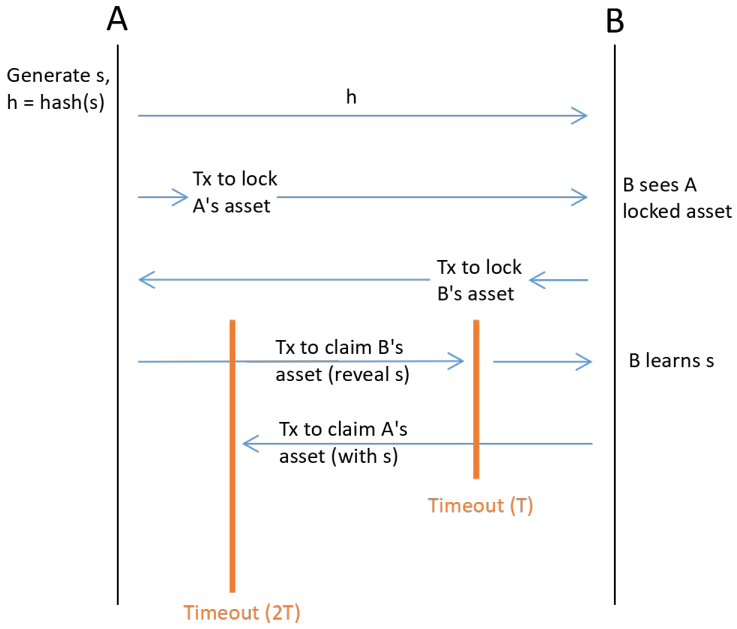


Figure 7.4: Hash-locking mechanism

7.3 Challenges to cross-chain interoperability

In this section, we will discuss the challenges to interoperability as mentioned above mechanisms, as well as promising techniques to solve these problems.

7.3.1 Scalability

One of the biggest limitations of blockchain for widespread use, especially in financial markets, is lack of scalability. This problem largely comes from the underline consensus algorithms adopted by blockchains. Taking the sidechain explained in Figure 7.3 for instance, whose consensus algorithm is proof-of-work. When the sidechain wants to verify that A has locked his asset successfully into the special address, firstly it should wait the time of block generation, which is about 10 minutes with large variance. After the block is generated, to lower down as much as possible the risk of reorganization(forks may emerge), the sidechain has to wait until several additional blocks have been created. This considerable latency undermines many commercial applications, which requires nearly instant execution.

A few researchers are trying to solve this problem and proposed different strategies. One promising solution is so-called *Strong Federation*. *Strong Federation* is a sidechain which introduces some advanced properties such as publicly verifiable, privacy protection, and most importantly, low transaction confirmation time [11]. To significantly lower the transaction latency and eliminate the risk of reorganization, *Strong Federation* adopts a group of fixed signers named *Blocksigners* and replace proof-of-work with a multisignature scheme. The formation of different forks in proof-of-work is because there are many subgroups of validators working on generating different blocks. Hence using a fixed group of signers on sidechain to validate the transaction will eliminate the risk of reorganization. Furthermore, the adoption of multisignature which is a mechanism requiring blocks to be signed

by a certain threshold of signers, will largely lower down the confirmation time of one block.

Another solution which is potentially suitable for commercial adoption is *Herdius*, which provides a different method dealing with the scalability problem [9]. *Herdius* is another sidechain solution which adopts proof-of-state as the consensus algorithm. This will lower down the time of transaction confirmation largely. Furthermore, it introduces the concept of *stretched block*. As shown in Figure 7.5, Herdius uses a transaction queue to gather transactions formed from the time of the generation of the last block up to now. If the transactions do not exceed the normal size of one block, Herdius chain will generate a singular block next time. If the number of transactions is too large for a singular block to hold, a stretched block will be generated, with a tree structure of a few more blocks whose root points to the regular block on the main chain. To verify these blocks, validators will be split into subgroups. In this way is Herdius chain able to handle a large number of transactions in parallel and hence the transaction throughput will increase significantly.

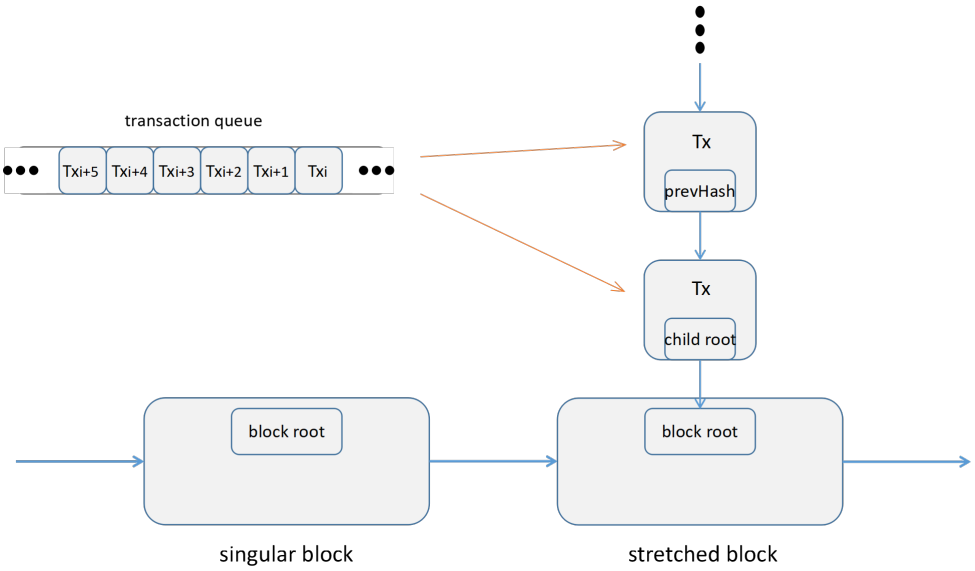


Figure 7.5: The block structure and transaction queue of Herdius

7.3.2 Security

Security has always been one of the most critical issues in blockchain and its ecosystem. However, in a multi-chain context, the security model is difficult to construct. Interoperable blockchains have different security models, and cross-chain information transmission also needs to be modeled. For instance, 51% attack is not likely to happen if the profit of reversing one block cannot cover the costs of large-scale resource manipulation, which means economical, infeasibility prevents attackers from attacking. However, in the context of multi-chain, transactions can involve multiple participants from different blockchains as well as multiple applications running on these blockchains. It may be that a 51% attack is not feasible when the involved value does not exceed 50000 in a single application, but it can be profitable when the attack can affect thousands of such applications. Therefore, security model in a multi-chain case should be treated differently.

7.3.3 Practice

As mentioned in [5], use cases involving blockchain interoperability will take a long time to come to fruition, since the set of dependencies is large and it is indeed resourced consuming. Cryptocurrency exchange is one driving force for the implementation of interoper-

ability system, and further use cases such as finance also motivate the works. Even though there are a few solutions proposed, most of them are still at the theoretical stage(theories and mechanisms are described in their whitepapers). The best practice and systematic methodology of cross-chain interoperability are still on its way to being explored.

7.4 Use cases of interoperability

7.4.1 General Purpose

A general purpose system for blockchain interoperability using 2-way pegged sidechains is *Strong Federations* by Blockstream. A Strong Federation is a group that serves as a mutually-incentivized protocol adapter between an "anchor chain" and one of its sidechains and acts as a unit to ensure forward progress of the sidechain. Using cryptographic tools and secure hardware, the participants construct a Byzantine-robust smart contract wherein each "functionary" is economically incentivized to operate in the best interest of the network by the mutually agreed upon rules.
While leveraging proof-of-work provides Bitcoin with unprecedented security for transaction history, this benefit comes at a cost in latency and throughput. Strong Federations address the delay by introducing a deterministic set of participants each with two responsibilities: generating valid blocks and enforcing withdrawal rules. Transactions are published in blocks that must be made visible to all participants in the network and validated. Pre-commitments are made and then blocks signed. This coordination is measured in seconds as opposed to minutes for Bitcoin. As in Bitcoin, the knowledge of a private key is sufficient for the "right to spend" without the permission of any third party [7].
The system process flow includes the following steps:

1. The user sends their asset to a special address that is designed to freeze the asset until the sidechain signals that asset is returned.

2. Using the *in* channel of a federated peg, the user embeds information on the sidechain stating that the asset was frozen on the main chain and requests to use it on the sidechain.

3. Equivalent assets are unlocked or created on the sidechain, so that the user can participate in an alternative exchange under the sidechain rules, which can differ from the parent chain.

4. When the user wishes to move her asset or a portion thereof, back via the "out channel," she embeds information in the sidechain describing an output on the main blockchain.

5. The Strong Federation reaches a consensus that the transaction occurred.

6. After consensus is reached, the federated peg creates such an output, unfreezing the asset on the main blockchain and assigning it as indicated on the sidechain.

A high level overview of the system is shown in Figure 7.6

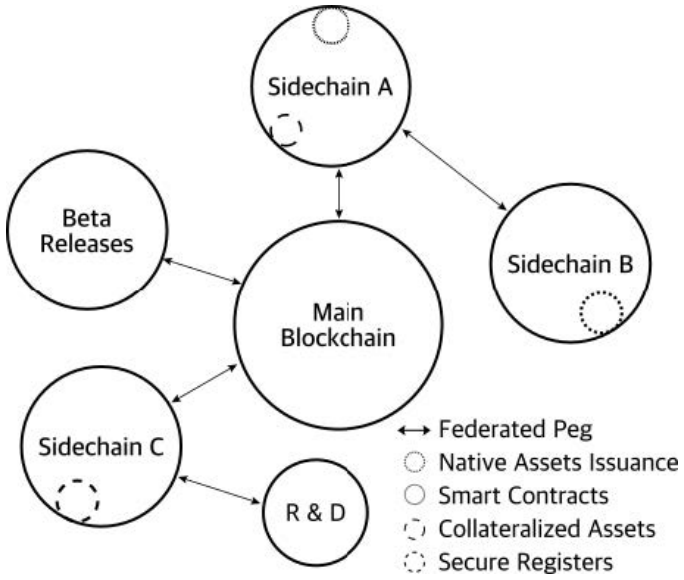


Figure 7.6: Pegged sidechains allow parties to transfer assets by providing explicit proofs of possession in transactions

Strong Federations could potentially be implemented to serve different kind of decentralized blockchain based applications and use cases.

7.4.2 Financial markets and Assets Portability

An implementation of Strong Federations aimed to serve the financial markets is *Liquid* which is an interoperable sidechain that extends the Bitcoin blockchain while adding an auditable, cryptographically-strong commercial privacy component. Using this arrangement, Liquid leverages the reliability and security of the Bitcoin network without trusting a centralized third party. This new construction establishes a security profile inherently superior to existing methods of rapid transfer and settlement, and is directly applicable to other problems within existing financial institutions.
Using sidechain technology, Liquid reduces ISL by allowing for rapid transfers between accounts held by the varied participants in a separate, high-volume and low-fee cryptographic system that preserves many of the security benefits of the Bitcoin network. This, in addition to increasing the security of funds normally subject to explicit counterparty risk, fosters conditions that increase market liquidity and reduce capital requirements for on-blockchain business models [15].
Benefits of Liquid:

1. **Faster Trading** Near instant bitcoin transfers between exchanges allow your users to take advantage of arbitrage opportunities like never before.

2. **Enhanced Efficiency** Market makers can improve their capital efficiency by reducing balances held across multiple exchanges.

3. **Better Privacy** Liquid supports Confidential Transactions for bitcoin amounts transferred in the system, which protects your users from exposure.

4. **Superb Reliability** Built using the battle tested Bitcoin code-base, Liquid software is highly reliable. Also, since Liquid uses signed blocks instead of mining, blocks are always one minute apart instead of an unknown amount of time like Bitcoin.

The participating exchanges and Bitcoin businesses deploy the software and hardware that make up the Liquid network so that they can peg in and out of the Bitcoin blockchain

and offer Liquid's features to their traders. Liquid provides a more secure and efficient system for exchange-side bitcoin to move across the network. End users benefit from the greater liquidity Liquid enables between exchanges.
Liquid is a federated sidechain, so it will never be as decentralized as Bitcoin. However, Liquid is designed to remove control from any single party, geographic location, or political jurisdiction. The Liquid Network is operated by functionary servers, each securely hosted by geographically dispersed, independently owned and operated Bitcoin exchanges. Updates are deployed by consensus of participants within the network. No single party, including Blockstream, can control the Liquid network, and furthermore, no single entity is in control of more than a single Liquid functionary server.
Liquid is built using the Elements blockchain platform and therefore has multi-asset issuance capabilities built in through the Confidential Assets feature. In its first release, Liquid will support Bitcoin only. Future versions of Liquid may support other assets, such as other cryptocurrencies or assets issued by participants [14].

7.4.3 Cross-chain Contracts

Aelf is a crosschain blockchain protocol that creates a highly efficient and customizable OS that will become the "Linux system" of the blockchain community. It focuses on defining and providing the most basic, essential and time-consuming component of the system and making significant improvements based on existing chains in the market. The system allows developers to customize it to meet their own needs, particularly commercial requirements for various industries. Firstly, the Aelf kernel is defined and implemented which includes fundamental functions of a blockchain system, namely the minimum viable blockchain system. Secondly, a "shell" is developed as the basic interactive interface to the Core. Users can either use the complete Blockchain OS or rapidly develop a customized OS based on the Core via redefining the Core through interfaces. [16]
Aelf consists of one main chain and multiple sidechains which are attached to it as it is shown in Figure 7.7.

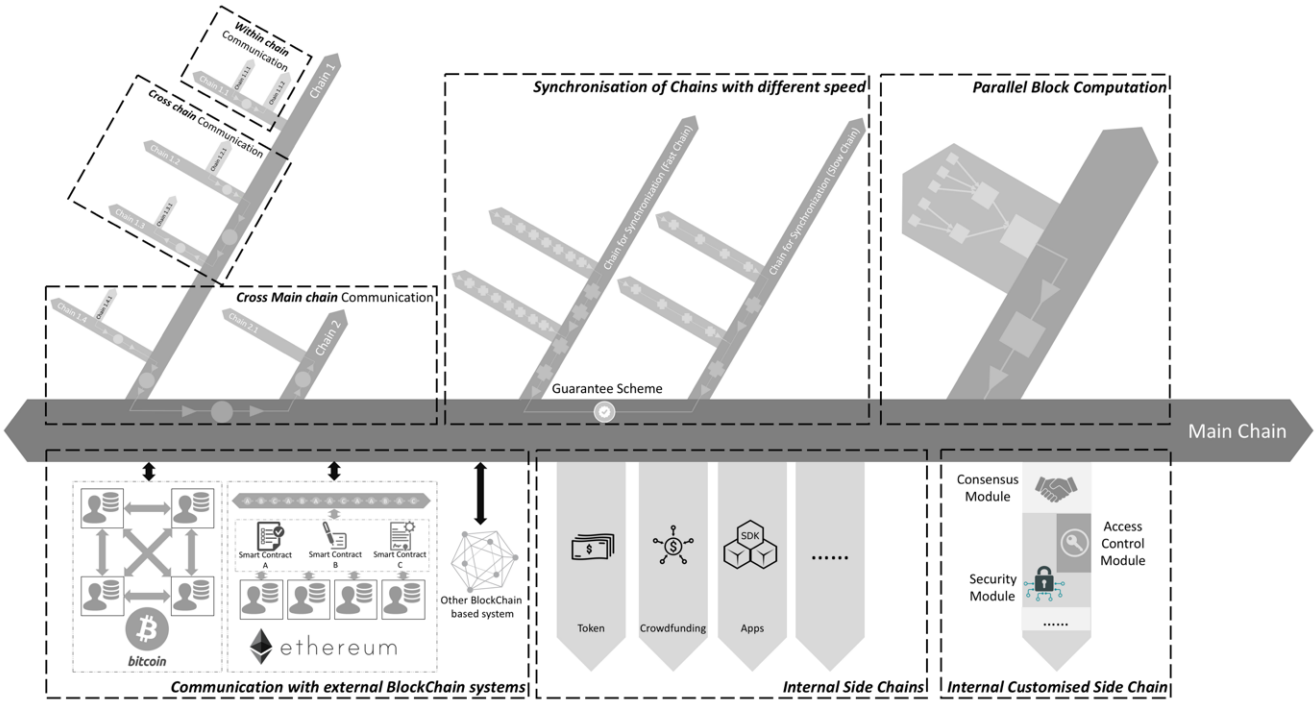


Figure 7.7: Overview of Aelf structure

Aelf will support the below main features [16]:

1. Introduces the concept of Main Chain and multi-layer Side Chains to handle various commercial scenarios. One chain is designed for one use case, distributing different tasks on multiple chains and improve processing efficiency.

2. Enables Aelf to communicate with external blockchain systems via messaging (e.g., Bitcoin, Ethereum).

3. Permits parallel processing for non-competing transactions and cloud-based services.

4. Defines basic components of minimum viable Block and Genesis Smart Contract collection for each chain to reduce data complexity and achieve high customization.

5. Permits stakeholders to approve amendments to the protocol, including redefining the Consensus Protocol. Permits sidechains to join or exit from the main chain dynamically based on COnsensus protocol, therefore introducing competition and incentive to improve each sidechain.

Each node in Aelf is a computer cluster network (e.g., a cloud network) instead of a singular computer. By leveraging cloud networks as nodes, Aelf aims to further empower the network participants with higher computational power as well as the storage capability. The parallel processing algorithm is developed and integrated to each node to ensure the optimal utilization of all the participating computers in the cloud network. When a node handles a complex set of transactions within a smart contract, it will dissect the transactions into groups of those that do not demonstrate interdependency and process them in parallel simultaneously. Consequently, the takt time is minimized and the overall processing speed maximized. A node's capacity can be easily scaled by adding new computers to the existing network without having to upgrade the node computer's hardware. [17]
As a multichain network, each side chain is independent of one another, and smart contracts reside are executed directly from a side chain, not through the main chain. This enables each side chain to be impervious to the high traffics on another chain, thereby localizing the traffic concentration and guaranteeing consistent transaction speed for smart contracts executed in other side chains. Each side chain would also have the ability to host its own set of nodes to guarantee low traffic and determine its processing speed. Each side chain is specialized for a specific business scenario, e.g., token issuance (ICO), an insurance database, in-game transactions, etc., and their consensus protocol, node delegation, chain privacy and various other chain qualities can be tailored to best support the specific business scenario. The main chain acts as the ledger and the communication hub, unlocking highly efficient cross chain communication, triggering of smart contracts across side chains and effective synchronization between chains with different speeds. [17]
Aelf aims to bestow its network participants an entirely self-evolving authority and capability through its voting protocol. Aelf coin holders will have the ability to vote on a diverse sets of critical decisions that will collectively shape the eco-system; this includes the decision for each side chain to host their own delegated node, choose whether the participating side chain will be public or private, determine the size and the speed of the side chain, remove or add side chains to the network, etc. Aelf utilizes Merkle tree root based chain indexing to communicate and interoperate with other consensus protocol based blockchains such as PoW and PoS. Aelf provides side chain templates to its developers for rapid smart contract development for those who do not have the in-depth understanding and capacity for ground-up smart contract coding. [17]
Aelf is intended to become the new "internet infrastructure" to support the next generation of "digital businesses." Some potential applications include:

1. **Financial Services** It is highly likely that multiple chains on Aelf will be developed specifically for financial services, such as cross-border payment, trade finance, supply chain financing, etc. The parallel processing feature is capable of handling business transactions at the international scale, and the inter-chain communication feature allows smooth coordination from asset registration, account management, real-time transaction.

2. **Insurance** A dedicated Aelf side chain for insurance will integrate various DAPPs for insurance, transforming the whole industry value chain, starting from user identity, to insurance contract execution, to claim to handle.

3. **Digital Identity and IPs** Aelf's multi-chain structure has a built-in chain for digital identity. This ensures the performance of such side chain if another side chain is busy. Within Aelf, digital identity can be used by other side Chains via "messaging." Using adaptor, Aelf is also capable of retrieving information and data from other established chains, such as Bitcoin and Ethereum.

4. **Smart City** Governments or organizations can customize the consensus protocol to meet national security requirement. Activities, such as utility recording, citizen identities, government agency information disclosure and polling can be realized on Aelf with high transparency and efficiency. A few countries are experimenting in this field, including Estonia, Singapore, China, etc.

5. **Internet of Things** Aelf supports light node and cloud service, which reduces the computational requirement for devices connected to it while maintaining high performance. This is critical to managing billions of devices and enables micropayment across them to link internet of things [16].

7.4.4 Supply Chain

Origin Trail is a decentralized protocol that has been designed to share supply chain data via the use of a completely transparent network. Origin Trail makes use of a blockchain that builds on well-established industry standards as well as promotes a P2P network that fosters consumer confidence, optimal supply chain efficiency, automated compliance and quality assurance. Every stakeholder is given the ability to securely share and store their data via encrypted channels. Origin Trail is also fully compatible with existing ERP systems, thereby making the implementation process highly streamlined and uncomplicated. Lastly, the Origin Trail ecosystem is regulated through a tokenized economy model that minimizes the possibility of collusion and introduces full accountability for the provided data. Users can develop direct relations with one another, and all of the network nodes facilitate internal transactions without incurring arbitrary fees; something that is commonly experienced by users of centralized data platforms. [18]
The two key factors that impede data collection and sharing in supply chains are:

- **Data is fragmented** Data siloes and low data interoperability exist across the supply chain in both multi-organisation and single-organization supply chains. There is a crucial technical challenge for various IT providers for supply chains (software and IOT) that need to be resolved to collaborate and establish full supply chain transparency. An illustration of data siloes is shown in Figure **??**

- **Supply chain data is centralized** It is aggregated by one or several entities prompting concerns about data integrity and omitting accountability. The centralized administration also allows for the possibility of data tampering and collusion between parties. By creating a decentralized system, we establish an environment

of complete accountability for all data as well as entirely remove the possibility of data tampering and collusion. [18]

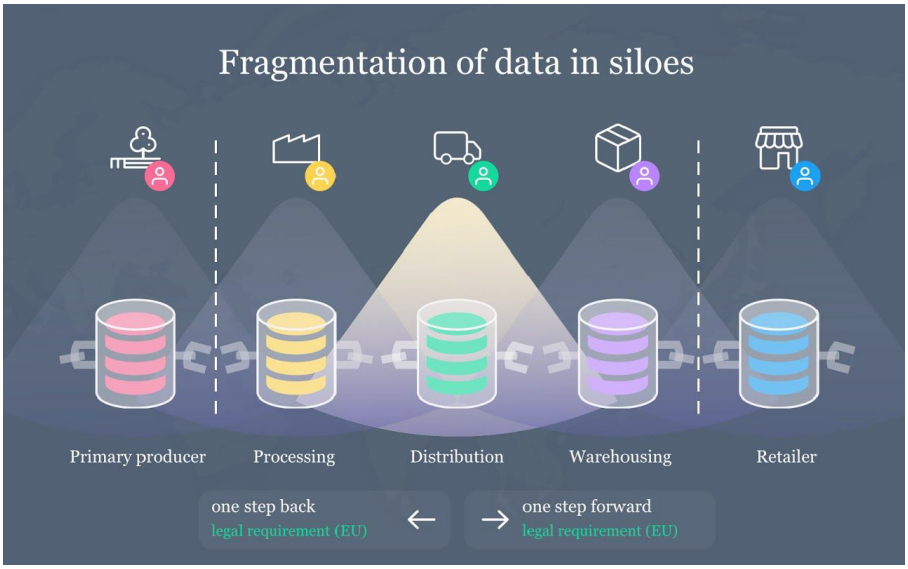


Figure 7.8: Supply chain data fragmentation in siloes

OriginTrail protocol runs on an off-chain decentralized peer to peer network, called the OriginTrail Decentralized Network (ODN). It enables peers on the network to negotiate services, transfer, process and retrieve data, verify it's integrity and availability and reimburse the provider nodes. This solution minimizes the amount of data stored on the blockchain to reduce cost and inefficiency. An overview of the Origin Trail solution stack is shown in Figure 7.9.

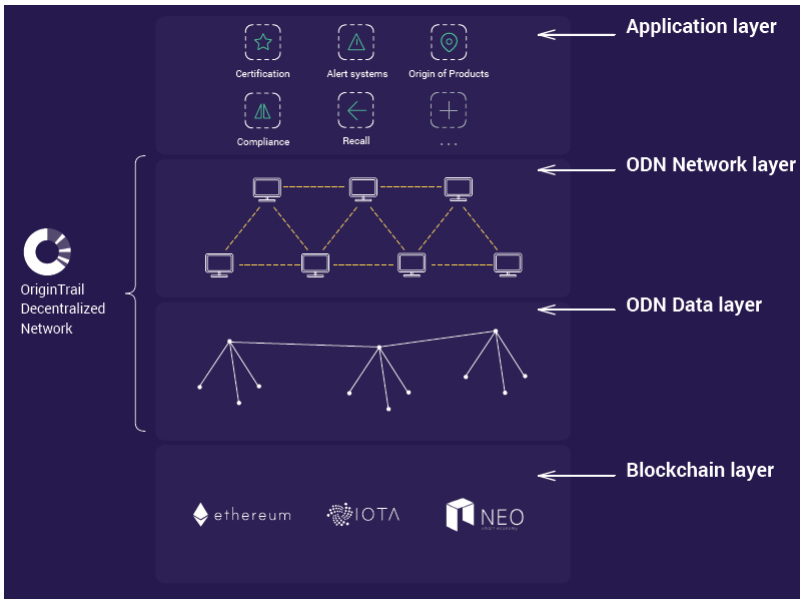


Figure 7.9: Supply chain data fragmentation in siloes

The main layers of Origin Trail solution stack are:

- **Application layer** The application layer is the built on top of the ODN network capabilities and presents the ground for implementing the consumer-facing instances - decentralized applications built by developers, explained further in this document.

- **ODN Network layer** The network layer takes care of the accessibility and data governance of the underlying data layer. It consists of a network of nodes which all contain parts of the decentralized database and store supply chain data in graph form. Access to the data is achieved through the provided data exchange API.

- **ODN Data layer** The data layer of ODN takes care of all the necessary data management and connectivity functionalities. Because of the need to connect many different data sets across the supply chain, while providing the flexibility to support many different connection options, data relationships are the key focus of the data layer. Therefore the basis of the data layer is a decentralized graph database.

- **Blockchain layer** OriginTrail incorporates blockchain as the platform to ensure data integrity and trusted payments. All the data entering the system gets immutably "fingerprinted" in the blockchain (using a cryptographic hash) which provides for a tamper-proof mechanism for supply chain data. The blockchain layer allows the OriginTrail network to utilize different blockchains for fingerprinting which provides flexibility and ensures the longevity of the protocol by not having "blockchain lock-in" to one single platform.

OriginTrail enables seamless and automatic data connection and interoperability between IT systems of different stakeholders in multi-organisation supply chains with consensus mechanisms for ensuring the integrity of data. Interoperability is delivered by integrating globally recognized GS1 standards for Master Data (descriptive attributes for products), Transaction Data (related to business relations), Visibility Data (related to tracing and tracking). Other data sets will include IoT and compliance data. A consensus among entities in the supply chain is achieved by performing cross-reference checks every time a new data set is added to the protocol. This ensures the entire supply chain is in accords regarding a particular batch of products. If there is no consensus, discrepancies can be quickly reported, investigated and reconciled. [19]
The consensus check is performed in 3 steps:

1. Creating a chain of accountability by mutual approval of supply chain stakeholders.

2. Matching of dynamic batch information is verified. Sensitive data is protected by a zk-SNARKs implementation.

3. Auditing and compliance organizations confirm the provided data.

Once the service providers configure the automatic data input (from supply chain ERPs, IoT devices, online and brick & mortar retails stores, etc.), it is introduced to Data Creator (DC) nodes which disseminate the data in the network to other Data Holder (DH) nodes for safekeeping, fingerprinting, performing data standardization checks, consensus checks and creating connections with other already available supply chain data in the system. Finally, supply chain data is read from the nodes by the decentralized applications from the application layer. All the nodes are reimbursed for these services by Trace tokens in the amounts agreed upon with a bidding mechanism. A system overview is shown in Figure 7.10

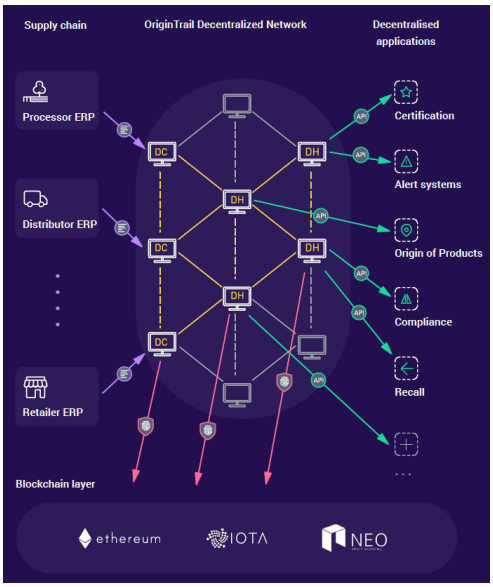


Figure 7.10: System Overview

OriginTrail will deliver the first generic open source applications built on top of the protocol showcasing some of the possible token utilities on the application level:

- **Tokenized data ownership** Creating models where data is sold up/down the supply chain using Trace will be created. This is especially important for primary producers where (production) data is a valuable asset that is currently insufficiently addressed. Using applications built on top of OriginTrail protocol they can take control over their data ownership and earn Trace from providing it to industry partners.
- **Tokenized reputation system** Will be stimulated to share reviews on products and services and contribute to the reputation system made possible by the protocol. Any supply chain stakeholder will be incentivized to provide a review of the product/service with Trace.
- **Tokenizing consumer engagement** Trace tokens will be awarded to end consumers in exchange for interaction with products and services.

Other application instances are to be created by direct users of the system IT providers. Examples of applications where OriginTrail's protocol delivers value are product authentication, supply chain mapping, inventory management, alert systems, supply chain compliance assurance and customs, audit and regulations process optimization. [19]

7.5 Conclusion

Due to the increasing adoption of the blockchain across the industry, Cross-chain interoperability has become an important solution to deal with problems like blockchain communication and scalability. In this report, we introduced the potential approaches to enabling cross-chain interoperability, which is Notary, Sidechain, and Hash-lock. Notary mechanism relies on a set of entities(notaries) to verify whether an event happened on other blockchains. Sidechain avoids intermediaries by validating transactions themselves. Hash-lock uses a smart contract to enable asset-exchange from different blockchains. Then we discussed the current challenges to cross-chain interoperability, including scalability, security, and practice.

The potential use cases for blockchain interoperability are numerous and difficult to predict. In this report, we identified and analyzed a few of the most prominent candidate use cases such as financial markets and assets portability, cross chain smart contracts and supply chain. Almost all currently known blockchain interoperability use cases fall under one of these three categories. It is important to note that blockchain as an industry is still in its infancy and the first applications other than cryptocurrencies entered the market commercially at the end of 2017. Therefore the immediate need for blockchain interoperability is not present. All use cases studied are still in a design phase, or at best in a proof-of-concept phase, we will only be able to verify if these solutions are functional, safe and usable after they have been implemented and deployed. If blockchain interoperability manages to address blockchain performance, privacy and lack of complex features limitations it could potentially give a significant boost in the overall industry and allow for a new global economy where easier, faster and more secure interactions of both systems and people from around the world are possible.

An important design decision will have to be made for all the potential projects that aim to solve blockchain interoperability. The designer of the new system will have to decide whether to entrust a third party or not to handle their transactions and consequently their data. If the Notary or Sidechain solution is used then a third party is needed no matter how the system is designed. By using the hash-locking technique there is no need to entrust a third party, but the implementation can be difficult and has to be done separately for each pair of blockchains. This assumes that all the chains will have to adjust their system and create interfaces. Our prediction is that when humans will have to choose between ease of use and security they will always choose the first over the latter, we have witnessed this kind of behavior repeatedly in the Information Technology sector both at a personal and an organizational level.

Furthermore, there comes other issues along with the adoption of interoperability solutions. The concept of sidechains, is to create extra functional blockchains which have the rights to verify data from other blockchains. This is potentially against the underlying decentralization purpose of blockchain technology. Suppose that in the near future a 'perfect' sidechain has been implemented by a powerful company, which overwhelms any other competitors and dominates the market. The consequence is that there will be more and more blockchains, with the need for data sharing and cross-chain transaction, adopting this dominant sidechain solution. This further enables the company to be the trusted third party in the blockchain ecosystem, which is a direct contradiction to the purpose of blockchain and decentralized applications.

Bibliography

[1] S. Nakamoto: *Bitcoin: A peer-to-peer electronic cash system.*, Bitcoin, 2009. https://bitcoin.org/bitcoin.pdf.

[2] CoinMarketCap: *Cryptocurrency Market Capitalizations*, March 2018. https://coinmarketcap.com/.

[3] Ethereum Community: *Ethereum Blockchain App platform*, March 2018. https://www.ethereum.org/.

[4] Sarah Underwood: *Blockchain beyond bitcoin*, Communications of the ACM, Volume 59, 15-17, November 2016.

[5] V. Buterin: *Chain Interoperability*, R3.com, September 2013. https://www.r3.com/blog/2017/01/23/chain-interoperability/.

[6] S. Thomas, E. Schwartz: *A Protocol for Interledger Payments*, Ripple, October 2015. http://blockchainlab.com/pdf/interledger.pdf.

[7] A. Back, M. Corallo, L. Dashjr, M. Friedenbach, G. Maxwell, A. Miller, A. Poelstra, J. Timon, P. Wuille: *Enabling Blockchain Innovations with Pegged Sidechains*, Blockstream, October 2014. https://blockstream.com/technology/sidechains.pdf.

[8] Wikipedia: *Merkle Tree*, March 2018. https://en.wikipedia.org/wiki/Merkle_tree.

[9] D. Balazs: *Herdius-Next Generation Decentralized Blockchain Financial Infrastructure*, Herdius, February 2018. https://herdius.com/whitepaper/Herdius%20Technical%20Paper.pdf.

[10] T. Euler: *A Cryptocurrency Transaction Layer: A Path for Blockchain to go Mainstream?*, Herdius, January 2018. https://medium.com/herdius/a-cryptocurrency-transaction-layer-86347c6688a3.

[11] J. Dilley, A. Poelstra, J. Wilkins, M. Piekarsk, B. Gorlick, M. Friedenbach: *Strong Federations: An Interoperable Blockchain Solution to Centralized Third-Party Risks*, Blockstream, January 2017. https://blockstream.com/strong-federations.pdf.

[12] Iuon-Chang Lin, Tzu-Chun Liao: *A Survey of Blockchain Security Issues and Challenges*, International Journal of Network Security, Vol.19, No.5, September 2017.

[13] A. Azaria, A. Ekblaw, T. Vieira, A. Lippman: *MedRec: Using Blockchain for Medical Data Access and Permission Management*, 2016 2nd International Conference on Open and Big Data, 2016.

[14] Liquid FAQ: *Liquid FAQ*, https://blockstream.com/liquid/faq/.

[15] Liquid Intro: *Introducing Liquid: Bitcoin's First Production Sidechain*, October 2015 https://blockstream.com/2015/10/12/introducing-liquid.html.

[16] Aelf: *Aelf - A Multi-Chain Parallel Computing Blockchain Framework*, 25 November 2017 https://grid.hoopox.com/aelf_whitepaper_EN.pdf?v=1.

[17] Aelf Summary: *In case you forgot, here is a little refresher on aelf*, 22 April 2018 https://medium.com/@aelfblockchain/in-case-you-forgot-here-is-a-little-refresher-on-aelf-3d5dbc5a1b47.

[18] B. Rakic, T. Levak, Z. Drev, S. Savic, A. Veljkovic: *Origin Trail First purpose built protocol for supply chains based on blockchain* 5 October 2017 https://origintrail.io/storage/documents/OriginTrail-White-Paper.pdf

[19] Origin Trail Overview: January 2017, https://origintrail.io/storage/documents/overview_document-english(Jan%209).pdf

Chapter 8

Commonalities of Network Function Virtualization, Blockchains, and Smart Contracts

Manuel Keller

Network operators are under much pressure to improve their services: On the one side, they need to push prices down for customers, on the other side they need to invest in new technologies and need to provide their services with great stability. With Network Function Virtualization (NFV), providers get a chance at introducing more flexibility into their network and thus react better and faster to future challenges. Instead of using specialized hardware, the same functions are performed by software which in turn can be run on generic server hardware. In combination with Software-Defined Networks (SDN), the traffic can be routed dynamically through these services, thus not requiring them to be in specific locations. This can be used to drive down cost, to increase service quality and more. At the same time, distributed ledger technology has made its way into the mind of the public. At the moment, the main focus is still the financial system, in which blockchain-based cryptocurrencies and startups could potentially redefine the way we handle transaction data. To find potential use cases of blockchain in an NFV environment, we want to establish the main benefits of distributed ledger systems. From there, we can look at how virtualized network functionalities could benefit from those same properties. This is done by looking at state of the art and the research challenges of the NFV environment. Based on that, the viability of such a system is analyzed. The core properties of blockchain are integrity, availability, and immutability. These allow participants to establish trust in an untrusted environment. In the NVF environment, this could be used to tackle the challenge of Orchestration and Management and Monitoring: Instead of storing configurations of the Virtualized Network Functions (VNF) in a relational database, a blockchain can be used. This way, the blockchain handles secure authentication through public and private key cryptography and ensures anonymous (encrypted) storage with high availability. As all changes to the configurations are stored in a transactional format, they can be tracked and audited. Monitoring can be handled by leveraging smart contracts. This ensures that service-level agreements are complied to at all times, or the violating partner is fined. Secondly, NFV and blockchain could drive competition. As network services do not need to be at the provider's premises, they can be outsourced. By using standardized blockchain-based NFV solutions, more competitors could enter the field and offer more specialized services. Also, a smart-contract-based real-time auction system could be used:

Network operators in need of VNF could post the inquiry on the blockchain where vendors could bid on them. This increases price transparency and drives competition.

Contents

8.1 Introduction and Motivation

Traditionally, evolution and improvements in the area of network infrastructure have been slow compared to other areas of computing. Reasons for this situation includes that the complex network topologies require strict function chaining and that the very specialized capabilities led to the development of equally specialized networking hardware. As a result, product cycles are slow and dependencies on specific devices is high. On the customer side of business, the situation is different: Network services are used ever more, leading to increasing workload on the networks' infrastructure. Predicting the increases is hard, as new services are launched, revamped and retired very quickly. At the same time, classical ways of earning money, such as phone calls and SMS, are used less in favour of new IP-based services.
Network Function Virtualization (NFV) is a proposal to decouple the service functions from their specialized physical hardware. It enables the same services to be supplied using generic server-hardware that can be located anywhere. This addresses the provider's challenges by offering the following advantages:

- Scalability: As the network functions can be run as virtualized services on generic servers, scaling up the network infrastructure can be done easily by starting up or turning off instances of network functions as needed.

- Flexibility: Switching from specialized hardware equipment to software allows an easier deployment of services. Providers are not required to install new devices when new services are added, but can instead deploy them instantly for the whole network. It also allows for dynamic service chaining, where traffic is treated differently depending on customer wishes or network needs.

- Cost advantage: As generic servers are used in great numbers in datacenters around the world, the high demand helps to drive down their cost. Using them, service providers can benefit from experience and economies-of-scale. It also allows them to rent server capacity from datacenters instead of building one of their own.

- Security: If new VNF is available to improve a network's security, such a system can be more quickly deployed on the whole network. Using widely-used generic server hardware and open source means that systems can be tested better and more thoroughly than their physical counterparts. Also, security audits are possible.

- faster product lifecycle and upgradeability: In contrast to firmware upgrades, software updates and improvements are very easy to apply. It is a well-known process which can be done step-by-step or all at once. There is also less risk of incompatibilities, as generic server hardware has more performance surplus (if the update results in a higher load) and can be tested more easily.

The blockchain is a data structure, which allows any data to be stored in a distributed ledger. Depending on the implementation and the configuration of a blockchain-based distributed ledger system, different properties can be reached. Two main differentiations are public and the private blockchains.
Public blockchains do not have access restrictions, meaning that anybody can add valid data to it. It operates purely on an incentive-based. By design, any user can verify the state of the system. Using incentives, the system gets users to verify the correctness of any new data that is added to the system. Its most important properties are:

- Immutability: Data stored in the ledger cannot be changed.

- Availability: The distributed ledger is being verified, maintained and made accessible by many independent users. Even if some peers are not accessible, the system still is working.

- Integrity: Participants can verify the state of the system.

Private blockchain differs from public blockchains by having access control. Only allowed participants to get access. This changes the fundamental properties of the blockchain in a way that it is not trustless anymore. Participants have to trust the verifiers and the access control. As such, it is often said to have no significant improvements over a centralized database. However, given a high number of participants, it keeps the availability advantage and given high enough number and trust in the verifiers and operators of the system, immutability, and integrity can still be better than traditional databases.
Blockchains store data in a transactional format. With authentication, a receiver of a transaction can use the received as inputs in further transactions. An interesting addition to this is smart contracts, which are small scripts stored in the transactional data. Clack defines them, et al. [2] as:

> A smart contract is an automatable and enforceable agreement. Automatable by a computer, although some parts may require human input and control. Enforceable either by legal enforcement of rights and obligations or via tamper-proof execution of computer code.

Smart contracts can be used for automation and enforcing. For example, a payment can be made after a condition is satisfied, e.g., that a shipment has arrived or is brought to the postal office. These small programs are only limited in functionality by their maximum script length. Because of their versatility, smart contracts are already being used by major industries to improve drug deliveries (which must be kept at a specific temperature), insurance policies or supply chain management.
Smart contracts do not have technical limits, but their inputs restrict their uses: Smart contracts cannot verify the correctness of information that is gathered outside of the blockchain. In these cases, the authors of the contract need to put trust in a third-party to supply truthful information about the real world. Because of that, smart contracts are not inherently trustless [2].
As blockchain-based systems provide many benefits over traditional databases, people are trying to integrate them with other systems. This paper presents the current research on using blockchain to improve Network Function Virtualization. It is structured as followed: Section 8.2 describes related works. Next, section 8.3 provides an overview of the concepts and their challenges. The following section **??** shows what challenges can be tackled and in section 8.4, a specific example is presented. Section 8.6 concludes the paper.

8.2 Related Work

In [4], the authors address the need for trust in an NFV environment. They consider the reasons why a trusted environment is needed and discuss possible solutions. They highlight that multiple situations are vulnerable to attacks and how added security can be implemented. They propose an attestation server to remotely verify the platform trust state and a TSecO database in which verifies VNF images before booting.
In [9], the author writes about the ecosystem security when using NFV in Software-defined networks (SDN). He argues that both components are highly dependent on controlling and management interactions. Thus, this area needs special attention. He argues that the blockchain's immutability property could be leveraged to guarantee the authenticity

of command messages and to create an authentic log of interactions with the system. However, he was unable to find any research on the topic.
In [13], the authors identify that service chaining in the environment of NFV would greatly benefit from Policy-based Network Management. They identify the advantages of the ability to dynamically reconfigure service graphs and propose an approach to design NFV service chaining graphs based on policies automatically.

8.3 Contextualization

This section presents an overview and the challenges of the two concepts that drive the development of this paper: NFV and blockchain.

8.3.1 Network Function Virtualization

Network Function Virtualization has great potential to change the way service providers operate. The first commercial solutions have already reached the market and a few network provider already use NFV in their network provision. However, most operators are still hesitant to deploy these solutions. This is because NFV is an innovation in a slow-moving industry which is focused on long-term projects. Especially when projects are expensive, the industry is rather going to wait until standardization efforts guarantee that their choice is going to be viable and compatible over a long time horizon. To properly manage the development of NFV and to ensure interoperability, the European Telecommunications partnered up to create the ETSI Management and Operation (MANO) standard and framework. ETSI has been the main proponent of NFV systems, and its framework is the de-facto industry standard for the implementation. Figure 8.1 depicts their reference NFV MANO architecture. The main components are:

- NFV Orchestrator: acts as coordinator where all VNFs are connected into the required structure to offer network services. It coordinates the resources and is responsible for authenticating and authorisation of network requests.
- VNF (Virtual Network Functions): a functional block with defined interfaces and functional behaviour.
- VNF Manager: coordinates the VNF instances, configures them and is responsible for event handling.
- NFVI (Network Function Virtualization Infrastructure): the generic server infrastructure on which the VNF are deployed.
- VIM (Virtualized Infrastructure Manager): Manages the virtualized NFV infrastructure and allocates virtual to physical resources.

This standard improves compatibility between vendors which means more freedom of choice and flexibility. As seen in the architecture model in Figure 8.1, the standard does not include specifications about the design of VNF but rather specifies how they are connected in the NFV framework.

8.3.2 Challenges of NFV

A big challenge for NFV is to provide improved orchestration and management over traditional, physical network function devices. It needs to be easy to manage and ensure smooth operations. The critical challenge in this area is to provide the maximum flexibility

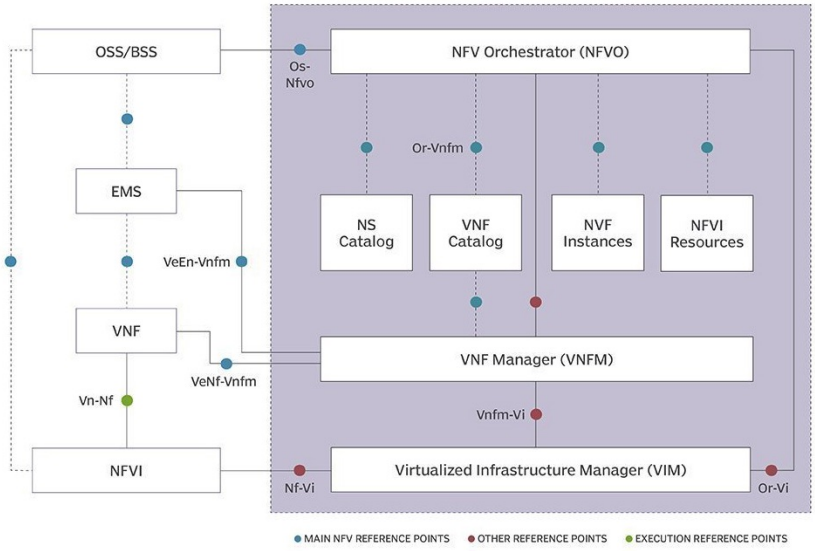


Figure 8.1: ETSI NFV MANO architecture

to improve service quality, customer satisfaction but also to reduce costs. To do this, the system needs to provide dynamic network function chaining. Policy-Based network management would significantly improve this and would allow dynamic reconfiguration of the service graph [13].
As discussed in section 8.3.1, interoperability and compatibility is a crucial challenge hindering the adoption of NFV. To introduce the technology step-by-step, network providers want compatibility with legacy systems. To not be dependent on single vendors, they also require interoperability between different vendor's solutions. In addition to that, they desire interoperability with future solutions and network services, such that the system will not be outdated soon [10].
Networks are dependent on network services. In case of hiccups or downtime of these services, the network will not operate as intended or stop working entirely. To mitigate this from happening, NFV systems need to be resilient to failure and offer high performance. If the network sees a higher load on specific components, it should automatically increase those capabilities to balance the load and ensure smooth operations [10].
In [14], the authors identify practical methods to increase an NVF system's security. They propose to establish trust at three critical steps in the lifecycle of VNF images: First, they tackle the boot of NFVI (NFV Infrastructure). Here, they use trusted platform modules as a hardware root of trust. This microchip can be used to store hash measurements of the components needed in booting a machine (See Figure 8.2), such as BIOS, boot loader, operating system (OS) and hypervisor. In each case, the components measure the following component to establish a chain of trust.

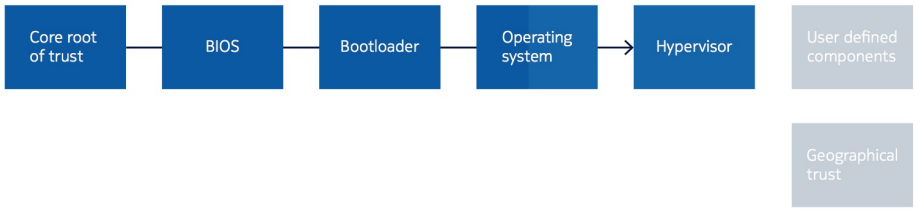


Figure 8.2: Trust chain during trusted boot

After the trusted boot, VNF images are booted. However, to ensure the integrity of the images, service providers may opt to verify them at runtime with an attestation server.

This is done by signing all images by a signing authority, preferably a trusted third-party. Before launching, these can then be checked for authenticity.
In many cases, NFV services require a special level of attention not to violate Service Level Agreements (SLA) and data privacy laws. To ensure the integrity and compliance of a system, an attestation server can be used to monitor the system. If queried, the server will measure the configuration of the NVFI and the VNF images and provide the verifier with a report if all systems operate as required (see Figure 8.3).

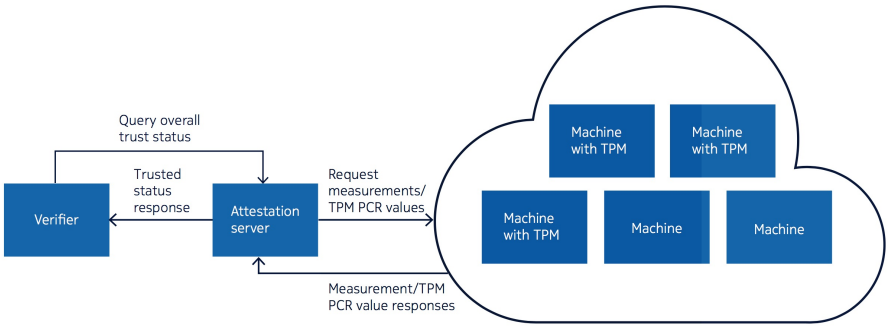


Figure 8.3: Trust status verification query

In conclusion, five areas can be identified as challenging for NFV systems. For an overview, refer to Table 8.1.

Challenge	Description
Orchestration & Management	Reliable, easy and flexible orchestration of VNF services
Compatibility	Compatibility with legacy and future systems as well as competitors' systems
Assurances	System resilience and performance
Security	Secure delivery of network functions and system integrity
Monitoring & Auditing	Monitoring of system state and auditability of changes and compliance

Table 8.1: Table of NFV challenges

8.3.3 Blockchain

Even though blockchain technology has been around since 2009 when Bitcoin was launched [7], it has not seen much adoption apart from cryptocurrencies yet. The main reason for this lack of adoption is the novelty of the concept. It is somewhat unstudied and unproven, thus seen as unsafe. So far, researchers focused mainly on the Bitcoin blockchain rather than the general blockchain technology. It is clear that to improve public blockchain's throughput, latency, performance, efficiency and other aspects, more research is needed.

Looking at private blockchain, most advantages versus traditional databases are lost. However, as there can be a controller which acts as an administrator, many problems associated with public blockchains can be circumvented. This is dependent on the design of the system. For example, Energy-consuming consensus mechanisms, such as Proof of Work (PoW), can be switched for simpler mechanisms. This could be a consortium signing the blocks together. Also, the centralized control and governance make it easier to scale.
Two of the most important blockchain frameworks are Ethereum [5] and Hyperledger [6]. The main innovation of Ethereum is the Ethereum Virtual Machine, which is run decentralized by participants of the network with the help of a public blockchain. Using this virtual machine, developers can build decentralized apps (Dapps) [5].
Hyperledger is a framework to build and deploy permissions (private) blockchain networks. The Linux Foundation backed open-source project to bring mainstream commercial adoption to blockchain technology. Its modular approach allows users to develop and deploy a blockchain based system according to their specifications. With the support of IT companies like Intel and IBM, this framework is seeing major development [6].
Even though the two frameworks both offer the ability to develop applications running on blockchain technology, their approach is very different. For a comparison of the most essential characteristics, refer to table 8.2.

Characteristic	Ethereum	Hyperledger Fabric
Description of platform	– Generic blockchain platform	– Modular blockchain platform
Governance	– Ethereum developers	– Linux Foundation
Mode of operation	– Permissionless, public or private[4]	– Permissioned, private
Consensus	– Mining based on proof-of-work (PoW) – Ledger level	– Broad understanding of consensus that allows multiple approaches – Transaction level
Smart contracts	– Smart contract code (e.g., Solidity)	– Smart contract code (e.g., Go, Java)
Currency	– Ether – Tokens via smart contract	– None – Currency and tokens via chaincode

Table 8.2: Characteristics of Ethereum and Hyperledger [8]

8.3.4 Challenges of Blockchain

Because blockchain has only been used for a short period, the research community did not yet fully research its potential and challenges. However, an increasing number of papers is being published on the topic, and a lot of new challenges and solutions are being identified. In their research paper, Yli-Huumo, J. et al. [3] summarize these challenges and present them in a figure (See Figure 8.4).

8.4 Use Cases

To find possible use cases of blockchain technology in the NFV environment it is needed to look at the commonalities of NFV challenges (See Table 8.1) and blockchain advantages. Considering these two concepts, the following areas can be identified:

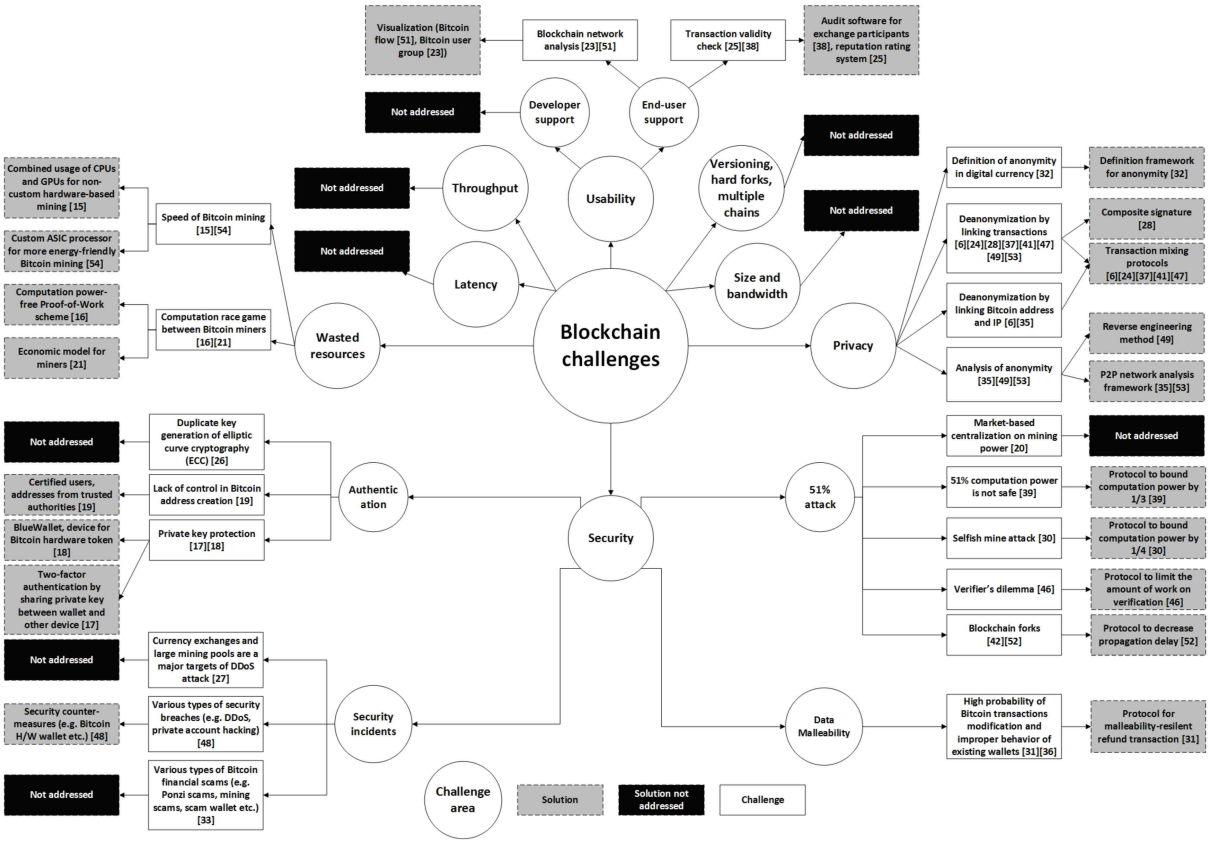


Figure 8.4: Blockchain challenges

- Management and Orchestration
- Security
- Monitoring and Auditing

Adopting a blockchain-based configuration and management for NFV systems offers advantages over traditional centralized approaches. First, blockchain's immutability also enables traceability, as past configurations can be easily accessed. Also, changes to the configuration can be handled securely and encrypted. The encryption of the blockchain helps in two regards: First, only authenticated participants can change configurations. Secondly, the sensitive configuration can be encrypted using public and private keys. This eliminates the need for safe storage of a service provider's tenant configurations. They can be stored anywhere, including a public blockchain. Doing so eliminates a single point of failure and provides high availability of the configuration data. Changes to the configuration can only be made by authenticated and authorized participants through transactions on the blockchain. This means that all changes will be immutably stored on the blockchain including the author of the transaction [12].
Addressed in the paper of Ravidas, S. et al. [4], trust issues in an NFV environment constitute a significant challenge. The authors propose an attestation server and an externally trusted security orchestrator (TSecO) and discuss how such a monitoring system improves security. In [14], the authors propose a system based on conventional client-server-model to establish a trusted computing environment. This could also be achieved by using blockchain technology in multiple ways. For example, instead of having a TSecO database, a distributed ledger could be used. In such a blockchain-based verification system, the components could periodically be attested by distributed app or a trusted server to be compliant to the state in the blockchain.
In the two areas not listed above, assurances and compatibility, no blockchain use case could be identified. However, both areas may benefit from other uses such as the one

described in the paragraphs above: High availability of the configurations in a blockchain-based storage system may increase the availability of the whole system. However, this effect is most likely minimal, as the VNF do not need access to their configurations at all times, but only sporadically. Compatibility issues can most effectively be solved by standardization. Here, introducing a new concept may have the undesired effect of further fragment the solutions. However, if standardized configurations are used in a standardized blockchain, it could also improve compatibility between all supporting solutions. It could also allow different vendors' solutions to access the same configurations.
In addition to the areas mentioned in the subsection 8.3.2, two other minor areas where blockchain and smart contracts can improve the experience are:

- Service Billing and Payment
- Stimulation of competition

Blockchain technology could also be applied in the billing process. By using smart contracts instead of traditional invoicing, service providers would have the assurance that payments are performed on time. Customers, on the other hand, gain the security that service level agreements could be included in the pricing schemes. Thus, if a service provider breaks the SLA, payments could be paused or reduced automatically.
So far, network functions have mostly been supplied by a few vendors. Thus, the customer is bound to the prices of these vendors. Also, with physical equipment and vendor-specific configurations ensuring a lock-in of customers, there is no flexibility. A standardized VNF system based on a common blockchain could change that and let customers benefit from more competition. In the future, smart contracts may enable even more competition by offering real-time auction possibilities: A customer in need of NFV services could post an inquiry on the blockchain, which is then answered by NFV providers' offers. The customer can then chose the cheapest offer which fulfills his demands. As this process can be done very quickly, short-term agreements could see more widespread adoption and help to increase price transparency and competition.

8.5 Example

In [11], the authors present a blockchain-based Management and Orchestration solution which they have implemented and released as open source. SINFONIA stands for Secure vIrtual Network Function Orchestrator for Non-repudiation, Integrity, and Auditability. For their architecture model, refer to Figure 8.5. The system is designed for datacenters with multiple, differing tenant configurations.
In their system, a blockchain is used to store configurations and configuration changes. This allows the system to be monitored, audited and configured more easily and safely. The main components are:

- Display module: The display module is the interface between the tenants that are configuring the system and the blockchain and orchestration module. It is responsible for providing a graphical user interface, where changes can be made, and monitoring can be done.
- Orchestration module: The orchestration module handles the communication with the Open Platform NFV Cloud. It provides the NFV system with the configurations stored in the blockchain module and monitors the state of the VNF.
- Blockchain module: The blockchain module is responsible for mediating and logging the changes and the access of the system.

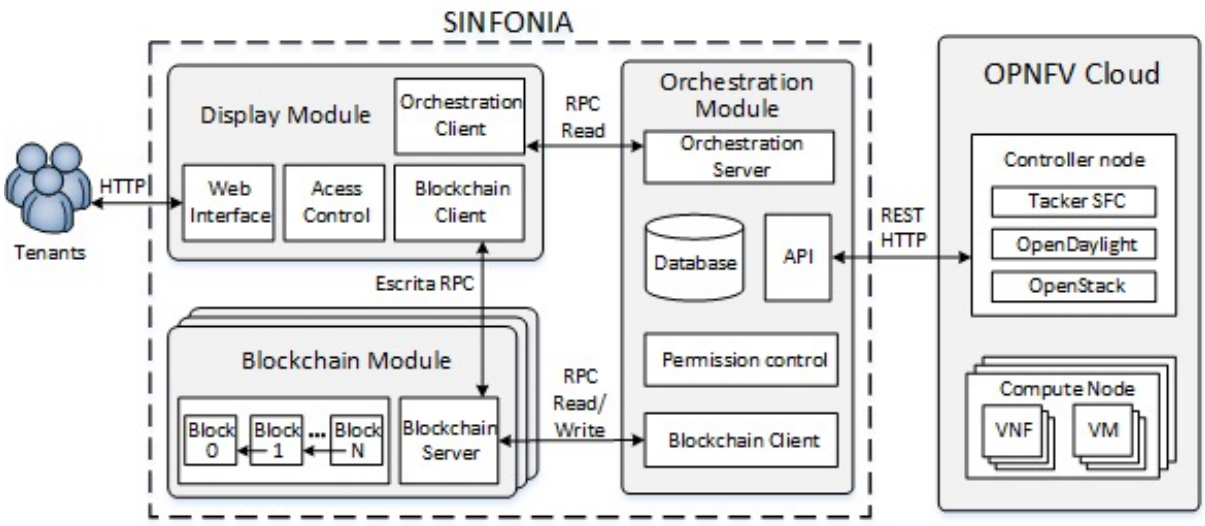


Figure 8.5: Modular architecture of SINFONIA

As this system does not replace the Open Platform NFV cloud, it is not yet the perfect solution. For example, as the orchestration module still has to be hosted in a centralized way, the NFV system cannot benefit from the high availability of the blockchain. Also, as the blockchain is SINFONIA-specific and thus self-hosted and private, significant benefits of public blockchains are lost.

8.6 Discussion and Conclusion

Blockchain technology offers unique advantages over traditional ways of data storage. As seen, these can be used to tackle some of the challenges faced by NFV services today. Especially the area of Management and Orchestration, which is seen as a significant challenge, benefits from the high availability and integrity of a blockchain-based system and is already the primary focus of early prototype development [11] [12]. However, these implementations are not yet perfect and still require more development. Changing privacy laws (GDPR in the EU) may mean that SLAs will get more complicated and more important to adhere to, as the fines are increasing. To be able to prove their compliance, forensic logging made possible by blockchain-based logging may offer a severe advantage to audits. A significant area which hinders the adoption of NFV is the compatibility issues. Here, standardization is a crucial aspect. ETSI is pushing for strict compatibility through their architecture, which will be an advantage going forward. In this area, blockchain will not offer advantages. By introducing a new part that can break compatibility, it may even complicate it more.
The type of blockchain that such systems should use is dependent on the application. The volatile performance and security implications of public blockchains could result in a problem for commercial, widespread adoption. A private blockchain, on the other hand, cannot provide all advantages, leaving the question if adoption is worth the investment. There may be a need for a hybrid system, such as a consortium blockchain or a private blockchain which regularly is backed up or timestamped onto a public blockchain. However, more research in this direction is needed to definitively answer the question of to what extent blockchains and smart contracts can be applied in NFV.

Bibliography

[1] Mijumbi, R., Serrat, J., Gorricho, J. L., Bouten, N., De Turck, F., & Boutaba, R.: *Network function virtualization: State-of-the-art and research challenges*, IEEE Communications Surveys & Tutorials, 18(1), 236-262, 2016.

[2] Clack, C. D., Vikram A. B., and Lee, B.. *Smart Contract Templates: foundations, design landscape and research directions.* 2016. `https://arxiv.org/abs/1608.00771`.

[3] Yli-Huumo, J., et al. *Where is current research on blockchain technology: a systematic review.* PloS one 11.10, e0163477, 2016.

[4] Ravidas S., Lal, S., Oliver, I., Hippelainen, L. *Incorporating Trust in NFV: Addressing the challenges.* Innovations in Clouds, Internet and Networks (ICIN), 20th Conference on, 2017.

[5] Ethereum Foundation. *A Next-Generation Smart Contract and Decentralized Application Platform.* Ethereum Wiki, abgerufen 2018. `https://github.com/ethereum/wiki/wiki/White-Paper`

[6] The Linux Foundation. *Hyperledger Architecture, Volume 1.* Hyperledger, abgerufen 2018. `https://www.hyperledger.org/wp-content/uploads/2017/08/Hyperledger_Arch_WG_Paper_1_Consensus.pdf`

[7] Nakamoto, S. *Bitcoin: A Peer-to-Peer Electronic Cash System.* www.bitcoin.org, 2007. `https://bitcoin.org/bitcoin.pdf`

[8] Sander, P. *Comparison of Ethereum, Hyperledger Fabric and Corda.* Medium.org, 2017. `https://medium.com/@philippsandner/comparison-of-ethereum-hyperledger-fabric-and-corda-21c1bb9442f6`

[9] Nolle, T., *Adding Another Dimension to SDN and NFV Security*, CIMI Corporation's blog, 2015. `http://blog.cimicorp.com/?p=2291`, accessed 8 March 2018.

[10] European Telecommunications Standards Institute, *ETSI GS NFV 004 V1.1.1*, 2013. `http://www.etsi.org/deliver/etsi_gs/NFV/001_099/004/01.01.01_60/gs_NFV004v010101p.pdf`.

[11] Rebello, G. A. F., Alvarenga, I. D. & Sanz, I. J.: *SINFONIA: uma Ferramenta para o Encadeamento Seguro de Funï¿½ï¿½es Virtualizadas de Rede Atravï¿½s de Corrente de Blocos.*, Technical Report, PEE/COPPE/UFRJ, 2017.

[12] Alvarenga, I. D., Rebello, G. A. F., and Duarte, O. C. M. B. *Securing Configuration Management and Migration of Virtual Network Functions Using Blockchain.* to be published in IEEE/IFIP Network Operations and Management Symposium - NOMS 2018, 2018.

[13] Scheid, E. J., Machado, C. C., dos Santos, R. L., Schaeffer-Filho, A. E., & Granville, L. Z.: *Policy-based dynamic service chaining in Network Functions Virtualization*, IEEE Symposium on Computers and Communication (ISCC), 2016.

[14] Nokia: *Trusted NFV Systems*, NFV Insight Series, 2017.