Universiteit Leiden

ICT in Business and the Public Sector

Blockchain technology for a better secured IIoT network

"The whole is greater than the sum of its parts."
Aristotle, philosopher 384-322 BC

Name: Denny M. Koemans
Student-no: 1853961

Date: 11/12/2018

Supervisors: Dr. M.T.M. Emmerich and Prof.dr. S. Jong Kon Chin

MASTER'S THESIS

Leiden Institute of Advanced Computer Science (LIACS)

Acknowledgement

The success and final outcome of this research required a lot of feedback and encouragement and I am extremely privileged to have received this all along the completion of my project.

Foremost, I would like to thank my company supervisor, prof.dr. Ben van Lier, Director Strategy & Innovation at Centric and expert in a.o. the Internet of Things, for providing me the opportunity to do this research. He believes in the relevancy of the subject and supported me from day one. I'm very thankful for his time and patience and for always being available for discussions. Without his feedback, suggestions and encouragement, this research wouldn't be what it is right now.

Also I would like to thank my supervisors from the university, dr. Michael Emmerich and prof.dr. Simcha Jong Kon Chin, for their valuable feedback, that brought this report to a higher level.

Many thanks to all experts who were willing to invest their precious time and participate in this research by sharing their thoughts and opinions about the proposal. I can't describe how much I've learned from the different insights given by (in alphabetical order) dr. ir. Mortaza Shoae Bargh, Daniel Burkhardt, dr. ir. Sunil Choenni, prof. dr. Sandro Etalle, Mark Hennessy, Tommy Koens, dr. Eric Pauwels, dr. Zhijie Ren and Alex de Vries. Their background and expertise is included in chapter 4.2.

Finally, my gratitude is for all my friends and family who continuously encouraged me to continue with this research project.

Abstract

Since the invention of the internet, people increasingly connect machines to it, to create a structure much more powerful than the sum of its individual parts. These interconnectedness is becoming a standard and machines are designed to connect and communicate. The essential component to make this possible is the software that's embedded into the physical objects.

The (perceived) benefits of this interconnection between machines is endless, but security knowledge and standards seem lacking behind. Research is already being done to give authority to machines and devices to collectively reach consensus and security without human intervention, also called device democracy.

Cyberattacks intending to steal data are a well-known problem in cybersecurity. This affected mostly countries and large companies whose client details or secrets were stolen. Although this occasionally resulted in damage of some sort, this was generally quickly resolved. But in the course of time core businesses like a nuclear power plant, a steel plant and a water supply system were hacked as well, causing physical and financial damage and making it a threat to everyone. In the past years most attacks focused on outages of websites and servers using DDOS attacks. The new element in 2016 was that also small "dumb" devices like security cameras were used to organize large scale attacks, instead of just PC's and laptops connected to the internet.

The latest malware not only does specific damage. Data is stolen and is lost forever. It's used as a general weapon to cause disruptive damage all over the world at the same time. Nowadays malware is developed to target the security systems of critical infrastructures. This eventually led to a new state of awareness about the risks faced in recent cybersecurity as an international problem.

That raised the question how a network of machines can be defended, or even better, can defend itself. It's impossible for humans to fully defend their infrastructures. Analyzing a network of connected operating machines is an enormous task that people can't do as fast as machines. Especially since the rise of big industrial networks, current defense techniques simply won't comply. It's necessary to look for possibilities to include machine learning to protect these networks. The rise of the blockchain technology might be a solution since it's a structure of machines which can operate autonomously and is therefore secured by its essential aspect that no human can interfere with the process. If machines themselves can learn from attacks, then that will increase their defenses enormously.

This research considers blockchain technology as a concept of chronological ordering of events saved in multiple databases in different locations in which new input is handled with a consensus protocol to guarantee consistency. The Paxos algorithm can be used for distributed systems where consistency is needed between databases on different physical locations. Reaching consensus about new data between the elements in the network is an essential part. This protocol however doesn't include verification of the proposed new

values, it assumes nodes to be honest and thus proposals should be correct. If honesty among the nodes can be guaranteed, the protocol can guarantee consistency.

In the context of this research a proposal has been described that can be the basis of a protocol to better secure an Industrial Internet of Things network (industrial or critical infrastructure) where new values can't always be verified. If the requirements below can be guaranteed, then a higher level of security may be reached. These requirements are:

* The nodes in the network can be identified

* The nodes in the network can be trusted before joining or performing any actions

* The network (all connected nodes) is able to verify the state of its individual nodes

Essentially the network is secured as long as malicious nodes can't join and the nodes in the network can be verified to be and stay honest. When the nodes in the network can verify that each other's software is not compromised, then one can state that the network is secured. It can eventually be based on a set of rules, but preferably it should also be supported by machine learning algorithms. Every machine would still be secured by its personal security measures, just like in the current situation. Once the machine is connected to the network, it would automatically get verified by the network, so this proposal adds an extra layer of security. Whenever someone tries to tamper with the software on a certain machine, it should get noticed by the network and the machine won't be allowed in the network until it's fixed.

Experts on IIoT, blockchain, cybersecurity and machine learning agree that the idea is promising. That it may well work and is worth to be studied further.

Contents

List of abbreviations

ADEPT	Autonomous Decentralized Peer-to-Peer Telemetry
ANN	Artificial Neural Networks
AR	Augmented Reality
ARPA	Advanced Research Project Agency
BGP	Byzantine Generals Problem
BoT	Blockchain of Things
BSI	Bundesamt für Sicherheit in der Informationstechnik
CPS	Cyber Physical Systems
CPS PWG	Cyber Physical Systems Public Working Group
CPU	Central Processing Unit
CTI	Cyber Threat Intelligence
DDB	Distributed Database (DDB)
DDOS	Distributed Denial of Service
DHS	Department of Homeland Security
ICS	Industrial Control Systems
IIC	Industrial Internet Consortium
IIoT	Industrial Internet of Things
IoE	Internet of Everything
IoT	Internet of Things
ITU	International Telecommunication Union
LBS	Location-Based Services
LOC	Lab-on-a-Chip
M2H	Machine-to-Human
M2M	Machine-to-Machine
NCCIC	National Cybersecurity and Communications Integration Center
PBFT	Practical Byzantine Fault Tolerance
PLC	Programmable Logic Controllers

PoC	Proof of Concept
RFID	Radio Frequency Identification
SIFT	Software Implemented Fault Tolerance
SoS	System of Systems
TIP	Threat Intelligence Platform
TTP	Trusted Third Party
VSR	View Stamped Replication
WEF	World Economic Forum

1. Introduction

Anno 2018 people live in an increasingly digitally connected world. What was unimaginable a few years ago, is reality today. New developments will change the way people communicate, work and live. Things like autonomous cars and refrigerators that supply themselves, seem to be realistic in just a few years from now. It's clear that there's a focus on connecting everything to the internet and to each other, in order to create new opportunities.

With this new innovations, cybersecurity has become a serious issue for every country, company and even individual. In recent years a clear and worrying trend can be seen, with an alarming amount of cyber-attacks. Nowadays also the number of cyber-attacks that do physical and financial damage towards civilian infrastructures and economies are increasing and their impact is getting bigger. This clearly needs to be faced and prevented before one can fully grasp the potential of technology innovations.

"Any network or connected devices, from military systems to civilian infrastructure such as energy sources, electricity grids, health or traffic controllers, or water supplies, can be hacked and attacked." (Schwab, 2016)

In the past, threats were mainly coming from cyber criminals (individual or organized) that would try to make money out of them. In recent years it became clear that also nation states are active in this field, what brings humanity closer to cyber warfare. It's very important that research towards the security of those networks in our economies and critical infrastructures is intensified.

The main objective of this research is to study the Industrial Internet of Things environments in general, from a security point of view. Are these networks sufficiently protected and if not, is there possibly a way to better secure them?

Report structure

The next chapter includes the results of a detailed literature study on the different areas concerned: Internet of Things, cybersecurity, blockchain technology and machine learning.

In the third chapter one can find the research methods used. Starting with the identified research gap or problem derived from the literature study, followed by research questions and the methods to find the answers.

In the fourth chapter a proposal can be found as well as the opinions about it, according to several experts in the relevant fields.

The conclusions and recommendations for further research are documented in chapter five.

2. Literature review

2.1. Internet of Things

2.1.1. The concept in general

Since the invention of the internet, in an increasing speed, devices of all kinds get connected to the internet. According to estimates from Cisco (2018) there will be 27.1 billion network devices in 2021. These devices get connected with humans but more and more also to each other. This trend is generally referred to as the 'Internet of Things' (IoT).

Probably the first article about such a connected world is published by Weiser (1991). He writes about 'Ubiquitous Computing' and describes the idea that the full potential of computing is making everyday life easier:

"*In our experimental embodied virtuality, doors open only to the right badge wearer, rooms greet people by name, telephone calls can be automatically forwarded to wherever the recipient may be, receptionists actually know where people are, computer terminals retrieve the preferences of whoever is sitting at them, and appointment diaries write themselves. No revolution in artificial intelligence is needed--just the proper imbedding of computers into the everyday world*" "*Depending upon the room you may see more than a hundred tabs, ten or twenty pads, and one or two boards. This leads to our goals for initially deploying the hardware of embodied virtuality: hundreds of computers per room*. " (Weiser, 1991)

This was basically the start of a new way of thinking about computers. Rather than just doing what the owner tells the computer to do, this suggests that computers should be able to do much more than that. It doesn't say much about connected computers, just computers imbedded in "normal" things. The term IoT was first used in 1999 by Ashton (2009), but originates from the innovation of connected devices that started in 1980 as stated by Madakam, Ramaswamy & Tripathi (2015). The term was defined more precise in an RFID journal 10 years later:

"*If we had computers that knew everything there was to know about things—using data they gathered without any help from us -- we would be able to track and count everything, and greatly reduce waste, loss and cost. We would know when things needed replacing, repairing or recalling, and whether they were fresh or past their best. We need to empower computers with their own means of gathering information, so they can see, hear and smell the world for themselves, in all its random glory. RFID and sensor technology enable computers to observe, identify and understand the world—without the limitations of human-entered data."*
(Ashton, 2009)

Almost 15 years after Ashton coined the term, the economic benefits from connected (IoT) devices that make decisions are growing, as can be seen in the following examples:

- Barcelona's energy-saving smart streetlights: sensors are installed in streetlights, enabling automatic control of brightness by analyzing the levels of noise, air pollution, and population density. Result: at least 30% energy savings per year (Ajuntament de Barcelona, 2014);
- UK's Intelligent Transport System that reduces traffic congestion: UK built a responsive transport system on the M42 motorway and reduced travel time by 25% and traffic accidents by 50% (Roadtraffic-technology, 2015);
- The research conducted by the Virginia Tech Transportation Institute (2016) concluded that the national crash rate of 4.2 accidents per million miles is higher than the crash rate for self-driving cars, which is 3.2 crashes per million miles.

Cisco defined the term IoT as follows:

"*The IoT is a more encompassing phenomenon, which includes Machine-to-Human communication (M2H), Radio Frequency Identification (RFID), Location-Based Services (LBS), Lab-on-a-Chip (LOC) sensors, Augmented Reality (AR), robotics and vehicle telematics. Many of these technologies are the result of developments in military and industrial supply chain applications; their common feature is to combine embedded sensory objects with communication intelligence, running data over a mix of wired and wireless networks.*" (Frahim, Pignataro, Apcar & Morrow, 2015)

The European Commission acknowledged that this development had a lot of potential and that it's important to stimulate this trend to gain the benefits:

"*The Internet of Things (IoT) represents the next major economic and societal innovation wave enabled by the Internet. With the IoT, any physical (e.g. a thermostat or a bike helmet) and virtual (i.e. a representation of real object in a computer system) object can be connected to other objects and to the Internet, creating a fabric between things as well as between humans and things. The IoT can combine the physical and the virtual worlds into a new smart environment, which senses, analyses and adapts, and which can make our lives easier, safer, more efficient and more user-friendly.*" (European Commission, 2016)

These developments have the side effect that machines are created to be "open" and "willing to communicate" and not as much to be secured. The authority to make important decisions is more often placed in the hands of computers. The EU points out that to enable this development and before all the benefits can be fully grasped, there's a need for a single IoT ecosystem that anyone can enter with high standards for the protection of personal data and security. The innovation progress made by humanity as a whole is an unstoppable trend with incredible speed. The capabilities to secure this new digital environment as well as our physical environment is becoming increasingly important:

"*IoT technology will be in 95% of new electronic product designs. While this statistic demonstrates the success of IoT, it is also a precursor for alarm. As the adoption of IoT*

*devices rises, manufacturers are competing to stay ahead. Creating cheap products quickly often means overlooking security and privacy measures." (*Jackson, 2017)

This priority to create a secured environment is also addressed by Shneyder (2018):

"*IoT, as a burgeoning technology subsector, needs to put security at the forefront of the march toward more innovative device manufacturing. There's no question that IoT is enriching our lives. We can all agree that from the mobile phone, to watches, to fitness trackers, we're all a little smarter because of it—however, security protocols and policies need to keep pace*." (Shneyder, 2018)

Pureswaran & Brody (2015) stated that IoT needs to become decentralized meaning that the devices or systems themselves need to be able to make decisions, the so called device democracy. It was also the start of Hyper Ledger Fabric, a coalition between Samsung and IBM to do research in enabling Samsung products to communicate autonomously.

"*In a network of the scale of the IoT, trust can be very hard to engineer and expensive, if not impossible, to guarantee. For widespread adoption of the ever-expanding IoT, however, privacy and anonymity must be integrated into its design by giving users control of their own privacy.*" (Pureswaran & Brody, 2015)

2.1.2. Industrial Internet of Things

Industrial Internet is based on closed structures within an industrial process. In general it was imaginable that these processes could be optimized and automated with embedded sensors. Evans & Annunziata (2012) described the potential benefits of a connected environment between different industries. Sensors can be put in any machine or even different parts of a machine to reach full optimization and efficiency (also less waste). The authors both worked for General Electric where they noticed that the future of their products would be a digital connection of all their product imbedded sensors. A definition for Industrial Internet is not supplied, it's rather the economic advances of the industrial revolution and the internet revolution combined.

"*The Industrial Internet brings together the advances of two transformative revolutions: the myriad machines, facilities, fleets and networks that arose from the Industrial Revolution, and the more recent powerful advances in computing, information and communication systems brought to the fore by the Internet Revolution.*" (Evans & Annunziata, 2012)

"*The full potential of internet-based digital technology has yet to be fully realized across the global industry system. Intelligent decisioning represent the primary ways in which the physical world of machines, facilities and networks can more deeply merge with the connectivity, big data and analytics of the digital world." "We estimate that the technical innovations of the industrial internet could find direct application in sectors accounting for more than $32.3 trillion in economic activity."* (Evans & Annunziata, 2012)

The Industrial Internet Consortium (IIC) was founded to combine knowledge about Industrial Internet:

"*A global not-for-profit partnership of industry, government and academia. The Industrial Internet Consortium was founded in March 2014 to bring together the organizations and technologies necessary to accelerate the growth of the Industrial Internet by identifying, assembling and promoting best practices.*" (Industrial Internet Consortium (IIC), 2018)

It's not easy to offer a clear definition of IIoT. This makes sense because it's still hard to fully understand the possibilities and scale. Even the IIC rather describes this phenomenon than give a definition:

"*WHAT IS THE INDUSTRIAL INTERNET? Imagine a highway where cars are able to safely navigate to their destinations without a driver. Imagine a home where an elderly patient's health is closely monitored by her hospital physician. Imagine a city that significantly reduces waste through sensor-embedded water pipes, buildings, parking meters and more.* " (IIC, 2018)

The following definition given by the company TechTarget describes what IIoT is. In general it's the combination of recent developments in smart machines connected to each other to optimize industrial processes.

"*The industrial internet of things, or IIoT, is the use of internet of things technologies to enhance manufacturing and industrial processes. Also known as the industrial internet or Industry 4.0, IIoT incorporates machine learning and big data technologies to harness the sensor data, machine-to-machine (M2M) communication and automation technologies that have existed in industrial settings for years.*" (Rouse, 2018)

The next step in this evolution was something called Cyber Physical Systems (CPS). Basically, in this stage machines are assumed to be created to become connected to many different things, not just one industrial system or process. This means that the development and production of the products need to be different. CPS was defined as follows:

"*Cyber-physical systems (CPS) are smart systems that include engineered interacting networks of physical and computational components*. *This document defines a CPS as follows: Cyber-physical systems integrate computation, communication, sensing, and actuation with physical systems to fulfill time-sensitive functions with varying degrees of interaction with the environment, including human interaction. CPS go beyond conventional product, system, and application design traditionally conducted in the absence of significant or pervasive interconnectedness.*" (Cyber Physical Systems Public Working Group, 2016)

So rather than being an isolated machine, these physical machines are created to be interconnected. These new machines (or so called CPS) have to be able to communicate with an undefined set of other CPS. In addition the CPS PWG adds that systems need to be designed to communicate in Systems or even Systems of Systems to contribute to the set of

common tasks and knowledge. CPS need a methodology to ensure interoperability, managing evolution, and dealing with emergent effects. One of the important aspects of these new way of thinking is that the physical objects per definition get software in them to communicate and perform other activities. This makes the machines more unsecure because the software can be hacked and attacked, not the physical object.

"*A CPS may be as simple as an individual device, or a CPS can consist of one or more cyber-physical devices that form a system or can be a SoS (System of Systems), consisting of multiple systems that consist of multiple devices. CPS are increasingly connected horizontally with each other and vertically with the broader systems. The horizontal connectivity paves the way for CPS to collaborate directly. The vertical connectivity brings about the possibility of realizing a global view of the states of the vast network of the CPS and the opportunity to coordinate or orchestrate their operations to achieve optimization at a global level*" (CPS PWG, 2016)

In 2012, Evans started to describe an even more connected level which he called the "Internet of Everything". In such an IoE environment basically everything one can touch, smell and feel would be connected. It would appear as normal to human beings as walking through the woods. For example:

"*Sensors placed on the skin or skew into clothing will provide information about a person's vital signs. People themselves will become nodes on the internet, with both static information and a constantly emitting activity system.*" (Evans, 2012)

What's also interesting about his article is the claim that

"*A simple network effect is generated when participants (or nodes) within a network are connected in a manner makes "The whole greater than the sum of its parts".* " (Evans, 2012)

This predicts unimaginable opportunities in connecting machines to each other. Connected machines will be stronger than single computers individually. The machine to machine communication is an important aspect of this view.

For this research IIoT was considered to be a full industrial process which can largely operate autonomously in a restricted environment. So this means that it does include different companies who don't necessarily want to share all their information, but do want to optimize the process for the benefit of all. It's restricted in the way that anyone who wants to connect to this system can be identified. A well-known example could be the harbor of Rotterdam where a lot of different companies need to connect, share information and work together and many autonomous machines work together as well.

A lot of calculations and explanations are given about the benefits of this connected Industrial Internet. Although little has been written about the risk and safety issues that come with the potential benefits, some enablers and possibilities that might help to keep it

safe were described. It's also indicated that humans are most likely not capable of defending this system themselves.

"*A robust cyber security system and approaches to manage vulnerabilities and protect sensitive information and intellectual property is needed to enable Industrial Internet." "Complexity has outstripped the ability of human operators to identify and reduce these inefficiencies.* " (Evans & Annunziata, 2012)

2.2. Cybersecurity

2.2.1. Development

Since databases are being used by companies and individuals, they're getting hacked and data has been stolen. This includes personal client details or even country secrets. Many if not all large companies are already hacked in some sort of cyberattack. More recent a trend can be seen that transforms the attacks from stealing towards doing actual damage. The damage varies from downtime with DDOS attacks to physical damage. Currently, the digital environment is facing an increasing cybersecurity threat since the network of connected devices is growing rapidly and attacks can come from virtually anywhere and are increasing in both frequency and impact:

"*Cyber warfare can take many different forms – from criminal acts and espionage to destructive attacks such as Stuxnet- that remain largely underestimated and misunderstood because they are so new and difficult to counter."* "*Defense, military and national security strategist had focused on a limited number of traditionally hostile states, now they must consider a near-infinite and indistinct universe of hackers, terrorists, activists, criminals, and other possible foes."* (Schwab, 2016)

The first and well known example of physical damage is the Stuxnet attack on Iran's uranium enrichment program in 2010. According to a large research investigation report performed by Symantec, this malware was created to make physical industrial systems work slightly different without the victims knowing.

"*Stuxnet is a threat that was primarily written to target an industrial control system or set of similar systems. Industrial control systems are used in gas pipelines and power plants. Its final goal is to reprogram industrial control systems (ICS) by modifying code on programmable logic controllers (PLCs) to make them work in a manner the attacker intended and to hide those changes from the operator of the equipment.*" (Falliere, Murchu & Chien, 2011)

This is a strong example of a secured industrial network that's been attacked by sophisticated hackers. Then in 2014 another hack took place on a German steel plant (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2014). The incident caused physical damage to a steel plant in Germany. The control components and entire production environment suffered outages due to the attackers actions. The outages prevented the plant from appropriately shutting down a blast furnace, leaving it in an undetermined state. This resulted in significant damage to the plant (translated from German):

"*Damaging Effect: Failures of control components were accumulating, even failures of whole plants. The failures lead to the situation, that a blast furnace could not be shut down in a*

regular manner and was in an undefined state. The consequence was a massive damage of the plant.“ (BSI, 2014)

Although the nuclear powerplant and steel mill caused physical damage, not many civilians noticed the damage. This changed in 2016 when the first known civilian infrastructure, a water treatment system in the US, was attacked. In this case the attackers managed to change the amount of chemicals in the water system making it unsafe to drink. This changed the cyber problem from an individual or company problem towards an international security problem.

“*An unexplained pattern of valve and duct movements had occurred over the previous 60 days. These movements consisted of manipulating the PLCs that managed the amount of chemicals used to treat the water to make it safe to drink, as well as affecting the water flow rate, causing disruptions with water distribution.*” (Verizon, 2016)

Also in 2016, the Mirai malware was discovered. This revealed a new kind of attack, to compromise simple IoT devices and use them collectively to generate extreme amounts of internet traffic to overload the targeted system. According to Ars Technica, IP cameras and video recorders are among the most frequently compromised IoT devices from the Mirai network. Although these machines are relatively small, collectively they form a serious threat.

“““*Someone has a botnet with capabilities we haven’t seen before,” McKeay said. “We looked at the traffic coming from the attacking systems, and they weren’t just from one region of the world or from a small subset of networks — they were everywhere.*”” (Krebs, 2016)

It’s important to note that simple IoT devices like cameras and video recorders are used for a large scale attack. They are relatively easy to hack and used to combine these devices in large botnets. These IoT devices generally can’t defend themselves well enough from sophisticated hackers. It’s the software part of the systems that gets hacked and is used to attack other systems. Essentially it doesn’t matter what physical object it’s on. The software is vulnerable due to the ”open” design of these machines, they are not designed to stay closed (secured). This makes sense because the different machines have to be able to work with many different software and protocols etc. The company who produces the physical camera wants to sell the product to different companies who all have their own operating software. These companies and their software are also designed to be compatible with the different operating software from their clients like PC’s and other security alarm systems. The openness of these machines is more important than the foreseen risks.

The longest attack lasted more than 12 days, which could be catastrophic for some companies or civilian infrastructures. Imagine the water cleaning system from the previous example or an electricity grid to be disabled for weeks. These attacks are continually growing in numbers and scale:

"*Q1 2018 saw a significant increase in both the total number of DDoS attacks, and the duration of those attacks, compared to Q4 2017, the report found. This rise is due in large part to a growing number of botnet attacks. The Linux-based botnets Darkai (a Mirai botnet clone) and AESDDoS were largely responsible.*" (Khalimonenko, Kupreev & Badovskaya, 2018)

In June 2017 again a new kind of attack occurred with malware called NotPetya. This software was different in a few ways from previous attacks. First of all this malware caused its victims data to be encrypted and thus unreachable. This is similar to ransomware when the victims need to pay to decrypt their data. The difference is that the data can't be decrypted and is lost forever. Basically this attack intended to do damage instead of making money out of it:

"*Researchers who have analyzed the high-level code of the encryption routine and determined that after disk encryption, the threat actor could not decrypt victims' disks.*" (Kasperskylab, 2017)

This malware uses multiple techniques to spread to other computers automatically. It didn't need any human intervention to target the malware in any direction. The malware itself sought vulnerable targets and decided where it could attack. This threat is getting worse when one's increasingly connecting all sorts of machines, as is happening in Industrial Internet. As a result multiple computers got affected in many different countries. Estimates on the impact of this attack varies but is at least $1 billion:

"*Some examples include shipping giant FedEx, drug maker Merck, software vendor Nuance Communications and food and beverage company Mondelez International. Cybereason first calculated that NotPetya cost companies a total of $592.5 million in quarterly and yearly revenue, but that figure exceeded $1 billion by November 2017.*" (Asher-Dotan, 2017)

This is not surprising since the estimated impact by one of the bigger victims (Maersk) was estimated between $200-300 million loss.

"*In the last week of the quarter we were hit by a cyber-attack, which mainly impacted Maersk Line, APM Terminals and Damco. Business volumes were negatively affected for a couple of weeks in July and as a consequence, our Q3 results will be impacted. We expect the cyber-attack will impact results negatively by USD 200–300m*. " (Maersk, 2017)

A few months later it became worse when a malware named "Triton" (also known as HatMan or Trisis) had been discovered with a much higher risk of physical damage. Instead of a website or system to go offline, this malware was targeting critical infrastructures including safety mechanisms. This caused the safety mechanisms from executing their intended function, resulting in physical consequences. Both Triton and NotPetya attacks are not only used by individuals or companies, but also by nation states. This brings the problem closer to cyberwarfare:

"*Security researchers have uncovered another nasty piece of malware designed specifically to target industrial control systems (ICS) with a potential to cause health and life-threatening accidents." "we assess with moderate confidence that the actor is sponsored by a nation state."* (Johnson, Caban, Krotofil, Scali, Brubaker & Glyer, 2017)

This is why the National Cybersecurity and Communications Integration Center (NCCIC) stated that it has serious potential to do physical damage to persons, property and environment.

"While it is safe to say that HatMan is a valuable tool for ICS reconnaissance, it is likely designed as part of a multi-pronged attack that collectively would degrade industrial processes, or worse. Were both the process and the safety systems to be degraded simultaneously, physical harm could be effected on persons, property, and/or the environment—barring the presence of additional safety mechanisms. " (NCCIC, 2018)

This situation in the connected world raises the question how this can be made more secured. A new way of defense is needed for this new connected environment and this might include a system that can defend itself:

"*Security threats are continuously emerging and require us to develop an architecture that can defend itself against those threats.* " (Frahim et al., 2015)

Cybersecurity is obviously becoming a bigger issue. Companies and institutions around the world of any sector and even the most secured environments are already breached in 2017 alone (Guerra & Tamburello, 2018). And they are the ones that became publicly known. There might be more cases where the victim doesn't know about or wants to keep it a secret.

"*In 2017 alone, cyber criminals breached major credit bureaus, telecom providers, government entities, mobile applications, shipping companies, U.S. voting institutions, and countless individuals. Data stolen from these groups contains personally identifiable information, financial records, and even classified intelligence; each of which attackers can use toward harmful means.* " (Guerra & Tamburello, 2018)

As most information, especially important information, is getting stored online and efficiency to work with it requires to share it among different places, it gets harder to secure it:

"*Today, though, if that information is to be useful in any way, it's stored in a digital form on a computer that is connected to a network. The problem, as we explored earlier, is that many of these networks are not as secure as their users may think. And so while computer networks are allowing groups to work more efficiently and effectively than ever before, they are making it easier to steal secrets. We have entered what one security organization calls the "golden age" of intelligence. As one report notes, "Nations don't need expensive ground stations, satellites, airplanes or ships to spy. Global intelligence capabilities now just need a few laptops and a high-speed connection.*" (Singer & Friedman, 2014)

Machines are developed and created to communicate and become inter-connectable. This makes them very insecure by design.

2.2.2. Cyber kill chain

Cyberattacks can come in many forms for example: viruses, worms, malware, ransomware, DDOS and more. Although there's a large variety in cyberattacks with different scale and impact, each cyberattack has an attacker (either individual or group) with a motive. Whether they are individuals or groups at any scale, these motives can be categorized as follows:

1. Financial gain
2. Political/religious actions
3. Revenge/emotions
4. Entertainment/challenge

To understand the vulnerabilities and threats, breaches have been investigated. Research has shown that cyberattacks have many things in common. This led to Lockheed Martin Corporation identifying a set of stages that any cyberattack has to go through, called the Cyber Kill Chain. It helps to categorize cyberattacks and increase understanding and security. It was stated that any attack needs to go through 7 stages before doing damage.

"*Intruder succeeds if, and only if, they can proceed through steps 1-6 and reach the final stage of the cyber kill chain.*" (Hutchins, Cloppert & Amin, 2011)

The stages from the Cyber Kill Chain are: "

1. **Reconnaissance**: Intruder selects target, researches it, and attempts to identify vulnerabilities in the target network.
2. **Weaponization**: Intruder creates remote access malware weapon, such as a virus or worm, tailored to one or more vulnerabilities.
3. **Delivery**: Intruder transmits weapon to target (e.g., via e-mail attachments, websites or USB drives)
4. **Exploitation**: Malware weapon programs code triggers, which take action on target network to exploit vulnerability.
5. **Installation**: Malware weapon installs access point (e.g., "backdoor") usable by intruder.
6. **Command and Control**: Malware enables intruder to have "hands on the keyboard" persistent access to target network.
7. **Actions on Objective**: Intruder takes action to achieve their goals, such as data exfiltration, data destruction, or encryption for ransom. "

This method gives a structured way to categorize attacks and their stages and prioritizes their responses. It also helps to give a global understanding of our IT defenses. In 2015 they addressed the importance of creating a Threat Intelligence Platform (TIP) to gain further insight into the vulnerabilities of an organization and required responses to attacks. This

kept the structure of the Cyber Kill Chain to organize such defenses. Threat intelligence is basically growing knowledge about historical attacks and thus becoming stronger from each attack.

"*Threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard.*" (Gartner, 2014)

For example the report about the attack on a Ukrainian power grid used the same structure to describe each phase. At each stage of the attack the report indicated what happened and what can be done to defend against these attacks (Lee, Assante & Conway, 2016):

"*Nothing about the attack in Ukraine was inherently specific to Ukrainian infrastructure. The impact of a similar attack may be different in other nations, but the attack methodology, Tactics, Techniques, and Procedures (TTPs) observed are employable in infrastructures around the world. "* (Lee et al., 2016)

Because this platform should become stronger by each event, it would be most effective when knowledge is shared among defenders. Research has shown that companies increasingly value the power of collective defenses.

"*In the last couple of years, organizations have demonstrated an increased willingness to exchange information and knowledge regarding vulnerabilities, threats, incidents and mitigation strategies in order to collectively protect against today's sophisticated cyberattacks.*" (Sauerwein, Sillaber, Mussmann & Breu, 2017)

This led to the development of Threat Intelligence Sharing Platform (TISP) where companies could combine their defenses to cooperatively come to a better defensive structure than would be reached by the individual members apart. Optimizing such a platform towards a real time updating and securing platform is crucial to protect economies and nations against cyber criminals. Today this seems to be the focus of cybersecurity:

"*To mitigate these types of attacks, it's important organizations understand, have access to and can leverage actionable, real-time cyber threat intelligence (CTI) to help bolster their security postures. In the end, visibility and awareness are key." (Connor, 2018)*

This indicates that real time threat detection and sharing among a network of systems will make the network as a whole better secured. The blockchain technology might be useful to create such defense mechanisms. Research also indicated the main issue of sharing cyber security data is trust (Sauerwein et al., 2017):

"*In order to overcome these trust and access control issues, threat intelligence sharing platforms must provide control mechanisms to specify what information is shared, how much of it and with whom. In addition, access control plays an important role to these platform, since these platforms might be of potential interest to attackers*." (Sauerwein et al., 2017)

Blockchain technology could solve trust issues. This indicates that the blockchain technology potentially could be used to create such a Threat Intelligence Sharing Platform to reach a better secured environment. Therefore the next paragraph describes detailed literature study on the blockchain technology.

2.3. Blockchain technology

2.2.1. The blockchain

Many articles were written about blockchain, but no clear definition has been given. Director of the Blockchain Project at Yeshiva University in New York, Aaron Wright, described the blockchain as follows:

"*The blockchain is a distributed, shared, encrypted database that serves as an irreversible and incorruptible public repository of information. It enables, for the first time, unrelated people to reach consensus on the occurrence of a particular transaction or event without the need for a controlling authority.*". (Wright & Filippi, 2015)

The blockchain technology has a lot of potential, maybe one can even say a technology like blockchain is required to enable other innovations, for example IIoT:

"*Blockchain gives us unprecedented capabilities to create and trade value in society. As the foundational platform of the Fourth Industrial Revolution, it enables such innovations as artificial intelligence (AI), machine learning, the internet of things (IoT), robotics and even technology in our bodies, so that more people can participate in the economy, create wealth and improve the state of the world.*" (World Economic Forum (WEF), 2017)

The rise of blockchain technology started with the introduction of the cryptocurrency, the Bitcoin. Nakamoto (2008) proposed a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. He mentioned some characteristics, that look similar to the ones described as requirements for an IoT environment. These characteristics basically mean an environment is required that's robust, machines can leave and rejoin and people can trust computers to communicate with each other and agree on the correctness of events without human intervention (trusting algorithms instead of human knowledge).

"*What is needed is an electronic payment system based on cryptographic proof instead of trust. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes. Nodes can leave and rejoin the network at will, accepting the proof-of-work chain as proof of what happened while they were gone.*" (Nakamoto, 2008)

Nakamoto also mentioned that other rules and structures can be enforced with this system as well:

"*The network is robust in its unstructured simplicity. Nodes work all at once with little coordination. They do not need to be identified, since messages are not routed to any particular place and only need to be delivered on a best effort basis. Nodes can leave and rejoin the network at will, accepting the proof-of-work chain as proof of what happened while they were gone. They vote with their CPU power, expressing their acceptance of valid blocks by working on extending them and rejecting invalid blocks by refusing to work on*

them. Any needed rules and incentives can be enforced with this consensus mechanism." (Nakamoto, 2008)

The technology became known as blockchain technology. It's important to understand what the basis is for blockchain technology. Chaum, Fiat & Naor (1990) stated that:

"*The use of credit cards today is an act of faith on the part of all concerned. Each party is vulnerable to fraud by the others, and the cardholder in particular has no protection against surveillance.*" (Chaum et al., 1990)

This is the first time someone stated that digital transfer of value should become better in terms of efficiency, trust and privacy. Everyone owns their own money and needs to use a bank to transfer it to someone else, but the bank doesn't know where it comes from and where it goes. It just knows that the one who sends it can prove that it's his or hers. The bank in this case is still needed as intermediary to witness the transfer.

Szabo (1994) mentioned smart contracts as a way to automatically execute the contract that's agreed on and doesn't need any authority to check or act to make it happen. This changed the perception of machines and the way one can use them to operate and make decisions:

"*A smart contract is a computerized transaction protocol that executes the terms of a contract. The general objectives of smart contract design are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries. Related economic goals include lowering fraud loss, arbitration and enforcement costs, and other transaction costs*" (Szabo, 1994)

This would minimize the need for trusted intermediaries, but not necessarily eliminate them out of the process. But essentially it's about giving machines the ability and authorization to handle in certain situations. Dai (1998) published an article about B-money, electronic cash that doesn't need a bank or any other trusted party:

"*The protocol proposed in this article allows untraceable pseudonymous entities to cooperate with each other more efficiently, by providing them with a medium of exchange and a method of enforcing contracts.*" (Dai, 1998)

This concept needed a way to reach consensus about where the money is, and a way to make it hard to create money. At that time he used a method to periodically check if the system is still consistent and everyone agrees on the amount of money he or she owns.

"*The creation of money. Anyone can create money by broadcasting the solution to a previously unsolved computational problem. The only conditions are that it must be easy to determine how much computing effort it took to solve the problem and the solution must otherwise have no value, either practical or intellectual.*" (Dai, 1998)

"*Also, each server must periodically publish and commit to its current money creation and money ownership databases. Each participant should verify that his own account balances are correct and that the sum of the account balances is not greater than the total amount of money created*." (Dai, 1998)

This periodical check of correctness comes from the then existing knowledge about distributed databases. Around 1980-1990 people needed their data in more than one place, but it was time consuming to reach the data at a central location. The distributed database is basically a database spread over multiple locations that are connected to act as one database:

"*A distributed database (DDB) is a collection of multiple, logically interrelated databases distributed over a computer network*" (Özsu & Valduriez, 1991.)

To ensure consistency, the databases were either replicated (state machine replication, periodically overwritten by the 'master' database) or periodically checked for inconsistencies. But both options don't guarantee consistency at any given time. Then in 1998 a different innovation came up, the ability to work on a database in different physical locations and still guarantee consistency. This technique was a consensus protocol called Paxos. Although the article was created in 1989, it was officially published in 1998. This consensus protocol described a way to agree on data input and guarantee all databases on different locations would add the same input (if connected).

"*The Paxon Parliament protocol provides a distributed, fault-tolerant implementation of the database system.*" "*A general algorithm ensures that all servers obtain the same sequence of commands, thereby ensuring that they all produce the same sequence of responses and state changes—assuming they all start from the same initial state*." (Lamport, 1998)

One important aspect to keep this type of database structure consistent was that a so called happening before relation could solve the synchronization problem.

"*The concept of "happening before" defines an invariant partial ordering of the events in a distributed multiprocess system. We described an algorithm for extending that partial ordering to a somewhat arbitrary total ordering, and showed how this total ordering can be used to solve a simple synchronization problem.*" (Lamport, 1978)

This concept basically means that one creates a chronological order of events and saves them in a "happened before" relation.

Nakamoto (2008) described the proposed solution of a digital cash system that could work without any trusted party. It guaranteed consistency at any given time. Anyone could transfer money and know it would be transferred safely and no money could be double spend:

"*In this paper, we propose a solution to the double-spending problem using a peer to peer distributed timestamp server to generate computational proof of chronological order of transactions.*" (Nakamoto, 2008)

This system was also actually build in 2009 where the digital cash named Bitcoin could be transferred to anyone else without knowing who he really was and without any trusted party to witness. It combined the earlier mentioned proposals of an online coin (B-money), with the consensus protocol from a shared ledger, saving the data connected with each other via hashes. Blocks were connected in a chain of blocks:

"*To modify a past block, an attacker would have to redo the proof-of-work of the block and all blocks after it and then catch up with and surpass the work of the honest nodes.*" (Nakamoto, 2008)

This is when the bitcoin system became known as blockchain technology, but the technology clearly is a combined set of different technologies invented before. Blockchain technology would better refer to the way of saving the data in the database as a chronological order of events linked to each other. This is also how it's defined in the proposal to the International Telecommunication Union (ITU) for a blockchain of things.

"*Blockchain is usually seen as a peer to peer distributed ledger based on a group of technologies for a new generation of transactional applications, which maintains a continuously growing list of cryptographically secured data records as hardened against tampering and revision.*" (China Unicom, NTRA Egypt, ZTE Corporation, CART MIIT, ISA CETC & Alibaba Group, 2017)

What's interesting about the view of Nakamoto, is that he sees the rise of online communication and trading as a change in interaction between machines. He argues that one makes it too complex with trusted third parties and still doesn't guarantee 100% correctness. Machines together can do this better without people influencing it. One of the most important aspects to achieve this is via consensus over the network. Honest nodes can work together, which is the main defense since it would be very expensive for an attacker to beat this.

"*As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers.*" (Nakamoto, 2008)

Also, the history should be impossible to change:

"*With the possibility of reversal, the need for trust spreads.*" (Nakamoto, 2008)

As shown before, this was already described by Lamport in the Paxos algorithm. Other aspects added for the Bitcoin system like coins, proof-of-work, private and public keys and enforcing the connection between events with hashes, wouldn't necessarily be needed to create a blockchain.

This development resulted in the proposal of a framework for an IoT environment to the ITU by a collaboration of the Chinese Government and large Chinese companies (China Unicom et al., 2017). It was agreed that it might be possible to use blockchain technology to create standards that machines need to have in order to communicate autonomously.

"*Considering the inherent properties of blockchain and IoT, there are many benefits to making blockchain and IoT together, called blockchain of things (BoT), especially for building trust, reducing costs, accelerating transactions, and connecting large scale IoT devices. A BoT can be seen as a decentralized service platform which works on the IoT.* (China Unicom et al., 2017)

The BoT offers new ways for IoT data to automate business processes among partners without setting up a complex and expensive centralized IT infrastructure. Data protection in BoT fosters stronger working relationship with partners and greater efficiency as partners take advantage of the information provided." (China Unicom et al., 2017)

This research focused on the essential parts to create a blockchain and consensus algorithms. A more detailed research to the Paxos algorithm has been conducted because this was one of the first consensus protocols and this protocol is known to be used as consensus algorithm by largescale projects like the google megastores:

"*As it turned out, Paxos was a really important thing, and it was widely reused through the Google codebase. Once I learned about it, I started seeing it everywhere."* (Chu-Carroll, 2015)

2.2.2. The Paxos algorithm

The Paxos algorithm is a protocol to enable a fault-tolerant distributed system that can guarantee consistency at any time (Lamport, 1998). It took almost 10 years to get it officially published, because it wasn't clearly understood by most people. He used a metaphor of a Greek parliament of the Island Paxos (therefore the algorithm got known as the Paxos algorithm). In 2001 he rewrote the article and published it without the metaphor in the article "Paxos made simple".

To understand some of the quotes in the metaphor, he mentioned the following correspondence:

- A legislator is a server including a database
- A messenger are the messages the servers can send to each other
- A decree is an input value

Lamport described a few requirements for this system to work , between "()" are citations directly from the article "the part-time parliament":

1. **The history can't be changed** ("*Ledgers were written with indelible ink, and their entries could not be changed.*")
2. **No validation of the input** ("*Paxon legislators were willing to pass any decree that was proposed.*")
3. **Communication only by messages** ("*Legislators could communicate only by messages, as many messengers as they needed*.")
4. **Databases were available for reads** ("*Legislators carried their ledgers at all times, and could always read the list of decrees*.")
5. **Nodes were honest** ("*The official records of Paxos claim that legislators and messengers were scrupulously honest and strictly obeyed parliamentary protocol. Dishonesty, although rare, undoubtedly did occur*.")
6. **Double or lost messages shouldn't become a problem** ("*Messages can be lost or delivered multiple times*.")
7. **Nodes could come and go anytime** ("*Legislators could disconnect for unlimited amount of time*.")
8. **All databases are updated once connected** ("*However, achieving consistency required that if one legislator had an entry in his ledger for a certain decree number and another did not, then the second legislator would eventually fill in that entry*.")
9. **How many nodes exist is saved in the data, to decide what's a majority of the nodes.** ("*The Paxons decided to add and remove members of Parliament by decree*.")

There're also 4 main requirements that the system has to meet. These are basically guarantee consistency, allow any node to fail or disconnect, guarantee progress and detect malicious actors.

Consistency

"*The first requirement of the parliamentary protocol was the consistency of the ledgers, meaning that no two ledgers could contain contradictory information.*" (Lamport, 1998)

In other words, whenever someone adds a value for line number 30, no one else could have a different value for line number 30. In the article Lamport published a few years later, he specified this requirement split into three requirements:

"*Only a value that has been proposed may be chosen, only a single value is chosen and a process never learns that a value has been chosen unless it actually has been.*" (Lamport, 2001)

This doesn't explicitly say that the ledgers need to be identical. If one ledger would be completely blank, it still doesn't contain contradictory information. Later he mentioned that if a value had been chosen, then other legislators would eventually learn this value.

"*However, achieving consistency required that if one legislator had an entry in his ledger for a certain decree number and another did not, then the second legislator would eventually fill in that entry. " "When inconsistencies were recognized, they could easily be corrected by passing decrees." "The difficult problem lay in correcting inconsistent ledgers even if no one was aware of the inconsistency.*" *"Unfortunately, we don't know exactly what sort of self-stabilization property the Paxon Parliament possessed or how it was achieved. Paxon mathematicians undoubtedly addressed the problem, but their work has not yet been found. I hope that future archaeological expeditions to Paxos will give high priority to the search for manuscripts on self-stabilization.* " (Lamport, 1998)

At that time he couldn't say exactly how this was possible. It might be possible that when the process is done properly and every decree that is chosen will be added to the database correctly and it's not possible to make any changes, then there's no need for self-stabilization.

"Ledgers were written with indelible ink, and their entries could not be changed." (Lamport, 1998)

Fault Tolerant

"*The protocol guarantees consistency even if priests leave the chamber or messages are lost."* "*A messenger could be counted on not to garble messages, but he might forgot that he had already delivered a message, and deliver it again. He might leave forever, in which case the message would never be delivered.*" (Lamport, 1998)

In a distributed network, it's important that any process and node keeps functioning even if one of the systems fails or disconnects. The protocol only needs a majority to respond to accept a certain decree, the rest could fail or those messages could be lost. This also means that the system can't wait forever on responses, it should simply time-out if there're not enough responses. The only thing important is to know when there is a majority.

Even if no majority would be online, the request to change the data should be kept "on hold". Lamport uses a scenario of balloting (voting rounds) to make sure whenever a value is accepted by a majority, everyone should get the same outcome. When no majority would respond, they basically wait for the next ballot (voting) to decide what the outcome will be.

Progress

"*If a majority of legislators stayed in the chamber and no one entered or left the chamber for a sufficiently long period of time, then any decree proposed by a legislator in the chamber would be passed, and every decree that had been passed would appear in the ledger of every legislator in the chamber.*" (Lamport, 1998)

This means that no value would get lost or deadlock the network, and defines what nodes in the network must do in order to guarantee progress. It only says that legislators in the chamber (online nodes) would record the data in their database. This can be interpreted in two ways: only the ones who are present will record the value and the others won't or the others would need to record the value eventually as well.

When the steps are described in more detail, the last two steps are:

" (*5) If p has received a Voted(b, q) message from every priest q in Q (the quorum for ballot number b), then he writes d (the decree of that ballot) in his ledger and sends a Success(d) message to every priest.*

(6) Upon receiving a Success(d) message, a priest enters decree d in his ledger. " (Lamport, 1998)

This indicates that every node in the network would record any decree even if it wasn't there. In this case this would mean that the initiator (or leader) could be malicious and send a success message without the first steps and everyone would save it in the ledger. From a security perspective, there needs to be a measure in place to avoid this.

Then another aspect needed for this requirement is to make sure every node in the network works with the same time.

"*The Paxons realized that any protocol to achieve the progress condition must involve measuring the passage of time."* (Lamport, 1998)

The system only has to know in what order all the different actions/messages took place. With these logical clocks there was no more need to use physical time because a system could use the so called "happened before" relation.

When agreement is reached on a new proposed value, it will be added to the database. When at least 51% of the nodes are honest, one can assume that only correct values will be added to the dataset.

Non Malicious (Byzantine Generals Problem)

"*The official records of Paxos claim that legislators and messengers were scrupulously honest and strictly obeyed parliamentary protocol.*" "*by sending contradictory messages, a malicious legislator could cause different legislators' ledgers to be inconsistent.*" (Lamport, 1998)

Since this network should guarantee consistency, there should be a method to make sure no database could be inconsistent. In other words, when a malicious node is sending contradicting information, this should be identified. This is known as the Byzantine Generals Problem - (Lamport, Shostak & Pease, 1981).

This problem is explained with the scenario where 3 generals would be camped around a village they want to attack together or evacuate together. They can only communicate via messages so if one would be malicious and send "attack" to one and " evacuate" to the other, they all would act differently and the mission would fail. They need a way to verify that the messages are inconsistent and detect which is malicious.

With messages the only way this can be done is to verify the sender of the message. This means that from every message that is send or the value chosen, a digital signature is needed. So it's important that within the network of databases in one way or another this can be identified. Compared to the generals problem, they could easily detect who would be wrong. The figure below will make clear how this is possible.

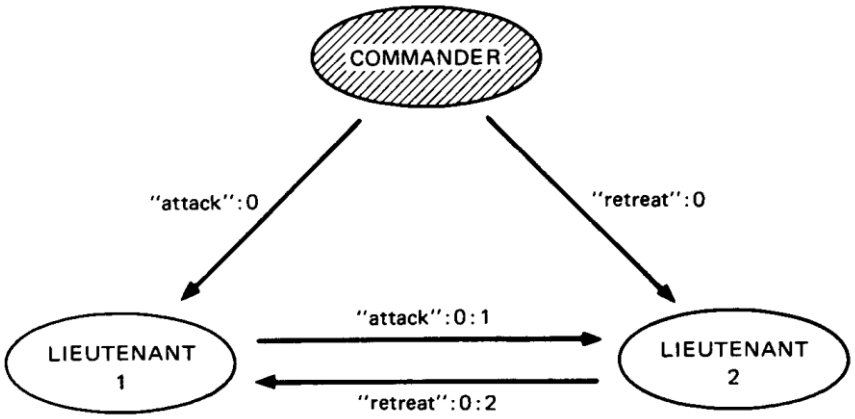


Figure 1: Byzantine Generals Problem (Lamport et al., 1981)

Only when using a method where the signature can't be falsified, one can rely on the correctness of the signature and thus rely on the message. This might be possible by simply knowing who's in the network.

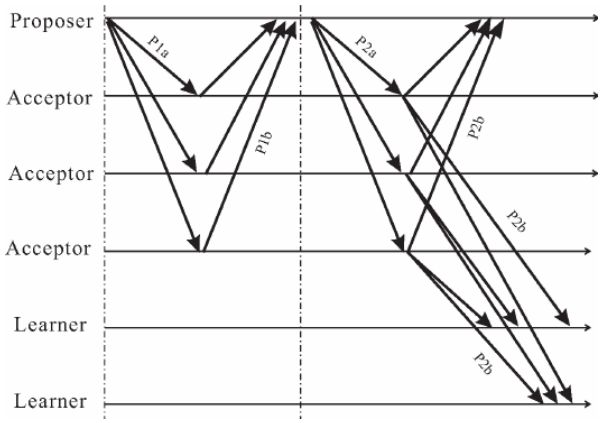
Even when knowing the sender of the message, in this situation one can't verify the correctness of the value but one knows all messages are equal.

How it works

Lamport mentioned three different tasks (proposer, acceptor and learner) in the proposed database structure. Each node in the network could be either one or multiple tasks.
"*Consensus is usually expressed in terms of agreement among a set of processes. Instead, we characterize it in terms of three classes of agents:*
Proposers (A proposer can propose values.)
Acceptors (The acceptors cooperate to choose a single proposed value.)
Learners (A learner can learn what value has been chosen.) " (Lamport, 2004)

Whenever someone wants to save or change something in the database, this will be done on any of the nodes that will convert this into a proposal. This proposal is send to the acceptors and when a majority accepts this, they'll send this to the learners to make sure everyone knows about the new added value.

The basic idea is, when one can guarantee that history can't be changed, and new input will be added similar everywhere in the network then one can guarantee consistency. To guarantee that the input is going to be added in all databases similar and no one can add something else, the system will use a few standard messages. This is shown in figure 2 below. The phases used are described next to the figure.



- The proposer asks "Do you want to accept value 'X' for number 30 or do you already have a value?" (P1a)
- The acceptors will respond "no we don't have this yet, I want to accept, (before actually doing so)" (p1b)
- When a majority of nodes respond they want to accept value 'X', then the proposer will send a message to everyone to accept the value. (p2a)
- Last step is all acceptors send everyone a message that they accept the value (p2b)

Figure 2: Validation of messages in Paxos (Zhao, 2015)

The learners and other acceptors can easily determine if a majority has accepted the value. Only if a majority accepts the value, it's considered to be a "chosen" value.

A more complex explanation including the mathematical calculations can be found in the articles from Lamport (1998, 2001).

After a value is accepted, the system needs to make sure everyone learns about the new value. This function as learner can be implemented in different ways. The learner can be implemented as an algorithm that continuously runs and checks new values or simply waits

for new values to be told. It could also refer to a machine learning algorithm that can guarantee correct values to be learned from the decision making process.

Implications

There're still a few aspects that can cause a security issue. The fact that Lamport assumed that the database is written with indelible ink doesn't mean it's possible to program this.

Another thing is that there's no validation by the nodes on the input so they might not detect faulty input. It's based on trust of the nodes that they are honest. This might be realized when the system continuously checks for malicious actors.

Summarizing, the Paxos algorithm can be used for distributed systems where consistency is needed between databases on different physical locations. Reaching consensus about new data between the elements in the network is an essential part. This protocol however doesn't include verification of the proposed new values, it assumes nodes to be honest and thus proposals should be correct. If honesty among the nodes can be guaranteed, the protocol can guarantee consistency.

2.2.3. Paxos in machine to machine communication

The protocol described in the previous paragraph can be used in the communication between machines. As described earlier the software component related to a particular machine makes it possible to communicate. As stated by IBM, the consensus protocol is essential in machine to machine communication with blockchain technology.

"*All nodes validate the information to be appended to the blockchain, and a consensus protocol ensures that the nodes agree on a unique order in which entries are appended.*" (Cachin & Vukolić, 2017)

There're many more consensus algorithms, but this research focused on Paxos because it is already being used in for example Google megastores and according to IBM research, it's one of the most prominent algorithms.

"*This section presents background and models for consensus in permissioned blockchains, the most prominent family of protocols for this task, which is based Paxos/Viewstamped Replication (VSR) and PBFT.* " (Cachin & Vukolić, 2017)

In 2015 IBM together with Samsung Electronics developed the Autonomous Decentralized Peer-to-Peer Telemetry (ADEPT) network. This was found to be a potential solution to a decentralized IoT environment:

"*Our PoC validated the feasibility of both implementing the foundational functions of a decentralized IoT, and enabling device autonomy in IoT transactions and marketplaces. ADEPT opens the door for the electronics industry to further explore the challenges and opportunities of potential hybrid models that can address the complexity and variety of*

requirements posed by an Internet that continues to scale." (Pureswaran, Panikkar, Nair & Brody, 2015).

This network was created from the idea to facilitate the growing number of Samsung machines that get connected, like laundry machines that need to order their own washing powder and spare parts.

At the end of 2015 IBM contributed to the development of Hyper Ledger Fabric, the first permissioned (closed) blockchain platform where businesses could get their own blockchains. The main network would be operated by Hyper Ledger Fabric but the information shared on the private blockchains shouldn't be visible by the owners of the blockchain, only by the owners of the data. The customers who created their own private blockchain would stay in control of their own data.

"*Intended as a foundation for developing applications or solutions with a modular architecture, Hyperledger Fabric allows components, such as consensus and membership services, to be plug-and-play. Hyperledger Fabric leverages container technology to host smart contracts called "chaincode" that comprise the application logic of the system.* " (Hyperledger org, 2018)

Again consensus was considered to be the most important element in this blockchain technology. However in this particular situation, the company or party in control of Hyper Ledger Fabric will have an increasing power since the others rely on it. Potentially a solution should include machines that have the ability to learn and have the authority to make decisions, therefore a study on machine learning can be found in the next paragraph.

2.4. Machine learning

The term machine learning was coined and described by Samuel (1959), which since then has been widely adopted:

"*Machine learning is an application of artificial intelligence (AI) that provides systems the ability to automatically learn and improve from experience without being explicitly programmed.*" (Samuel, 1959)

The basic idea of machine learning is that computers can learn. This is a discussion topic dating from before 1950, but the most well-known statement comes from Turing (1950):

"*I propose to consider the question, "Can machines think?" This should begin with definitions of the meaning of the terms "machine" and "think."*" (Turing, 1950)

He described "the imitation game" as a test to prove that machines could learn. At the time no machine was able to do so, since then this test has become known as the Turing test. Also in this same year 1950 Shannon published an article in which he described a method to let a computer program play a game of chess. The actual goal of this project was to show that computers can learn.

"*Chess is generally considered to require "thinking" for skilful play; a solution of this problem will force us either to admit the possibility of a mechanized thinking or to further restrict our concept of "thinking"*" (Shannon, 1950)

Shannon described the procedures to deal with certain problems don't always require to come up with the optimal solution, but rather with a calculated option that would satisfy. This is derived from the concept of how people are assumed to think.

"*The proper procedure involves general principles, something of the nature of judgement, and considerable trial and error, rather than a strict, unalterable computing process. Finally, the solutions of these problems are not merely right or wrong but have a continuous range of "quality" from the best down to the worst. We might be satisfied with a machine that designed good filters even though they were not always the best possible.*" (Shannon, 1950)

The article resulted in the Proposal for the Dartmouth Summer Research Project on Artificial Intelligence (McCarthy, Minsky, Rochester & Shannon, 1955). Again the fundamental idea was that machines can learn like humans do, using the method of (artificial) neural network.

"*The study is to proceed on the basis of the conjecture that every aspect of learning or any other feature of intelligence can in principle be so precisely described that a machine can be made to simulate it.*" (McCarthy et al., 1955)

The idea already existed in this proposal that machines could learn from different sources like sensory data, could combine this to learn other, more valuable things and draw conclusions from it.

"*A number of types of "abstraction" can be distinctly defined and several others less distinctly. A direct attempt to classify these and to describe machine methods of forming abstractions from sensory and other data would seem worthwhile*". (McCarthy et al., 1955)

This proposal resulted in the 8 weeks project in the summer of 1956, where many experts came together to study and share ideas. This is when the study field of Artificial Intelligence was born.

The next step was made in 1958 when Rosenblatt (1959) published a paper describing the Perceptron, which is basically an algorithm to describe and transform different variables as input data into more detailed data to classify certain things. The perceptron can learn from previous data by gathering feedback and improving the relation between different variables. The figure below shows the idea of the perceptron.

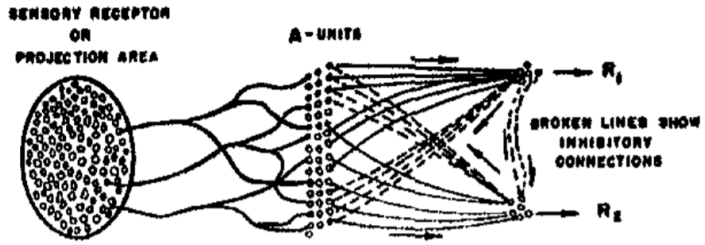


Figure 3: Schematic representation of connections in a simple perceptron (Rosenblatt, 1959)

This is used in a neural network where many different inputs from different sensors can send their values. In order to draw conclusions out of all their variables, the perceptron takes the data and calculates an outcome based on the relation between the data. In this way it could classify (calculated guess) new data by comparing it to what it has seen before.

"*Recognition of any stimulus involves the matching or systematic comparison of the contents of storage with incoming sensory patterns, in order to determine whether the current stimulus has been seen before, and to determine the appropriate response from the organism*". (Rosenblatt 1959)

In reaction Minsky and Papert (1969) criticized that a single perceptron couldn't solve all problems. This resulted in a cut of funds for much projects working on this concept of the perceptron. This turned when improvements were made and innovations like the backpropagation algorithm described by Werbos (1974) could solve these problems. Also the perceptron was found to be useful in multiple layers where each layer modifies the data a little bit and sends it to the next perceptron until the data eventually can be classified.

This field of Artificial Neural Networks has made significant improvements until it got a lot of attention in 1997, when a computer beat the world chess player Garry Kasparov:

"*On May 11, 1997, an IBM computer called IBM Deep Blue beat the world chess champion.*" (IBM, 1997)

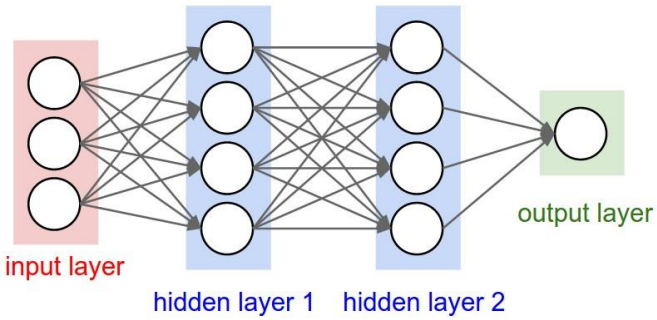
Although it wasn't a clear win (2 wins, 3 draws and 1 loss for the machine) and a request for a rematch wasn't honored, it started a new era in which people began to realize that computers potentially outsmart humans in certain areas. Although chess has many possibilities, it's still based on a set of fixed rules. Therefore the machine to beat a human in chess "only" had to do much calculations. At the time a computer like Deep Blue needed a lot of space and power, but nowadays free online chess games can win from human champions.

In 2010 IBM announced a computer called Watson. This computer was initially designed to beat humans in the game Jeopardy. This is a game in which contestants are tested on their "knowledge". The difference is that the presenter in this game gives hints and the contestants need to find the question that would suit the answer given. This makes it harder for the machine algorithm to come up with the correct response, since it needs to understand the hints first. Later this machine Watson developed into a machine that could answer sophisticated questions, asked in speech. Nowadays the program is commercially available for companies in all different industries with extraordinary complex questions. Watson might still be able to see all variables and come up with an answer.

In 2016 a machine learning program from Google beat Korean grandmaster Lee Sedol, this time in the board game GO. This game has much more variations and also more intuition is involved that simply can't be calculated. The machine learning algorithms basically calculated the best chances to win, similar to what humans would do.

"*The game of Go has long been viewed as the most challenging of classic games for artificial intelligence owing to its enormous search space and the difficulty of evaluating board positions and moves. These deep neural networks are trained by a novel combination of supervised learning from human expert games, and reinforcement learning from games of self-play. Without any lookahead search, the neural networks play Go at the level of state-of-the-art Monte Carlo tree search programs that simulate thousands of random games of self-play*" (Silver & Huang, 2016)

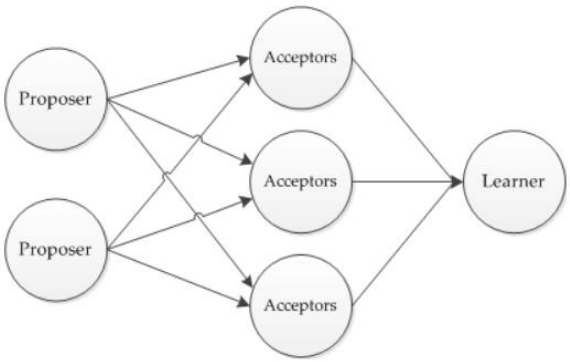
The essential idea from these Artificial Neural Networks is that many inputs can be combined and the network can learn from this data. This corresponds well to the Paxos algorithm described in the previous paragraph. Paxos is also a network of individual functioning components that can communicate, exchange data and can learn from what has been chosen.



This figure illustrates an Artificial Neural Network where the input comes from different nodes, is handled by different nodes and then has a single output on which can be learned.

Figure 4: Illustration of an Artificial Neural network (Karpathy, 2018)

In 2001 Lamport described the Paxos protocol but included a distinguished learner.



"*We let the three roles in the consensus algorithm be performed by three classes of agents: proposers, acceptors, and learners. In an implementation, a single process may act as more than one agent, but the mapping from agents to processes does not concern us here*." (Lamport, 2001)

In this process the nodes send their proposals to different nodes that verify this and eventually the learner would learn what value has been chosen.

Figure 5: Paxos consensus algorithm (Macdonalds, 2012)

If a network of different operating nodes is based on the Paxos protocol, it might be able to agree and learn on the security of the network based on different input variables that the nodes can send. For example every node in the network sends their own software status or security software status and the actions it wants to take. This is verified by other nodes in the network, based on previous data. At the end of this process, it can calculate if the individual node should be trusted. This could enforce simple things like nodes updating their security software or operating software but potentially detect anomaly changes that identify intrusions. These nodes in the network would be doing their own specified functions but work together as a whole to reach consensus to ensure security. This is assumed to be more effective than human operators could be.

"*Network learning effects are another benefit of machine interconnection with a system." "Building out intelligent systems harnesses the benefit of widely deploying intelligent devices. Once an increasing number of machines are connected within a system, the result is a continuously expanding, self-learning system that grows smarter over time. "* (Evans & Annunziata, 2012)

For a long time computers were mainly having the advantage of being quicker in analyzing, but intuition, for example, was very hard. Now analyzing a network of connected operating machines is an enormous task that humans simply can't do, let alone do it as fast as machines. With the increasingly autonomous operating and connected machines, it's necessary to look for possibilities to include machine learning to protect these networks. The Paxos algorithm might support machine learning in Artificial Neural Networks.

3. Research project

3.1. Problem definition

Currently devices all over the world rapidly get more and more connected to the internet and to each other. The problem arises that today a network with on a large scale connected devices, can't effectively be protected against malicious actors.

The detailed literature study has shown that the software on all sorts of devices is developed to be open in its communication and interoperability. Manufacturers focus on the benefits of new developments. However, by connecting large amounts of small devices, a vulnerable network will be created. Simple devices already have been used for DDoS attacks. If they also can be used to intrude and corrupt their own network lying behind, all security doors will be opened unintentionally. Literature study on cybersecurity has shown that most intrusions include some sort of software change on a certain machine in the network, from where it can spread or act. Literature about the blockchain technology and its consensus algorithm Paxos clarifies, that it enables machines to cooperatively work in a network and make decisions. The literature about machine learning shows that algorithms can be used to improve the decision-making skills of machines.

The question arises whether or not machines in an industrial network can be taught to protect themselves autonomously, by prohibiting anyone to mess with their software.

3.2. Research questions

This research is focusing on the possibility to use the blockchain technology with its consensus algorithm Paxos, as foundation for a better secured autonomous machine network. The following research question is defined for this project:

Is the consensus algorithm Paxos, if possible in combination with machine learning, suitable to improve intrusion detection systems in Industrial Internet of Things networks?

To answer this question, the following sub-questions will be studied:

How can blockchain technology be used to better secure IIoT networks?
Is the proposal possibly a feasible solution to improve intrusion detection in IIoT networks?

3.3. Significance of the study

This study intents to develop a scenario that could result in better secured industrial networks of interconnected machines. Financial costs and benefits are impossible to calculate in the context of this research. Specialists in the technologies concerned will have to study on that, if the proposal is generally considered to be worth exploring. However, it can be stated that one undoubtedly needs a way to create more secured (I)IoT environments. The rapidly increasing physical and financial risks involved with cyber-attacks makes this study extremely relevant.

3.4. Research methods

The research strategy used for this project is the exploratory case study (Yin, 2013). With the critical literature study described in chapter two, knowledge about the topics Internet of Things, cybersecurity, blockchain (with Paxos) and machine learning was gathered. This contributed to a clear understanding of theories, innovations, developments, concepts and opportunities. It also made the extent of the problem very clear, as well as a possible solution to that problem.

Based on the Paxos consensus algorithm, a proposal will be made to add an extra layer of security in IIoT networks, by teaching machines to check another's trustworthiness. The model proposed will then be discussed with experts in all relevant areas.

This will be done via semi-structured interviews with open questions to all interviewees. The interviewees will be carefully selected to make sure experts with different views and backgrounds are included. However, it’s unlikely to find experts with extended knowledge on all topics, so the first questions will give insight in the knowledge level on every subject and will be scaled. These questions are removed from the transcriptions documented, to guarantee anonymity. After that the proposal will be discussed to find out whether or not it would be a feasible solution and what complications are foreseen. The quotes concerned will be cited and analyzed in a qualitative and quantitative way.

The final result will be a collection of arguments that may lead to the hypothesis that the model proposed may or may not make industrial networks better secured.

4.0. Blockchain technology in an IIoT network

4.1. Proposal

An industrial network of machines can be compared to a private blockchain network. The devices in the network should be identifiable and only a defined set of machines are allowed in the network. This research project led to the development of the following scenario. This is an industrial process with big operating machines, all known to the network and closed to unauthorized machines. A minimum of 4 machines would be connected and operating and can be considered the “center”. They operate individually but are connected to each other although it’s not guaranteed that they’re connected all the time.

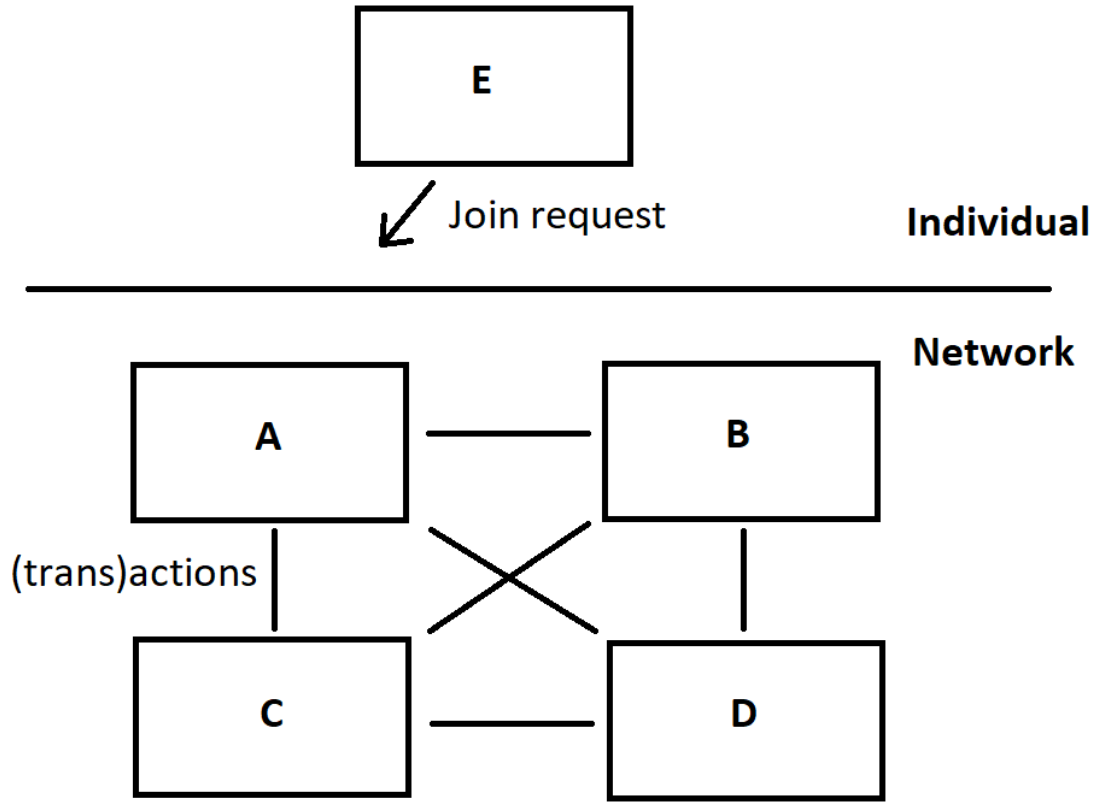


Figure 6: Scenario industrial network

Each node can perform its intended operations individually
Each node in the network can identify itself
In the network every action gets “published” and verified by the other nodes
Every node saves its verified actions (“witnessed”)

Concept

This proposal is a scenario that would be the basis of a protocol to better secure a network of machines (industrial or critical infrastructures) where new values can't always be verified. Some requirements must be guaranteed:

- The nodes in the network can be identified
- The nodes in the network can be trusted before joining or performing any actions
- The network (all connected nodes) is able to verify the state of the individual nodes

In this concept the network needs to be protected from other machines that are not allowed in the network. Because it's a private network and machines can be assumed to work correctly, as long as there's no influence from outside. Therefore the network has to be able to determine new connection requests and verify actions that are published within the network. Essentially the network is secured as long as malicious nodes can't join and the nodes in the network can be verified to be and stay honest.

Basically when the nodes in the network can verify that each other's software is not compromised, then one can state that the network is secured. Both can eventually be based on a set of rules, but preferably it should also be supported by machine learning algorithms.

In this proposal every machine would still be secured by its personal security measures, just like in the current situation. Once the machine would be connected to the network, it would automatically get verified by the network and thus this proposal adds an extra layer of security. Whenever someone tries to tamper with the software on a certain machine, it should get noticed by the network and the machine won't be allowed in the network until it's fixed. The proposal is based on the following assumptions.

Assumptions

1. When a node is not connected to the network, it doesn't form any threat to the network.
2. Anyone can send a **join request** to join the network, but if the machine is not (yet) in the network nothing else should be accepted.
3. The network can verify every join request via consensus to **verify join requests** among all nodes to grant authority to connect.
4. Once connected, all actions are distributed to the other nodes including data to guarantee the trustworthiness from the individual nodes. What data is shared can be decided upon every different implementation.
5. Other nodes witness and **verify the actions** by consensus and continue (using Paxos).
6. Every machine keeps track of what happened and they keep consistent databases.
7. Every node in the network can look for inconsistencies at any time to ensure honesty within the network.

Verify join request

The system needs to determine whether or not a machine is allowed to connect to the network. It's possible that machines can identify themselves and ensure that this can't be falsified. For example the criteria for this request could be but is not limited to the following set of rules:

- Identifiable (for example IPV6)
- Physical location
- Up to date security standards (security software)
- Software state (changes in software might indicate that it's compromised)

The request will be send to every node in the network and they all evaluate and determine if the new node can be trusted. Once consensus is reached the node can either join or be rejected. The node can send a new request to join but should not go through consensus if nothing is changed to avoid overload of requests. Basically the node should "upgrade" before connecting again if its request is rejected because of the individual security standards. Most important to note is that no person should be able to connect to a certain machine without for example the correct individual security standards. Even though the person might believe the machine is honest and wouldn't do harm to the network, the network and the algorithms are in charge. This keeps the network in control of the secured environment and reduces the risk of malicious actors from outside as well as inside.

Verify actions

Assuming the nodes in the network can't always verify the transactions to be correct, other measures need to be in place. In short the network can verify only the likeliness of correctness of a certain value by determined boundaries or it can verify the trustworthiness of the individual nodes that want to perform a certain action. This step can go quick or take longer, depending on the situation and the frequency. The main security measure would be that everyone in the network can verify each other's status and determine if they might be compromised. Basically they learn from the process of reaching consensus, and not just from the value itself because they can't always determine that would be correct.

Some set of rules to determine this could be:

- Trustworthy score of the participants, similar to the ones when verifying a join request
- Possibility to verify the value
- Consistency of the (trans)action
- Impact

Once the network reaches consensus about the actions or transactions to be correct, they all save the events they witness in their database so it can't be reversed (immutability). Every action in this situation will have a certain machine to be responsible and others that witness.

If they don't accept the proposal, this indicates a malicious actor. Optionally when one wants to avoid many false alarms and needs flexibility, certain actions can be accepted even if the proposed value is new. If the machines aren't compromised, basically can be trusted and the impact of the proposal is minimal, then the value can be trusted as well.

The short benefit would be that machines in the network are forced to stay updated with personal security standards. Over the long term this scenario might become increasingly secured if the network can learn. Assuming this network operates for a certain period and will be monitored but the network is allowed to learn the behavior of the nodes in the network it can become increasingly better secured and more efficient.

Human interaction

Most important is that operators can't solely take any actions to join or change the network and protocols. In the first preferred situation the network decides which nodes to trust, reject or even discard from the network at a certain time. There might be the need for a certain exception plan because especially at the beginning exceptions and false alarms will occur. Again it should be included in the network's protocol that under certain trusted conditions changes can be made. This can include different manual physical actions that need to be taken by certain people or anything like this but that will depend on the situation. Again the mindset should be that one wants to avoid a single point of failure, so even the difficulty to change anything in the network can be adjusted according to the preferred security level.

Once this structure has been applied, one can assume the network would secure itself and every participant once connected. The issue arises that once a single machine gets disconnected it becomes vulnerable for attacks. This shouldn't cause problems when it connects again, since it should be detected by the other machines in the network (it checks if any changes in the software were made).

This principle doesn't affect machines once disconnected, so it should still run its own defenses. Operators could be notified once a machine gets disconnected, this could increase security indirectly. This basically means that the node is under supervision of the network, but once disconnected it can be less secured.

Machine learning

Both set of rules can be extended and preferably be managed by machine learning algorithms. The literature research conducted showed too little evidence of what the possibilities are in this field. It will be asked to the interviewees that have additional knowledge and ideas. Essentially the basic idea would be to implement this scenario with a defined set of rules and let the system learn over time.

Another aspect that should be kept in mind is whether or not the machine learning algorithms should be placed on all nodes. This would take away the risk of single point of

failure from that certain node. On the other hand the other nodes in the network should be able to identify that node as being compromised. Therefore it might be enough to have the machine learning algorithms being only performed on a single secured node. Also it might be possible to run machine learning as neural network on all components of the network and learn from this.

4.2. Expert opinions

The scenario in the previous paragraph is derived from the literature study on different relevant areas. For this research there're also interviews conducted with experts who have knowledge in at least one of the relevant fields IIoT, blockchain, cybersecurity or machine learning. The questions and interviews can be found in appendix B. After each interview the theoretical concept was evaluated to make sure it would still hold.

The main goal of the interviews was to identify and discuss different views and approaches to the proposed scenario. Possibly the experts would identify certain obstacles or problems, or conclude that it's simply not worth to experiment and test such a scenario.

The interviews had a predefined sequence that started with a few introductory questions about the interviewee and general knowledge about the topics IIoT, blockchain, cybersecurity and machine learning. After that the interviewer could identify knowledge gaps and steer the rest of the interview towards the questions about the theoretical concept.

The interviewees were critically selected to make sure experts with different views and backgrounds were included to gain most valuable insight and discussions from the interviews. The complete list of interviewees is included below in alphabetical order.

Interviewee	Function	Company
Dr. ir. M.S. Bargh	Researcher at the WODC Lector on privacy & cybersecurity	Wetenschappelijk Onderzoek- en Documentatiecentrum Ministry of Security and Justice, the Hague University of Applied Sciences, Rotterdam
Study in electrical engineering, telecommunication and PhD in information and communication theory. Current research areas of interest include: privacy by design engineering & privacy enhancing technologies, cybersecurity engineering & data security technologies, distributed systems (algorithms, architecture & protocols) with a focus on privacy preserving data-sharing & intelligence-distribution, and machine learning & (value sensitive) algorithm design for data mining and information fusion.		
D. Burkhardt	PhD researcher in distributed ledger, blockchain and IIoT Leader of the German research team	Ferdinand-Steinbeis institute, Berlin Industrial Internet Consortium
Study in information systems. Focus research on the integration of distributed ledger technology to fields like blockchain and IoT, in combination with other technologies like AI and machine learning. Leader of the German research team within the Industrial Internet Consortium in the field of the IoT or IIoT.		
Dr. ir. S. Choenni	Head of Statistical Data and Policy Analysis	Wetenschappelijk Onderzoek- en Documentatiecentrum Ministry of

	Lectureship Human Centered ICT	Security and Justice, the Hague University of Applied Sciences, Rotterdam
Study in theoretical informatics and PhD in database technology. Research in big data, data mining, e-government, cybersecurity, distributed databases, artificial intelligence, and human centered design. Since 13 years head of the WODC research department. Lectureship research i.a. big data.		
Prof. dr. S. Etalle	Professor and chair of the security group	Technical University of Eindhoven
Study in mathematics. Phd in computer science. Professor in computer security at the Technical University of Eindhoven. Also one of the founders of a company doing network monitoring for industrial environments in order to identify, react, and respond to industrial threats and flaws.		
M. Hennessy	Head architect & project lead for blockchain activities	Philips, Eindhoven
Technology professional with 22 years of working experience in technology, performing architectural, technical as well as product related and customer facing functions. In depth knowledge about software, application frameworks and cloud systems. Embedded systems, building web app ends and reservation systems. Electricity and water network provisioning and maintenance network systems.		
T. Koens	Blockchain researcher PhD researcher in distributed ledgers including blockchain	ING Radboud University, Nijmegen
Study in IT & business processes. Researcher in ING's distributed ledger team. PhD focusing on distributed ledgers, including blockchain technology, both from a computer science as well as information science perspective. 15+ years of experience in security and risk, specifically in threat intelligence and WiFi hacking.		
Dr. E.J.E.M. Pauwels	Senior researcher	Centrum Wiskunde & Informatica, Amsterdam
Study in mathematics. CWI researcher for 16 years. Research in computervision and sensor data. Now focus on data analyses, modeling of time series, predicting time series based on deep learning, as well as more classical techniques. AI from a mathematical point of view. Energy intranets project. Coordinator of NWO-ISCOM Project Scalable Interoperability in Information Systems for Agile Supply Chains (SIISASC).		
Dr. Z. Ren	Postdoc in blockchain technology and consensus algorithms Lecturer in blockchain related topics	Delft University of Technology
Study in telecommunication followed by a PhD focused on information theory. Currently a postdoc researcher in blockchain technology. The major research area is the consensus protocol in blockchain. Background in telecommunication engineering, information theory, and cyber security. Currently involved in multiple blockchain projects includes finance, logistics, energy, IOT and the NWO project "Blockchain and		

Logistic Innovation". Leading researcher in the blockchain innovation and consensus model, communicator to the industry as the expert in blockchain.		
A. de Vries	Senior consultant and blockchain specialist	PricewaterhouseCoopers, Amsterdam
Study in economics and business. Post graduate business analytics & data science. First career in banking. Because of Bitcoin technology knowledge transfer to PWC. Data analyses and security, then consultant in blockchain technology. Now in the PWC Experience Center Emerging Technologies team with a focus on blockchain and AI.		

Table 1: List of interviewees with their function and expertise

All interviews are documented and each transcription has been verified by the interviewee and can be found in appendix B. In appendix B. the interviewees are not listed in alphabetical order. The order is randomly selected, therefore interviews can't be traced to an individual person. However, the interview numbers do relate to all the tables in the current chapter. For all readers that don't understand Dutch, all Dutch quotes are translated in English.
The interview questions are divided into three subsets. The first part includes two questions about the background of the interviewee. These questions are used to create a profile of the interviewees. These questions are also removed from the transcriptions, to guarantee anonymity.

The second part contains three questions about the four different knowledge area's (IoT, blockchain, cybersecurity and machine learning), to gauge the level of the interviewees. All aspects can be scaled from 1 to 5 (from less towards much knowledge about the specific topic). The criteria to determine the score are described in appendix A.

The last part consists of five questions that go into more detail about the proposed concept. These are open questions to give the interviewee the opportunity to give his full opinion and thoughts. In contrast to the first two parts, the last set of questions are analyzed in a qualitative and quantitative manner. The remarks given by the interviewees are noted down, evaluated how many times they get mentioned and handled accordingly.

The questions asked are the following:

4.2.1. Interviews Part 1 – experience and expertise

- **Could you tell me something about yourself and your career in ICT?**
- **Can you shortly describe your experience and expertise in ICT?**

The results of these questions were included in table 1 with the list of interviewees and their expertise.

4.2.2. Interviews Part 2 – knowledge about specific subjects

For all questions the interviewees were scored 1 to 5 (low to high). The full list of criteria for every question and certain scores can be found in appendix A. The scores are transformed into percentages (score 1=0%, 2=25%, 3=50%, 4=75%, 5=100%).

(I)IoT

The following three questions were asked in the interviews:

- **Could you tell me what you know about Internet of Things (IoT)?**
- **Are you familiar with the Industrial Internet of Things (IIoT)?**
- **What consequences do you think these developments have to critical infrastructures?**

All individual scores of the Interviewees are listed in the table below:

Transcription number	Average	1	2	3	4	5	6	7	8	9
IoT/IIoT	**67%**	**75%**	**75%**	**42%**	**83%**	**67%**	**83%**	**83%**	**25%**	**67%**
Definition and components IoT	**83%**	75%	100%	100%	100%	75%	100%	100%	25%	75%
Knowledge about IIoT	**56%**	50%	75%	0%	100%	25%	100%	50%	25%	75%
Consequences for Networks	**61%**	100%	50%	25%	50%	100%	50%	100%	25%	50%

Table 2: Scaled knowledge on IoT/IIoT

Most interviewees had a clear understanding about IoT, on average they scored 83%. When talking about IIoT the knowledge dropped to 56%. About the consequences what this connectivity would do to the network, they scored 61%. All interviewees realize things are getting more and more connected. Also one can imagine much benefits can be gained in industrial purposes. When looking at the bottom line about the consequences of this connectivity, 6 out of 9 interviewees scored 50% or lower, so their answers were focused on the positive consequences. Only 3 out of 9 interviewees realized the potential threats that are created by connecting all those machines:

"*I believe it's getting more and more dangerous. Because during the design of these critical infrastructures they never considered things like the Internet of Things. They didn't consider their equipment will have their own capacity of computation and communication. They are getting more capable devices connected and making it vulnerable to outside sources.*" (interviewee 1)

"*Sure, of course it has been the dream of every hacker that we simply connect all those devices.*" (interviewee 5)

"It's waiting for a disaster to happen, like a certain group or even schoolboys who just lay down the country. It just will certainly happen with those big complex systems and networks with a lot of machines that are connected and communicate. If you're looking for example at power grids with loads of sensors to create better efficiency, this usually makes the network also more vulnerable." (interviewee 7)

Cybersecurity

The following three questions were asked in the interviews:

- **Do you have experience or expertise in cybersecurity?**
- **What do you know about cybersecurity in critical infrastructures?**
- **What do you know about cybersecurity in Industrial Internet of Things?**

The table below shows all individual scores of the interviewees.

Transcription number	Average	1	2	3	4	5	6	7	8	9
Cybersecurity	**54%**	**50%**	**67%**	**67%**	**50%**	**75%**	**33%**	**42%**	**33%**	**67%**
Knowledge about cybersecurity	**78%**	100%	100%	100%	50%	100%	50%	50%	50%	100%
Cybersecurity in critical infrastructures	**53%**	50%	75%	50%	50%	75%	25%	25%	50%	75%
Cybersecurity in IIoT	**31%**	0%	25%	50%	50%	50%	25%	50%	0%	25%

Table 3: Scaled knowledge on cybersecurity

Most interviewees had an understanding of about 78% in cybersecurity, but when it was specific to critical infrastructures the knowledge was about 53%. All interviewees scored 50% or lower on the knowledge about cybersecurity in IIoT. This means that experts from different fields don't realize the threats coming with this increased connectivity. This also means that most experts are mainly focusing on where IIoT can be useful, not necessarily on the security of those networks:

"*You can see from the logs who are actually being compromised or if that someone just fails." (interviewee 1)*

Current critical infrastructures are organized in a centralized manner and the focus is on managing failures and not on security against cyber-attacks:

"They use the detect based spare systems. When they detect that something fails, they will go back to a backup, not actually use distributed scenarios like your proposal." (interviewee 1)

"They seem to be able to manage downtime and outages very accurately." "They don't do or have very basic measures to keep their systems secure." (interviewee 2)

"In the kind of networks that I work on, I'm talking about oil&gas, energy, power generation and manufacturing, there's no agreement on things. There's one system, determining what all other systems are doing. Then there's a safety system checking that all systems are doing the right thing and there's a fallback system in case the initial machine is failing." (interviewee 8)

When talking about IIoT networks, the average knowledge was very low. However 3 interviewees indicated that the individual sensors would be a weak component because attackers could compromise the sensors and change the values:

"*Another problem is that you can mess up with sensors. So it gives false alarms, that causes the system to do abnormal behavior that will harm the system. For example it will tell the network that the temperature is low, even if the temperature is not low. So the controller will heat up and might overheat.*" (interviewee 1)

"*Devices can have an identity in the network, but the question comes about the integrity of the device. Can you trust the data that's coming at you from that device.*" (interviewee 2)

"Those devices are vulnerable, if hackers can mess with the sensors then the network would still be unsecure. That is the problem that IoT will bring and blockchain still doesn't secure this." (interviewee 4)

Blockchain

The following three questions were asked in the interviews:

- **Can you tell what the characteristics are from blockchain technology?**
- **Where do you think blockchain could be useful?**
- **Are you familiar with the consensus algorithm Paxos?**

The table below shows all the individual scores of the interviewees.

Transcription number	Average	1	2	3	4	5	6	7	8	9
Blockchain	**66%**	**92%**	**100%**	**42%**	**67%**	**100%**	**75%**	**92%**	**0%**	**25%**
Knowledge about blockchain technology	**78%**	100%	100%	75%	100%	100%	100%	75%	0%	50%
Use cases of blockchain	**69%**	75%	100%	50%	100%	100%	75%	100%	0%	25%
Paxos consensus algorithm	**50%**	100%	100%	0%	0%	100%	50%	100%	0%	0%

Table 4: Scaled knowledge on blockchain technology

Most interviewees are well aware of blockchain technology (78%). Also the interviewees could tell enough about the use cases for blockchain, so beyond cryptocurrency. When Paxos was discussed, the average knowledge was 50% and in 8/9 cases they scored either 0 or 100%.

Most experts mentioned that the most important aspect from blockchain would be the consensus algorithm to agree on new values. The problem with IIoT, that values can't easily be verified, remains. So basically in the IIoT networks where a lot of data is shared, it's not yet possible to ensure data integrity with blockchain technology.

"Generally you can use any sort of data sharing mechanism, but what is really important, and this is not made possible by blockchain, is the need for a way to make claims in an immutable system that other parties can check for the integrity." (interviewee 2).

"*If I propose I want to go to 100 degrees, then people can come up with reasons why that would be good or bad, machines can't do that and would agree and reach consensus*." (interviewee 3)

"*True, when the data meets the requirements defined beforehand, then it could still be wrong data and the whole network would accept that data*." (interviewee 4)

To use Paxos for this scenario seems a good solution according to one of the interviewees:

"*Very interesting, especially why you use Paxos over PBFT makes a lot of sense here, and is never considered before I think.*" (interviewee 1)

Machine Learning

The following three questions were asked in the interviews:

- **Do you know something about machine learning?**
- **Where do you think machine learning can be useful in Industrial Internet?**
- **What do you know about machine learning in cybersecurity?**

Transcription number	Average	1	2	3	4	5	6	7	8	9
Machine Learning	**44%**	**8%**	**67%**	**8%**	**25%**	**50%**	**58%**	**83%**	**8%**	**83%**
Machine Learning in general	**56%**	25%	75%	25%	25%	50%	75%	100%	25%	100%
Machine Learning in IIoT	**39%**	0%	75%	0%	25%	50%	50%	75%	0%	75%
Machine Learning in Cybersecurity	**36%**	0%	50%	0%	25%	50%	50%	75%	0%	75%
Grand Total	**57%**	**56%**	**77%**	**40%**	**56%**	**73%**	**63%**	**75%**	**17%**	**60%**

Table 5: Scaled knowledge on machine learning

The first thing that can be noticed is that most interviewees didn't have much knowledge about machine learning, in general they scored 56%, but for machine learning in IIoT or critical infrastructures, the score on average was 39%. Although they didn't know how, most experts however did acknowledge that it should be used whenever possible, to increase cybersecurity. The 3 interviewees who scored high on machine learning acknowledged that it should be possible and useful in an Industrial Internet of Things network:

"*It's really about a system where you have a lot of events going on and you try to determine behavior. So you have certain nodes op operations that have been identified in the past as malicious, then you could use machine learning to quarantine that user in your system.*" (interviewee 2)

"*I think in the future it will happen that AI on our network is working to control and secure our network.*" (interviewee 7)

"*It's possible to let machine learning algorithms search for patterns in behavior and when things change they can be detected. You do need a lot of computational power though and therefore is done at a centralized location."(interviewee 9)*

4.2.3. Interviews Part 3 – could it work?

For this part a few questions were asked to test the proposal. Depending on the knowledge of the interviewee the questions about the proposal were adjusted.

- **Do you think blockchain technology could be used in defending these networks?**
- **Do you think blockchain technology could be used to connect components via consensus algorithms and allow them to jointly make decisions?**
- **Do you think machines connected in a network could learn from their decisions and increase security?**

After discussing the proposal, 8 out of 9 interviewees declared that the proposal could work and suggested further research. Interviewee 8 didn't fully agree but saw some potential. Below the quotes that indicate this:

"*But I'm sure that if the attacker could do malicious actions in the node that runs the security protocols and machine learning algorithms, it might cause the security layer to fail. With your proposal that would be better secured. If your scenario is Byzantine Fault Tolerant it definitely would be better secured, because nobody considered BFT in traditional systems*" (interviewee 1)

"*Especially when you have the connectivity between many nodes, and you work together with other companies and you know they're honest and the staff can be trusted. You now need to rely on their word that they're running the right software. It might just be that even though they're honest, they might just don't care about and update. This is very useful that you indeed can do with the blockchain because you can set these rules and let them be verified. So I indeed can see an architecture like this could help*." (interviewee 2)

"*Yes, I certainly think you have a good proposal. 1 thing I know very certain, especially the knowledge sharing usually brings better insights. I think with this proposal it would make it better secured, just the question is if it would be worth the cost, more research will be needed to answer that question. But with these kind of things it's usually that you simply need to build a prototype and then evaluate what works."* (interviewee 3)

"Well that sounds very nice, I don't know any party that's currently looking at this or is trying to solve this problem. At the blockchain we're already hashing and comparing the data and differences are noticed immediately. Maybe in the same way you could compare the consistency of the individual device and when something is different it gets immediately detected and probably something will be wrong." (interviewee 4)

"Within the scenario that you said, this indeed could become valuable or you could use it as an extra layer of defense. Essentially you mean that the nodes in the network don't just reach consensus about the values and the state of the database, they also reach consensus about the security of the network." (interviewee 5)

"That's very interesting to be honest, and I can imagine you need something like that if you think about smart cities or connected cars and other things like that in supply chains. They need to be secure and some mechanisms be in place that guarantee that the parties are trustworthy. Basically it's not good enough to have a secured network, but you also propose some kind of security protocol or second layer that guarantees the trustworthiness between the assets." (interviewee 6)

"I can imagine something like this would work. For this you could maybe also look at how the immune system in our body works. Maybe you could use something like this also in computer networks, so they detect what doesn't belong in the network or is not correct. I think machine learning will eventually be capable of protecting our networks." (interviewee 7)

"*In that case you do have a better security, but if it would be feasible for IIoT networks, that would be fighting a small problem with a big cannon. So I think the solution that you're proposing has value, that certainly. Only the place where you place the solution is probably not the most ideal place where you need it.*" (interviewee 8)

"*To let the others in the network validate your status indeed would be a good idea. In the old way if someone sends a command, the machine would immediately do this. In your proposal it would first be send to the network so they reach consensus about your state and then send the order to the unit and would execute this. That could actually work very well.*"
(interviewee 9)

Potential Issues

Most interviewees came up with a few potential issues. When they're combined, it comes down to the issues communication costs and many false alarms:

Communication costs (mentioned 6 times)

"*I would say if they really do it based on this detection whether or not it would fail etc., it would be better secured at extra cost though.*" (interviewee 1)

"*That will have network and communication cost, so we have some time to go before that's realistic*." (interviewee 2)

"*The question is if it will be worth it, more search needs to be done to answer this question.*"
(interviewee 3)

"*You're sending a lot of messages to reach consensus about a certain value, if you add things like current status, this might require much more capacity.*" (interviewee 5)

"*It would cost more money*." (interviewee 8)

"*You need to look at how much communication cost this will need*." (interviewee 9)

Many false alarms because of minor changes (mentioned 4 times)

"*That might mean that certain nodes get punished a lot, when it acts differently but completely legit it would be classified as untrustworthy*." (interviewee 3)

"*A lot of legit things will happen on the devices, like updates. The question is, how can you manage this.*" (interviewee 4)

"*Especially when new parties come in, how do you calculate the trustworthy score then*." (interviewee 6)

"*I'm not sure if it's possible to compare the status, because things like current time on the machine would always change*." (interviewee 7)

5.0. Conclusions and recommendations for further research

This research was focusing on whether or not blockchain technology could be used to better secure IIoT networks.

In October 2018, the National Institute of Standards and Technology (NIST) published an article named “Blockchain Technology Overview” and started the first chapter about history and background with the following:

“*The core ideas behind blockchain technology emerged in the late 1980s and early 1990s. In 1989, Leslie Lamport developed the Paxos protocol, and in 1990 submitted the paper The Part-Time Parliament to ACM Transactions on Computer Systems; the paper was finally published in a 1998 issue. The paper describes a consensus model for reaching agreement on a result in a network of computers where the computers or network itself may be unreliable. In 1991, a signed chain of information was used as an electronic ledger for digitally signing documents in a way that could easily show none of the signed documents in the collection had been changed. These concepts were combined and applied to electronic cash in 2008 and described in the paper, Bitcoin: A Peer to Peer Electronic Cash System.*” (NIST, 2018)

This indicates that the conclusion in the literature study, about the consensus algorithm Paxos being a fundamental part of the blockchain technology, is correct. Further literature study on machine learning indicates that this might be used as security feature in industrial networks. After the critical literature study a proposal has been designed and described in chapter 4.1. With this proposal the following research sub-question has been answered:
How can blockchain technology be used to better secure IIoT networks?

This proposal was then discussed with experts who have different backgrounds and knowledge on the subjects concerned. The results from the interviews showed that 8 out of 9 experts believe this proposal might be valuable to better secure industrial networks. With that the following research sub-question has an affirmative answer:
Is the proposal possibly a feasible solution to improve intrusion detection in IIoT networks?

Two challenges were indicated by the experts, further research will be needed to verify the following issues:

- How much (communication) costs this will generate;
- How to prevent the network from initiating (too many) false alarms.

At this point costs obviously can’t be calculated yet. The challenge of getting many false alarms would be an investment that would prove itself worthwhile, if the system indeed gets increasingly better at defending the network.

Also with this research it became clear that the experts agree that the increasing connectivity introduces great risks but the knowledge about cybersecurity in IIoT is low. This is mainly due to the focus on the use cases and benefits expected.

This research led to a proposal that suggests to include a consensus algorithm (Paxos) and machine learning algorithms to better secure Industrial Internet of Things networks, by instructing the nodes involved to check their mutual reliability. Experts on IIoT, blockchain, cybersecurity and machine learning agree that the idea is promising. That it might work and is worth to be studied further. Therefore the following research question has been answered:

Is the consensus algorithm Paxos, if possible in combination with machine learning, suitable to improve intrusion detection systems in Industrial Internet of Things networks?

Further research needs to prove the potential of this concept.

References

Ajuntament de Barcelona. (2014). *Barcelona Ciutat Digital*. Retrieved 06-04-2018 from smartcity.bcn.cat/eng

Asher-Dotan, L. (2017). *NotPetya vaccine discovered by cyberreason*. Retrieved 02-07-2018 from https://www.cybereason.com/blog/cybereason-discovers-notpetya-kill-switch

Ashton, K. (2009). *That 'Internet of Things' Thing*. Retrieved 06-04-2018 from http://www.rfidjournal.com/articles/pdf?4986

Bundesamt für Sicherheit in der Informationstechnik (BSI). (2014). *Die Lage der IT-Sicherheit in Deutschland 2014*. Retrieved 24-07-2018 from https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?__blob=publicationFile

Cachin, C. & Vukolić , M. (2017). *Blockchain Consensus Protocols in the Wild*. Retrieved 25-07-2018 from http://drops.dagstuhl.de/opus/volltexte/2017/8016/pdf/LIPIcs-DISC-2017-1.pdf

Chaum, D., Fiat, A., & Naor, M. (1990). *Untraceable Electronic Cash*. Advances in Cryptology — CRYPTO' 88. Lecture notes in Computer Science, vol. 403. Springer: New York.

China Unicom, NTRA Egypt, ZTE Corporation, CART MIIT, ISA CETC, & Alibaba Group. (2017). *Framework of blockchain of things as decentralized service platform.* Retrieved 10-07-2018 from http://www.circleid.com/pdf/T17-SG20-C-0008!!MSW-E.pdf

Chu-Carroll, M. (2015). *Paxos, a really beautiful protocol for distributed consensus*. Retrieved 07-07-2018 from http://www.goodmath.org/blog/2015/01/30/paxos-a-really-beautiful-protocol-for-distributed-consensus/

Cisco. (2018). *VNI Forecast Highlights Tool*. Retrieved 05-04-2018 from https://www.cisco.com/c/m/en_us/solutions/service-provider/vni-forecast-highlights.html

Connor, B. (2018). *Real-Time Cyber Threat Intelligence Is More Critical Than Ever*. Retrieved 15-07-2018 from https://www.forbes.com/sites/forbestechcouncil/2018/05/22/real-time-cyber-threat-intelligence-is-more-critical-than-ever/#6ef8374617fb

Cyber Physical Systems Public Working Group (CPS PWG). (2016). *Framework for Cyber-Physical Systems.* Retrieved 03-07-2018 from https://s3.amazonaws.com/nist-sgcps/cpspwg/files/pwgglobal/CPS_PWG_Framework_for_Cyber_Physical_Systems_Release_1_0Final.pdf)

Dai, W. (1998). *B-Money*. Retrieved 17-05-2018 from http://www.weidai.com/bmoney.txt

European commission. (2016). *Advancing the Internet of Things in Europe - Digitising European Industry - Reaping the full benefits of a Digital Single Market*. Retrieved 06-06-

2018 from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016SC0110&from=EN

Evans, D. (2012). *The Internet of Everything - How More Relevant and Valuable Connections Will Change the World*. Retrieved 07-07-2018 from https://www.cisco.com/c/dam/global/en_my/assets/ciscoinnovate/pdfs/IoE.pdf

Evans, P., & Annunziata, M. (2012). *Industrial Internet: Pushing the Boundaries of Minds and Machines.* Retrieved 18-06-2019 from https://www.ge.com/docs/chapters/Industrial_Internet.pdf

Falliere, N., Murchu, L., & Chien, E. (2011). *W32.Stuxnet Dossier*. Retrieved 06-07-2018 from https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

Frahim, J., Pignataro, C., Apcar, J., & Morrow, M. (2015). *Securing the Internet of Things: A Proposed Framework.* Retrieved 05-03-2018 from https://www.cisco.com/c/en/us/about/security-center/secure-iot-proposed-framework.html

Gartner. (2014). *Threat Intelligence: What is it, and How Can it Protect You from Today's Advanced Cyber-Attacks?*. Retrieved 04-04-2018 from https://www.gartner.com/imagesrv/media-products/pdf/webroot/issue1_webroot.pdf

Guerra, P., & Tamburello, P. (2018). *Modernizing Cybersecurity Operations with Machine Intelligence.* Sebastopol, USA: O'Reilly Media Inc.

Hutchins, E.M., Cloppert, M.J., & Amin, R.M. (2011). *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains.* London: Lockheed Martin Corporation. Retrieved 10-08-2018 from https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf

Hyperledger org. (2018). *Hyperledger Fabric*. Retrieved 23-07-2018 from https://www.hyperledger.org/projects/fabric

IBM. (1997). *Deep Blue*. Retrieved 10-08-2018 from http://www-03.ibm.com/ibm/history/ibm100/us/en/icons/deepblue/

Industrial Internet Consortium (IIC). (2018). *The industrial internet consortium: a global not-for-profit partnership of industry, government and academia*. Retrieved 26-06-2018 from https://www.iiconsortium.org/about-us.htm

Industrial Internet Consortium (IIC). (2018). *What is the industrial internet?*. Retrieved 26-06-2018 https://www.iiconsortium.org/about-industrial-internet.htm

Jackson, D. (2017). *The Rising Dangers of Unsecured IoT Technology*. Retrieved 07-07-2018 from https://www.secureauth.com/company/newsroom/rising-dangers-unsecured-iot-technology

Johnson, B., Caban, D., Krotofil, M., Scali, D., Brubaker, N., & Glyer, C. (2017). *Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure.* Retrieved 30-06-2017 from https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html

Karpathy, A. (2018). *Convolutional Neural Networks for Visual Recognition*. Retrieved 27-11-2018 from http://cs231n.github.io/neural-networks-1/

Kasperskylab. (2017). *New Petya / NotPetya / ExPetr ransomware outbreak*. Retrieved 02-07-2018 from https://www.kaspersky.com/blog/new-ransomware-epidemics/17314/

Khalimonenko, A., Kupreev, O., & Badovskaya, E. (2018). *DDoS attacks in Q1 2018*. Retrieved 02-07-2018 from https://securelist.com/ddos-report-in-q1-2018/85373/

Krebs, B. (2016). *KrebsOnSecurity Hit With Record DDoS*. Retrieved 25-06-2018 from https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/

Lamport L. (1978). *Time, Clocks, and the Ordering of Events in a Distributed System*. Retrieved 02-03-2018 from https://lamport.azurewebsites.net/pubs/time-clocks.pdf

Lamport, L. (1998). *The Part-Time Parliament*. Retrieved 05-02-2018 from https://lamport.azurewebsites.net/pubs/lamport-paxos.pdf

Lamport L. (2001). *Paxos Made Simple*. Retrieved 07-04-2018 from https://lamport.azurewebsites.net/pubs/paxos-simple.pdf

Lamport, L. (2004). *Lower Bounds for Asynchronous Consensus*. Retrieved 15-05-2018 from https://lamport.azurewebsites.net/pubs/lower-bound.pdf

Lamport L., Shostak, R., & Pease, M. (1981). *The byzantine generals problem*. Retrieved 03-04-2018 from https://people.eecs.berkeley.edu/~luca/cs174/byzantine.pdf

Lee, R.M., Assante, M.J., & Conway, T. (2016). *Analysis of the Cyber Attack on the Ukrainian Power Grid.* Retrieved 15-07-2018 from https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

Macdonald, A. (2012). *Paxos By Example*. Retrieved 5-7-2018 from https://angus.nyc/2012/paxos-by-example/

Madakam, S., Ramaswamy, R. & Tripathi, S. (2015). *Internet of Things (IoT): A Literature Review*. Journal of Computer and Communications" , 3, 164-173. Retrieved 15-04-2018 from http://dx.doi.org/10.4236/jcc.2015.35021

Maersk. (2017). *A.P. Moller - Maersk improves underlying profit and grows revenue in first half of the year.* Retrieved 08-08-2018 from https://www.maersk.com/press/press-release-

archive/2017/20170816-a-p-moller-maersk-improves-underlying-profit-and-grows-revenue-in-first-half-of-the-year

McCarthy, J., Minsky, M.L., Rochester, N., & Shannon, C.E. (1955). *A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence.* AI Magazine Volume 27 Number 4. Retrieved 22-11-2018 from https://www.aaai.org/ojs/index.php/aimagazine/article/download/1904/1802

Minsky, M., & Papert, S. (1969). *Perceptrons*. Oxford, England: M.I.T. Press.

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Retrieved 03-03-2018 from https://bitcoin.org/bitcoin.pdf

National Cybersecurity and Communications Integration Center (NCCIC). (2018). *MAR-17-352-01 HatMan—Safety System Targeted Malware*. Retrieved 10-07-2018 from https://ics-cert.us-cert.gov/sites/default/files/documents/MAR-17-352-01%20HatMan%20-%20Safety%20System%20Targeted%20Malware%20%28Update%20A%29_S508C.PDF

National Institute of Standards and Technology (NIST). (2018). *Blockchain Technology Overview*. Retrieved 30-11-2018 from https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf

Özsu, M.T., & Valduriez, P. (1991). *Principles of Distributed Database Systems*. Englewood Cliffs, NJ: Prentice-Hall

Pureswaran, V., & Brody, P. (2015). *Device democracy - Saving the future of the Internet of Things*. Retrieved 15-07-2018 from https://www-935.ibm.com/services/multimedia/GBE03620USEN.pdf

Pureswaran, V., Panikkar, S., Nair, S., & Brody, P. (2015). *Empowering the edge - Practical insights on a decentralized Internet of Things.* Retrieved 12-05-2018 from https://www-935.ibm.com/services/multimedia/GBE03662USEN.pdf

Roadtraffic-technology. (2015). *M42 Active Traffic Management Scheme, Birmingham*. Retrieved 06-03-2018 from https://www.roadtraffic-technology.com/projects/m42/

Rosenblatt, F. (1959). *The perceptron: a probabilistic model for information storage and organization in the brain.* Psychological Review Vol. 65, No. 6. Retrieved 22-11-2018 from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.335.3398&rep=rep1&type=pdf

Rouse, M. (2018). *Industrial internet of things (IIoT)*. Retrieved 10-07-2018 from https://internetofthingsagenda.techtarget.com/definition/Industrial-Internet-of-Things-IIoT

Samuel, A.L. (1959). *Some Studies in Machine Learning Using the Game of Checkers*. Retrieved 15-07-2018 from https://www.cs.virginia.edu/~evans/greatworks/samuel.pdf

Sauerwein, C., Sillaber, C., Mussmann, A., & Breu, R. (2017). *Threat Intelligence Sharing Platforms: An Exploratory Study of Software Vendors and Research Perspectives*. Retrieved

10-07-2018 from https://pdfs.semanticscholar.org/0b9b/00a2dbf6ae467395fac917e0f7b73cc3e7aa.pdf?_ga=2.13979377.710190.1535366208-979846532.1535366208

Schwab, K. (2016). *The fourth industrial revolution*. Geneva, Switzerland: World Economic Forum.

Shannon, C.E. (1950). *Programming a Computer for Playing Chess*. Philosophical Magazine, Ser.7, Vol. 41, No. 314. Retrieved 15-07-2018 from https://pdfs.semanticscholar.org/64a0/3e75e867b67de855d6d6c6013df9600d53ae.pdf

Shneyder, L. (2018). *Unsecured IoT, Unlimited Vulnerabilities*. Retrieved 08-07-2018 from https://sendgrid.com/blog/unsecured-iot-unlimited-vulnerabilities/

Silver, D., & Huang, A. (2016). *Mastering the game of Go with deep neural networks and tree search.* Retrieved 25-07-2018 from https://www.nature.com/articles/nature16961#abstract

Singer, P.W., & Friedman, A. (2014). *Cybersecurity and cyberwar : what everyone needs to know".* New York: Oxford University Press.

Szabo, N. (1994). *Smart Contracts*. Retrieved 08-05-2018 from http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html

Turing, A.M. (1950). *Computing Machinery and Intelligence*. Mind 49: 433-460. Retrieved 20-06-2018 from https://www.csee.umbc.edu/courses/471/papers/turing.pdf

Verizon. (2016). *Data breach digest. Scenarios from the field*. Retrieved 26-07-2018 from http://www.verizonenterprise.com/resources/reports/rp_data-breach-digest_xg_en.pdf

Virginia Tech Transportation Institute. (2016). *Automated vehicle crash rate comparison using naturalistic data*. Retrieved 06-04-2018 from https://www.vtti.vt.edu/featured/?p=422

Weiser, M. (1991). *The Computer for the 21th Century*. Retrieved 15-07-2018 from https://www.lri.fr/~mbl/Stanford/CS477/papers/Weiser-SciAm.pdf

Werbos, P.J. (1974). *The Roots of Backpropagation - From Ordered Derivatives to Neural Networks and Political Forecasting.* USA: Wiley-interscience.

World Economic Forum. (2017). *Realizing the Potential of Blockchain - A Multistakeholder Approach to the Stewardship of Blockchain and Cryptocurrencies*. Retrieved 12-05-2018 from http://www3.weforum.org/docs/WEF_Realizing_Potential_Blockchain.pdf

Wright, A., & Filippi, P. (2015). *Decentralized blockchain technology and the rise of LEX cryptographia*. Retrieved 14-05-2018 from https://www.intgovforum.org/cms/wks2015/uploads/proposal_background_paper/SSRN-id2580664.pdf

Yin, R.K. (2013). *Case Study Research – Design and Methods.* Los Angeles, USA: Sage Publications Inc.

Zhao, W. (2015). *Fast Paxos Made Easy: Theory and Implementation*. Retrieved from http://www.academia.edu/20859091/Fast_Paxos_Made_Easy

Appendices

A: Interview questions and scaling criteria

Below is the full list of criteria to determine the knowledge scores of an interviewee about a certain topic.

(I)IoT

- **Could you tell me what you know about Internet of Things (IoT)?**

Score 2; Has something to do with machines getting more connected.

Score 3; Rapidly increasing amount of devices, in particular devices beyond laptops, computers and mobile phones, that get connected to the internet and each other.

Score 4; Enormous amount of data can be collected from sensors and analyzed, usually in a centralized cloud based platform.

Score 5; Machines are getting more capable of connecting, sharing data and making autonomous decisions.

- **Are you familiar with the Industrial Internet of Things (IIoT)?**

Score 2; Making machines in industries connected

Score 3; An extension on IoT but is focused on industrial processes and are mostly private networks.

Score 4; These networks contain and share (sensitive) data among different locations and different machines.

Score 5; IIoT is part of the fourth Industrial Revolution (also referred to as Industry 4.0 or Industrial Internet). This includes higher efficiency, predictive maintenance with autonomous machines like robots and cars.

- **What consequences do you think these developments have to critical infrastructures (power grids, water supply systems etc.)?**

Score 2; They get more connected.

Score 3; Increasing efficiency, financial gains and better choices can be made because of the load of data that can be analyzed.

Score 4; By connecting everything it gets more vulnerable when malicious actors can get in.

Score 5; Machines are developed and produced to be open and communicate with other machines, often at the cost of security.

Cybersecurity

- **Do you have experience or expertise in cybersecurity?**

Score 2; Cybersecurity is about keeping machines and IT networks protected.

Score 3; Simple form is frequently update firewalls and operating software.

Score 4; Often in layers to protect against specific threats.

Score 5; Includes different aspects from correctly developing software to correctly using the software.

- **What do you know about cybersecurity in critical infrastructures?**

Score 2; Organized in a centralized form with a control panel watching the network.

Score 3; Two sides, data protection (cryptography) and Intrusion Detection, with models like Lockheed Martin.

Score 4; Most critical networks are failure proof (power or maintenance issues) but not so much against cyber-attacks.

Score 5; The centralized organization and the lack of focus on cyberattacks makes it vulnerable when attackers manage to get in the network especially on control panel level.

- **What do you know about cybersecurity in Industrial Internet of Things?**

Score 2; Strong firewalls would be used to keep attackers outside.

Score 3; Low computational power sensors, data often send to a centralized point where it can be monitored.

Score 4; These industrial systems usually have old software and it's hard to patch updates.

Score 5; Much communication and connection between the devices makes them more decentralized but also vulnerable because everything is connected in a way.

Blockchain

- **Can you tell what the characteristics are from blockchain technology?**

Score 2; Blockchain is the technology behind Bitcoin.

Score 3; Blockchain is the set of technologies that are combined to create a solution for different use cases.

Score 4; The central component in blockchain is consensus to reach an agreement about a certain value in a distributed network.

Score 5; Blockchain also is a shared ledger where immutability is an important safety mechanism. Often people distinguish between open networks where the nodes in the network are completely unknown, closed networks where the nodes in the network are known and semi-closed where the nodes are known but controlled by different operators.

- **Where do you think blockchain could be useful?**

Score 2; Cryptocurrencies, to take out the bank.

Score 3; The open blockchain principle, first initiated by Bitcoin is useful in taking out the trusted third party.

Score 4; Sharing data peer-to-peer in a distributed network without single owner.

Score 5; Share and store data with the safety mechanisms to ensure the data owner decides who is allowed to see that data.

- **Are you familiar with the consensus algorithm Paxos?**

Score 2; Paxos is a fault tolerant consensus algorithm.

Score 3; Used to reach consensus about a certain value in distributed systems.

Score 4; The first consensus algorithm and many older ones are based on this.

Score 5; Paxos is described by Leslie Lamport in the part-time parliament, the same author as the Byzantine Generals problem. It applies to closed distributed networks where the nodes in the network are known.

Machine Learning

- **Do you know something about machine learning?**

Score 2; This is where people let machines learn

Score 3; Machine learning is the field of research where people try to let machines learn from a large set of data. It will search for patterns and eventually tries to make predictions.

Score 4; Machine learning is based on the idea that computers can learn similar to the way people learn but faster.

Score 5; Machine learning is as a research area that's existing already a long time (since 1950). This can be used to find efficiencies or predict maintenance but also to decide on actions with AI robots without them being told what to do.

- **Where do you think machine learning can be useful in Industrial Internet?**

Score 2; Make better decisions

Score 3; Predictive maintenance and indicate potential efficiencies.

Score 4; The data that's getting gathered in Industrial networks from all different sensors and chips can't effectively be controlled and analyzed by humans

Score 5; Potentially many things can become autonomous, giving authority to machines to make decisions and handle accordingly can be used in many different fields and will need some sort of machine learning.

- **What do you know about machine learning in cybersecurity?**

Score 2; It could analyze cyber-attacks

Score 3; Machine learning can be used to find patterns and anomalies in data that's transferred over a network.

Score 4; Machine learning has different classifications and usually has specific tasks.

Score 5; Machine learning can excess the understanding of humans and is already being used by viruses or cyber criminals. Therefore ML should also be used in cybersecurity to detect anomalies and make decisions itself to take action.

B: Interview transcriptions

Below are the transcriptions of the interviews held for this research by the writer of this thesis. The introduction and every other aspect that could link to a certain interviewee is taken out to ensure anonymity. The interview numbers don't relate to the list of interviewees in chapter 4.1. However, the numbers do relate to all the tables in that chapter.

Interview 1

Date: 01-10-2018

Introduction

..

All right, could you tell me what you know about Internet of Things (IoT)?

Internet of Things, not so much. In fact I never did any study or saw the definition of Internet of Things. I can imagine for example in Industrial Internet you have an individual chip or small computer in every sensor and controller. They will all communicate with each other. For "normal" IoT you think about smart home or something, every of your electrical equipment will also have a chip and they can do a certain time of computation and communication with each other. That's what I know is IoT?

Yes I think you're right and everything like freezers get connected. It's funny that you started with Industrial Internet of Things, because indeed you see now that also the industry sees the advantages of getting things connected. Obviously those machines are already advanced but they now try to connect them so they can work together better.

Yes from our point of view as a researcher what I see from IoT is that when we talk about a computer or big networks, it's not necessarily the internet, it could also be a network of sensors or small computers on some industrial equipment and they can also form a network. That's what we see from Internet of Things, so it's the same problem but a different scenario. In Industrial Internet also the computers and machines get chips to make communication just like normal computers.

I do believe that in Industrial Internet of Things, those machines are more isolated and connected to the secured network that it's in.

Well that I'm not sure if they're better secured because I never did any research on it, but I'm sure there're a lot of security problems because we have a room full of experts who are doing research about it.

Yes essentially this study is also about that problem. Obviously all machines are basically getting more and more connected. What consequences do you think these developments have to critical infrastructures who also get more connected (power grids, water supplies etc.)?

You mean on cybersecurity for the infrastructures if they're move to more connected?

Yes indeed.

Well I speak a lot to my colleagues about this topic. I believe it's getting more and more dangerous. Because during the design of these critical infrastructures they never considered things like the Internet of Things. They didn't consider their equipment will have their own capacity of computation and communication. They are getting more capable devices connected and making it vulnerable to outside sources. I think the problem is mainly on the design principle. Because essentially they were not designed for this purposes. According to my expertise in cybersecurity, these kinds of unexpected things happen and when you need to upgrade will cost many flaws in the system.

Ok, so basically you're saying that these systems are very old and weren't designed to be secured? That's actually also what I found when doing this research, that they are actually designed to be very open because they need to communicate with a lot of different operating systems and software. For example a camera when produced by the fabric, they just make a dumb machine that needs to communicate and be connected with many different software and machines. That makes them perhaps very vulnerable. It's probably hard to upgrade all machines now at this point.

Yes, ok so that's more solid, I have some other ideas but they might not be relevant.
Well go ahead, it's good to talk about it.
Maybe from a different point of view, it's also a problem the scheme you design for a normal network (the internet), the traditional communication protocols are designed to connect between people will also have certain flaws if you use them in industrial purposes, but I'm not sure how that would work. And I might be wrong, because there're already a lot of studies performed on those problems.
So you think, that if they want to create such a network it shouldn't be like the internet?
Yes, well some elements and protocols for example IP addresses were not designed with the IoT scenario in mind. But I'm not sure if that's valid, because there might be better protocols already.
Yes I believe you're right, that a lot of research is done about it, but there's no perfect solution yet.
I believe for example key distribution is still a problem, like Public Key infrastructures are already being used, but to do that in the Industrial Internet of Things is still a valid problem. But it's not my expertise.

No problem, well lets continue about cybersecurity, you have some expertise in your PhD, could you elaborate a little bit more about your experience and expertise in cybersecurity?
All right, so for my PhD I got involved into that a little bit, but I did something called information theoretic security but that's more information security than cybersecurity, so most of the security experts wouldn't say that it's security. It's about the fundamentals of cryptography, so current cryptography they are all based on computational hard problems. So basically we're assuming that the enemy can have some information, but they do not have the sufficient computational power to get or use that information.
But before that, back in the 60's when cryptography enters the modern era, starting with Claude Shannon, he's the founding father of the information theory and modern cryptography. He considered something called information theoretic security where the enemy cannot get any information. So that's when modern cryptography started, but people thought that wouldn't be realistic so people got back to the computational hard problem. But my study was about that information theoretic security.
Ok, so you mean to make sure that the enemy can still not get any information?
Yes, but that is almost too theoretical to be used in practice.
Probably too expensive to create?
Yes, that has some relation to the quantum communication, to exchange keys, so you can reach this level of security. Because then you know that there is only one possible party that can have access to the key, and when you use them to encrypt your information so nobody else can get that. So that was my research, but very theoretical.
Then I started to learn blockchain , because I also had some background knowledge about cryptography. It was a very logical step, but also there was not much information available about blockchain and no better option. So everyone starts with not much knowledge about that subject.
Still it's not a commonly understood thing, and people hardly know that it can do more than cryptocurrencies.
Yes indeed, if you want to have a postdoc on blockchain, in the ideal scenario you would find a PhD on blockchain, but I think there're less than 10 people in the world who really study this topic for a PhD.

All right, we'll get to blockchain in a little while, but first a bit more about cybersecurity in IIoT and critical infrastructures. Do you have some knowledge about cybersecurity in critical infrastructures?
Well I guess there're many risks. But to be honest I learned most from my colleagues who work on cybersecurity, I don't know much about it.
I understand, you didn't do research about it.
Correct, according to them, they focus on the network layer. So how to actually hack into the system and cause some problems. Another problem is that you can mess up with the sensors. So it gives false alarms, that causes the system to do abnormal behavior that will harm the system. For example it will tell the network that the temperature is low, even if the temperature is not low. So the controller will heat up and might overheat. To cause that attacks you can just mess up with the sensor or plug something in the network. I guess my colleagues work on the network layer to prevent people from getting in, and others will collect the data and

learn a pattern from the data. When they find a pattern and detect abnormal behavior they can blacklist certain addresses etc.

Ok well, we'll continue now to the blockchain, can you tell me in your own words what the characteristics are from blockchain technology?
Blockchain is the technology that you can use to decentralize something, so you can move the functionalities that are traditionally considered to be only carried out by a centralized party. But now blockchain can distribute this to multiple parties.
Ok, and what are the most important parts or elements of blockchain?
Well consensus algorithms I would say is the key part and well I think depends on the application and area I think incentive mechanism is an issue but that is already in the consensus algorithm. Essentially meaning that it's a financial transaction included. Some of the consensus algorithms only function if those incentives are designed correctly.
But do you mean there're also blockchains without the incentive?
Well we can say like the product of IBM, Hyper Ledger Fabric, it's a blockchain without incentives. In my point of view it's just a matter of taste. But for example in a consortium blockchain or private blockchain, if the involved parties are naturally incited to not act malicious because they will be punished in other ways. They're all part of the same organization or group, they wouldn't want to harm the system. They want to achieve something together, and individuals wouldn't act malicious because they would be punished via other ways. Then it doesn't make much sense to add incentives in the blockchain.
According to me I would say, the real critical component is consensus algorithm and besides that its mostly applicational, sometimes like smart contracts. For example in logistics and IoT you need critical components that are the link between the physical world and the blockchain, like reliable sensors or another reliable source of data.
I understand, well and you know a lot about the use cases of the blockchain and also the consensus algorithms. The one I studied most was the Paxos consensus algorithm. Are you familiar with the consensus algorithm Paxos?
Yes, I know Paxos. It's not something usually considered for blockchain, because it's a normal fault tolerant algorithm. And for blockchain, you always use the Byzantine Fault Tolerant algorithm. Which actually means you also tolerate malicious behaviors, so you intentionally cause inconsistency in the network. So for example for blockchain we use Asynchronous Byzantine Fault Tolerance so the nodes can do whatever they want. They can send different messages to different parties, they can delay the messages arbitrarily and sometimes we consider that they are more powerful and can cause problems in the network like blocking other people's traffic. That is the scenario for blockchain, but Paxos is the normal fault tolerant so it only consider the nodes can go offline. The major thing it doesn't consider is that the nodes intentionally can cause inconsistencies and send different messages to different parties. In most of the scenarios of blockchain, that would cause problems.
Ok, I understand, so which consensus algorithm do you think would be different than Paxos and used now?
Well I think it's mostly the Byzantine Fault Tolerant version of Paxos, which is called PBFT, Practical Byzantine Fault Tolerant.
So Practical Byzantine Fault Tolerant, is essentially based on Paxos, right?
Well, it adds another round of communication than Paxos. So that everyone can make sure that they have reached consensus. To explain that a little bit more, Paxos has other of N communication cost and PBFT has other of N^2 communication cost. So no it's not directly related to Paxos, but it borrows some concepts from Paxos and turned it into PBFT. But Paxos is described by Leslie Lamport, and the Byzantine Fault Tolerant problem is also described by Leslie Lamport. And PBFT comes later, in 1995 designed by Miguel Castro and Barbara Liskov (also Turing award winner) so they borrow ideas from Paxos but it's not a simple extension. It took around 10 years for people to build this version, from the date PBFT was proposed. PBFT is before Blockchain the only Byzantine Fault Tolerant algorithm considered by People, but it's not scalable, because it has N^2 communication cost, and computation cost.
So actually it's not practical?

Well it's very practical if you consider N nodes (small network), basically people do not consider cryptocurrency and huge network is a scenarios for PBFT. That's why people think PBFT is already practical enough, if you consider a database and you only have around 10 servers. In that point of view, PBFT is quite efficient. And then we have the Bitcoin, who solved BFT problems in another angle, by bringing in the incentives. Especially recent years people tried to extend BFT algorithms, but the idea is that you first consider a normal situation where the malicious node will have less capacity or do not do so much malicious behavior. So you basically will have an optimal scenario with a much less expensive solution to reach consensus. But there is the exit condition, if they detect something is wrong in the network, they'll change to a more expensive way to reach consensus algorithm like PBFT.

Ok, so I can imagine you have a certain network with known nodes, and if all goes correctly you work with a basic "easy" consensus algorithm, but if they detect anomalies, you kick that node out and step up the security level?

Yes, indeed. And in my point of view, if you look at it very closely it is not so much different from the consensus algorithm used by Bitcoin. With the blockchain consensus algorithm, it's basically the best case scenario, but they can assume this best case scenario because they have the incentives, they know the nodes will not behave maliciously. If you turn to BFT, if you also say we form a consortium blockchain and we believe people will not behave malicious, then you can use the less expensive version of consensus algorithms.

Ok so can I say that PBFT is more for the open blockchains and normal consensus algorithms more for the private and consortium algorithms?

Well these two blockchains are both the same in speed and latency etc., the only problem is that BFT still requires that you know the number of nodes and keys in the network in advance. So that's more suitable for permissioned blockchains.

I can imagine indeed, then you don't need the more expensive consensus algorithms, you can basically rely that the nodes will stay honest?

Yes so let me give you an example, do you know Hyper Ledger Fabric?

Yes, from IBM.

Yes, so they have the earlier version 0.6 were they use PBFT for consensus algorithms. Also Corda, Tendermint and NEO use PBFT for the consensus algorithm. So currently there're still some blockchains that use PBFT. So people are slowly realizing that PBFT has the limitation of throughput. So it's limited to 10 nodes, and then it’s still slightly worse. So they start changing to a slightly different approach, they have the assumption that the first communication round is the easy and cheap one, then secondly they use a more secured but more expensive consensus algorithm for the abnormal values.

So you basically use two versions of consensus algorithms?

Yes, there're many blockchains now who use that philosophy. But Hyper Ledger Fabric takes a different approach. So they completely separate the validation of the value from the consensus. So they have the strange endorsement mechanism (in the new 1.0 version). First you validate the data before it goes into the blockchain.

Yeah, I heard about it, I think they called it external validation. Because you validate the values before it goes through the blockchain.

Yes, and then it's different from the traditional blockchain, because it doesn't need to be validated by every node and they reach consensus. They have a private channel for the value validation, so a certain defined number of nodes validate the values and then got published to the others.

Because then actually the malicious nodes cannot do much, because they cannot change the data. In that case it makes perfect sense not to use the expensive Byzantine Fault Tolerant version of the consensus algorithm. So Hyper Ledger Fabric is using something similar to Paxos for consensus (normal Fault Tolerant).

Very good to hear that you know a lot about this algorithms. When I studied Paxos they have the requirement that they know everything in the network and secondly they don't do the validation of the input. They assume that they know everyone in the network, and they act honest so the information that goes in will be honest as well. If you can assume that you can guarantee everyone in the network stays honest without the incentive, just because you know them and they don't get attacked. Then you can

assume that all the information will get passed on correctly. Then you will have the Paxos blockchain, but it's still better secured than current situation in critical infrastructures.
So, are you suggesting that for the industrial scenarios you could use Paxos?
Yes, I can imagine that if you know everyone in the network, like in Industrial Internet, you don't need the validation of the values. If you can assume that all the nodes stay honest, it should be secured. The only thing then you need to know is when someone gets attacked or compromised.
Well that could be, I think there's a lot studied around this subject, but not much Paxos for this purpose. So first of all I think because in the BFT area before blockchain people do not consider how to distinct two different type of attacks, the one is on purpose and the one accidentally. So how to detect those attacks is not considered by the researchers before in blockchain. So I think that could be an interesting study.
Sometimes we do not need to protect the network to all attacks, because most of the time they are honest nodes who just did something wrong unintentionally. If you could distinguish that in the blockchain, you'll already have a valuable solution for industrial purposes. But I'm not sure if that's even possible. So the main problem is if you use Paxos for industrial use, it will end up with inconsistencies because it will think things are wrong even if they are correct.
So the problem of Paxos is that you need to consider how secured you need it and how many nodes will be included. If it's small like 4 nodes, then you can use Paxos, because it's not very likely that they are compromised. And you can see from the logs who are actually being compromised or if that someone just fails (offline, or makes mistakes). But if you go to lower layers for example a blockchain that contains all the sensors, if you just use Paxos, misbehavior will give a lot of false alarms.
Let me show you the visual version of what we're talking about. This is an example of 4 nodes, like you just said. It will be a private blockchain, maybe 1 company or more companies combined. These are for now the more advanced machines, not the sensors yet. I assume that Paxos could be enough if you can guarantee that it's private and no malicious node could come in the network, and they reach consensus over who can get into the network (via join request). What do you think about this scenario?
Well if you use Paxos, it means that if these nodes have different opinions, it will still reach consensus. The problem is, that they won't figure out who will be wrong.
I guess you're talking about the (trans)actions in the network, if for example node A wants to do something, it'll ask it to the others. There's indeed no validation on that value to make sure it's correct. However what I want to find out is that they can determine the value can be trusted. The others in the network can maybe detect anomalies in the nodes or the value or the nodes in the network.
Oke, well how is that different in for example the auto-pilot system for an airplane? You'll also have spare parts and if one goes wrong (fail), the others will still give you the correct information. They reach consensus to make sure the correct value will still be given.
I can imagine that indeed this will be done via consensus (when someone goes offline). But then I can image that malicious people can still enter that network because the nodes in the network don't really know what's correct.
No we assume nobody can enter the network and nobody can mess up with the network. It can for example give a false read, but the others will give the correct value, so they will reach consensus and still give the correct value. But maybe I don't really understand your picture, are these all sensors?
Well that would be more the advanced machines for now. If one of them goes offline and comes back, it will have to ask permission to get back in the network again via consensus. They can determine this on the public key or IPV6 or whatever way is suitable (that's not part of this research). Individually they'll have their own security measures like now, and you can update them etc.
But when they're in the network, they will become better secured. Because we can use blockchain technology to let them communicate and create a shared ledger.
Yes, sure that's possible.
Well then the next step is that the values in the network won't always be possible to validate (else you'll have a lot of false alarms), but they might be able to validate in different ways, because they can see if the transaction is consistent with previous transactions, or not that much different, or won't cause problems with other actions.

But then when you mean validation, it still will be validated by each one of them, then they'll use Paxos to reach consensus, the only problem you need to consider then is that some of the nodes will be compromised to send different information to different parties. If that could happen than Paxos won't work.
Ok, because you mean in general, Paxos is not Byzantine Fault Tolerant. Ok, well am I right that if you know everyone in the network, the only attack that could happen is that one node would be compromised.
Yes, that's correct.
Ok, I'll note that down and have a look into the inside attack, but I can imagine in this situation it would be already much better secured than currently.
Yes, I think so too.
Well let's continue on this scenario. Essentially if such a network would be created, you can say from every transaction that they are verified in whatever possible way. Then the next question is, could the nodes learn from the actions in the network that something is wrong?
Ok, so if you use Paxos then the only benefit will be that you tolerant the failure of one machine, because the others will have copies. And then the whole system will be similar to just one machine. You can also use machine learning approach to detect anomalies, but it'll be the same as you do on the information of just one machine like it is now. But now I guess those infrastructures will already have some spare data (normal Fault Tolerant).
Yes, indeed they should use backups etc. and most likely not a distributed database or shared ledger. But I can imagine that they haven't considered this scenario from a security perspective. Obviously if one fails, the network will still work, but at the moment we know that if the attack occurs on just a small part in the network, then the whole network will be compromised.
Yes, that's true. For the critical infrastructures, they don't use these kind of systems. They use the detect based spare systems. When they detect, something fails, they will go back to a backup, not actually use distributed scenarios like this.
Well it seems a good solution, and it will certainly help I would say. In my point of view, it's really weather it's a ledger or chained by hash functions, but those innovations are not made by blockchain in my opinion. Using hash to guarantee integrity is already an old technique, and in distributed databases they're already using that.
Ok, but the distributed databases don't use the shared ledger principle yet am I right?
No but the distributed database will be consistent.
But for example if you would change the data on one of the nodes, the others in the network won't notice that?
Well they do not consider malicious behavior.

Ok, thank you very much. Well the last part I want to discuss is;
If you imagine such a network and they reach consensus about the values, and they can also detect anomalies, and in such way create the Byzantine Fault Tolerance. How far can those nodes learn and create better secured environments? Because obviously they all learn the same things, from the whole information they can all see what would be abnormal. What do you think about that? Would you think would that be better secured?
Well in my point of view, that will certainly help. But if you just use Paxos for normal fault tolerant is not really new. It's kind of the same as distributed databases where you also consider single point of failure. I would say if they really do it based on this detection whether it would fail or not etc. it would be better secured at extra cost though. The thing is, is it really a new idea.
Yes, I understand. Well when I did research about it, I couldn't find any papers or something where they describe such a scenario that's focused on the security part of it. I think the essential benefit compared to a distributed system would be that all the nodes in the network could work on keeping the network safe with (machine learning) algorithms. In a regular distributed network that won't be possible because cybersecurity is essentially centralized (including the machine learning algorithms). So if you need to analyze the data at one certain point and arrange your cybersecurity from one single point, then you will still create a single point of failure.
Ok, well let's say it this way, if you use machine learning on all the data and try to detect malicious behavior. Traditionally if malicious behavior would be detected, you need to react to the alarm and check them. In your

proposed network, the malicious node will instantly get kicked out and need to ask to rejoin again? Also if your machine learning (cybersecurity) node is getting attacked, the others will still notice that and take actions?
Yes indeed, the network will want to kick out the malicious influence. In the traditional network the people still need to go through the alarms that the system detects, but the new network should kick it out and then further make sure the network will still keep running.
I need to think about it as well, to me it definitely seems interesting and I need to do a bit more research into it. I'm also not sure how you can implement the machine learning into the network, because it's a different layer right now.
So what kind of things for example can go wrong here in the network?
You run machine learning on the data, but it won't be much different than the system defense maybe?
Well let's first ask the question, would this proposed network essentially be better secured already even without machine learning. Because they can learn from al the actions in the network from each other. Then if that's possible it's likely that machine learning can be added. In that case I'm not sure if the nodes would learn the same or that would probably even vary?
Well I'm also not sure, but I assume that it should learn the same. Although it depends on the algorithms I guess.
Well it should be the same outcome I guess. Else 1 node will think it is malicious and the others don't. Well anyway, how much we can learn to protect it will not be the question for this research. Essentially the question still remains now is: can we learn on the actions that the nodes do, witnessed by the others? I can imagine that would already be better secured than the current situation?
Ok, I'm not completely sure, especially not if it's fundamentally different. But I'm sure that if the attacker could do malicious actions in the node that runs the security protocols and machine learning algorithms, it might cause the security layer to fail. With your proposal that would be better secured. But if the nodes for example all learn slightly differently and they would make a different decision it would be better secured. For example if all nodes need to verify if an action is allowed but they all have created slightly different criteria I can imagine over time that could be a much better secured protocol. Then you need to consider if it's possible to run different machine learning algorithms on different nodes.
Yes that's a good point, and to make sure the network decides whether or not something is allowed, with their own arguments. It should be that not people can just change things or force machines or actions into the network. Essentially you want to make sure that the network can handle that without humans.
For example if 1 machine wants to rise the temperature, the others cannot validate if that would be a correct thing to do. But at least they can detect if this node behaves normal, if it would be likely to be a good thing to do and that it wouldn't be conflicting with other actions in the network. That means that the action or value can still be new but wouldn't be too much out of bounce, so it avoids giving false alarms.
Yes, ok I can imagine that in current critical infrastructures they're all using different approaches and definitely not all will be enough secured. So with the example you just give, if the request to raise temperature comes in, and they all will use the same way to validate that action, it will be the same as one would validate that action. But if they kind of use their own ways and criteria, then it definitely would makes sense. But it's hard to organize this, but very interesting. It actually gives me some interesting ideas, especially why you use Paxos over PBFT makes a lot of sense here, and is never considered before I think.
Yes indeed, and I can imagine that's because Paxos doesn't include any validation and in a lot of networks, people assume that you do need the validation to become secured. But in this scenario, you kind of still do the validation, but not on the traditional way. The thing I still consider is what can a network see when it gets attacked. How would that be in the current scenario and what would be the benefit of having this proposed structure?
I got your point, well I'm not completely sure how that would be organized at the moment. The way I would look at it, is to see what the attacker is allowed to do. Could it send different messages to different nodes to create inconsistency. So for example it could completely enter one node, and what could it then do.
Well and what if all messages are signed?
Yes, but when a node is compromised, you can send different signed messages to different nodes. In that case it would break the whole consensus. You will need some version of Byzantine Fault Tolerant, if that's possible than this scenario can definitely work.

Ok, thank you very much for all your input. I'll have another look at the Byzantine Fault Tolerancy but also PBFT and the example you gave about the auto pilot btw, and how much it will differ from current scenarios.
Yes that would be good, if your scenario is Byzantine Fault Tolerant it definitely would be better secured, because nobody considered Byzantine Fault Tolerant in traditional systems. But if it's normal fault tolerant I think it's very similar to what's already operating. So when you consider that one node could be compromised and would be detected or at least the rest of the network would operate correctly, then it would make perfect sense in my opinion. And to keep in mind, BFT is not actually designed for decentralization, for the Bitcoin type of scenario. Lamport works for NASA projects and he was worried about Russian spies to compromise their systems, so that's how he came up with Byzantine Fault Tolerance.
BFT actually never got popular, one of the reasons is that they couldn't find a good scenario for that. It only got popular with the Bitcoin. But you could say for these critical infrastructures, you also need BFT it would make sense. Because this is a new problem, because of the Internet of Things indeed.
That's good to know, then I think for now I got all the information I need. Is there anything you would like to add?
Thank you too, I enjoyed the conversation, it makes me think a bit different as well.
Thank you very much again for your time. If you don't mind I'll contact you with some further questions if I get them in a later stage?
Sure, no problem!

Interview 2

Date: 12-10-2018

Introduction
..
Ok, thank you, I think that gives a good profile. Could you tell me in your own words what you think about the Internet of Things(IoT)?
Sure, well the IoT, how I look at it, it's the scaling of and miniaturization of devices, such that we can get more value from them. So rather than it's in industrial device, we start now seeing more connected sensors. Connecting everything in fact to gather data for the purpose of getting more insight in their best usage and good deployment. So I would call it more data collection of even the smallest devices all connected.
Mostly in the case of sensors, but also for predictive maintenance of sophisticated devices as well.
Yes indeed, well also because I can imagine with your background, that you also see many projects where a lot of small devices get connected.
Indeed, we have projects that work around predictive and preventative maintenance, for example CT scanners and MRI scanners. In there you try to prevent breakdown but also improve the operation of the machines and the efficiency of the technical workers.
Ok, and are you familiar with the Industrial Internet of Things?
I am yes, there's also the term Internet of Medical things. And of course you're probably thinking of some of the blockchain providers who enter this area?
Yes, so you mean that it's just the bigger version of IoT and in different areas?
Well essentially yes, but I think one of the challenges for a large company is that you have a lot of legacy and often an awful lot of devices were created without the side where predictive maintenance can be used on them. Now it gets complicated to work those predictive maintenance into those type of systems. For example hospitals etc. seem to have these challenges. If you're talking about more modern devices you'll get the benefits of improved software design with of course the data collection is already a major part of those devices.
I understand, and it's very expensive to update all those systems now and people are trying to make their way around it. You still want to have the benefit of the possibilities but that comes with a price. One of the things though I see from the Industrial Internet of Things is that they're usually talking about the connected

closed network where IoT is more open I think. So as you mentioned there's a trend going on were everything gets more and more connected. In IoT the devices are created to be open, they need to be able to communicate with many different software or operating systems. In IIoT you see that all the sensors also need to get connected but they still seem to have that openness elements that they want to communicate rather than being secure. Have you seen any of the consequences that those large networks are also getting more and more connected?

Well, I think interestingly enough, for example electricity networks, they're pretty well connected. What I mean is there've been systems like SCADA, that are there for many years and deal with reasonably modern networks. They manage power outages very accurately. Before that they had older networks you normally had major components to the data network and problems would seem to go downstream. But with SCADA widely being deployed, they seem to be able to manage downtime and outages very accurately.

So you can imagine way before IoT was coined, we've been doing this already. I think when we're talking about the Internet of Industrial Things, it's just another step of extra scaling up of connectivity. So it might even be the surrounding of such devices with extra sensors to do environmental readings and combine that data with other data.

To give you a concrete example, let's say you have a network component in an electricity network that failed. You might surround in with sensors, to determine the environmental condition at the time of failure, to see if you can correlate certain conditions with the failure. So you're augmenting systems with this extra sensor level in order to predict maintenance.

Ok, and this is already from back in the days when they focused on breaking down of devices. But I guess this was not on the "cyberattack" level?

Indeed, so the preventative side of breakdowns. I know from previous companies that they spend a lot of time trying to do prevention, because if you try to react to every event you need a much larger team and will be more expensive. One of the things that also is connected to IoT are the drones. A company I worked for actually used drones that made pictures of the environment of the electricity lines, for example trees that would overgrown. So they would effectively plan when to cut the tree and this would be much cheaper than fixing the problem afterwards.

Yes, of course, you cannot see that from the data in the network itself. Like you said, then you need an extra layer of environmental conditions.

Indeed, you can imagine even with water networks. The problem there is that there's generally not an electricity line along them, for good reasons. So how do you use IoT around there with much less access to electricity. It's a significant investment to add all the extra sensors and devices to gain better insight.

Yes, I can imagine and it's also harder to estimate what would be the cost or benefit what it would be to not do anything. Especially when governments need to pay for these projects and need to prove that it's well worth spend money.

Indeed, I suspect that you need other reasons to justify these spending. Round environmental concerns, what kind of damage would it do if something breaks and do you really need to prevent it.

Indeed, well also I think we see an increasing amount of cyberattacks on those infrastructures. I believe that most of these networks are not designed to protect against this attacks. They are mostly developed to protect against failures and breakdowns.

Yes you're right. I can give you some insight though on what is actually happening there. For example many hospitals are their own worst enemy. They don't do or have very basic measures to keep their systems secure. When the devices are sold to them, they often in the past didn't want to pay for all the security features. Now they kind of are paying for that. They internally didn't have the knowledge or the budget, again they also don't have the arguments to justify the expense. You see a many times that they still run Windows 95 machines on the same network as their medical devices are connected to. This is obviously highly insecure operating systems connected to highly insecure operating systems on the medical devices, this gives significant risks. But if you're trying to fix those problems now, it's very hard, because you have to stay operational. So now there're a lot of questions how you would update those devices or how would you replace those devices with new security features. There're also hospitals that deploy the right staff and leadership (like Chief Information Security Officers CISO) that try to prevent this lacks from happening in the first place. They do already monitor attacks, try to prevent and educate all the other staff members to increase security.

Yes, I can imagine indeed that if they would already start with updating Windows, it would already be much better secured in most cases.
Yes exactly, so moving to blockchain is probably a bit too far away in most cases. They don't have that degree of connectivity etc.
Exactly, so just to jump to another subject. Like you already said before, your experience in cybersecurity was already included in the last 22 years.
Yes, correct. Security always has been not the main focus but it was always part of our process when developing software. But often you always need to bring in the security architects to take a look over the approach that's been taken to ensure that security is maintained. Of course a lot of frameworks already try to include a lot of security measures. But then you have to be mindful what you really want to open and include.
Ok, so it's not customized when you're programming.
Indeed, but it helps to some degree. Because sometimes when you're designing software, the security issues are not top of your mind. This makes sure at least some measures are automatically taken or prompted to make sure the developers do think about it.
Allright, but basically you think most security measures are there but just not always used properly where they're needed?
Indeed, it's a common practical issue day to day in software development.

Ok, well let's get further to the subject of blockchain. As already said before, the last few years you did a lot of research on blockchain. Could you tell me shortly in your own words how you see a blockchain and what the characteristics are?
Sure, well my first statement is, that a blockchain on its own does very little. I view it in a similar way as you view a service or kind of database where you build your applications on top. Obviously underneath there're a couple of interesting things going on there, like effectively a blockchain is a log that's shared among many different parties. What can be built on top of that is very interesting of course in terms of applications but also the implications. When we talk about properties of the blockchain, I think the immutability is important of the technology, integrity of the storage. So architecturally I would separate the blockchain part from its data sharing part. If you look at Etherium it tends to not really do that, it tends to say that the ledger is the blockchain. But I think much more successful would be, similar to Hyperledger and some others, is that the ledger itself is average and not useful. Generally you can use any sort of data sharing mechanism, but what is really important, and this is not made possible by blockchain, is the need for a way to make claims in an immutable system that other parties can check for the integrity. The consequence is that you can for example, when data is exchanged, the other party can be guaranteed about the integrity of the data. It's also timestamps, so you can prove that certain data have existed at a certain time. You can say that this is actually not new, we've had this for many years within companies that already had agreements to share data. But recently we start seeing more need to share data between companies where they don't have such agreements, like hospitals. When they have customer data that needs to be shared with other hospitals outside their own group. You then need consent, and somewhere to store that consent. Today what happens is, the consent is given in the original hospital, then the receiving hospital will call the source hospital and ask if the patient consents to share the data, but there's no clear record of that transaction. So the idea is that you want to scale up this and want to manage compliance and all the regulation that are in place to protect peoples data. To make this cost effective, we're going to need a better way to do this. So I see the key value of blockchain in the healthcare for example, is something that could underpin patient health care data. So in other words, I'm in one location and I can move the records to my mobile phone. There's a blockchain with all the data that guarantees the integrity of the data. When I turn up at another health care provider, it's nice that you have a list of data that you're showing on your phone, but how do I prove that you didn't modify the record, and how do I know where it came from. So this trusted chain is a place where you can go to check the origin of the data and integrity of the data. So in some ways for large networks blockchain can become interesting. Because it creates a system of interaction where people can verify the source of data.
So pretty much everything where data need to be stored and shared, you can do that on the blockchain because you know it can be trusted. But in such a scenario, do you suggest you still need to store the data centralized somewhere?

Yes, could be. But I think there're various ways to do that. An interesting scenario for example is something called linked data. In such a case you submit the hash of the data, rather than the full data being stored in the blockchain. But with the hash data you still get a receipt of the integrity of the data and also a meta data description so you can read the data. So then anyone else can still be guaranteed about the source and integrity of the data. This removes some of the direct connections that are needed, so you don't have to know the person you're connecting to, and both parties will be under control what data will be shared.

Ok, so I can imagine that in such a case you could store data centralized as long as the central party cannot see the data what's stored. But you could also make sure the data is stored where the owner wants the data.

Exactly, but you can also use encryption right, but then the problem is how do you manage the encryption keys. There're so many opinions and ways to do it. Each approach has advantages and disadvantages. For example, if you are the person who generates the keys and stores them on your phone, then you can sign and encrypt the data without anyone else being able to do that, and it can be guaranteed that the action comes from you. But you can also delegate that to hyper security model within an enterprise, that's also strong, but you might say that it's weaker because the keys are created and shared via a central place, so you don't really guarantee optimal security etc.

Encryption technology is also very hard to use for people who don't really understand the technology.

Ok, and essentially it's still very hard that you create a system that anyone can trust but still is owned by a single party.

Indeed, well it doesn't even exist actually.

Exactly, the different elements might be there, but still it's always owned by a company and they can run away with everything or have other ways to manipulate the system.

Exactly, so this is one of the things where the blockchain was supposed to help, because you can store your data completely decentralized. There's a degree of truth on that, but then you need another layer of infrastructure that needs to build them. For example a peer to peer file share system build by the company called FileCoin. It's nothing new, it’s similar to for example Napster that did similar things for specific kind of files.

You mean the media and sound track files.

Indeed, and they are much more mature, so people have basically stored data decentralized for years already. But it tends to be more secured and data copyright will be better guaranteed. They said that it's because of security reasons, because you indeed reduce the possibility from getting taken if it's stored on different locations.

Well, you mainly prevent it from getting lost I guess? Because if you store data on multiple places it only increases the risk of attacks?

You do, but if you have it encrypted, then at least whatever is stolen it's not easily interpretable and understandable.

So it's combining these techniques that at some level can already help. But you're right, you have to take a risk based approach on what's best. Introducing distribution adds cost and other risk as you said. But centralization has their own cost and risk as well.

Like mainly the single point of failure is a very crucial aspect I think, in most cases you simply need it distributed because you can't take the risk of having single point of failure?

Indeed, and to be honest, cloud systems kind of already offer this solution by storing data in multiple regions. If you take a look at amazon where they have object storage called S3, you don't even think about regions, it gets automatically managed. You still have the option to encrypt the data. But at some level you must trust amazon because their business model is that they do a lot of work on the security and protect your data. But you can take extra measures yourself like encrypt data at rest. If you're processing data that is unencrypted you will still have a risk because somebody could probe a processor. But there're again a lot of solutions in the making, but everything will be just another plaster on top of each other. Usually when you work like that with plaster for different risks, there's always some gap in between. You have to see the gap to close it, and often we rely on someone to find it like hackers, or we need to hire expert teams to find them.

But at the same time, if your company needs to worry about all of these concerns, than you need to ask yourself the question, is your data worth that much?

Exactly, they can think about what would happen if they get breached. As long as your data is not lost but only stolen, you can ask how much damage that would be.
Well you could argue that if your data is worth that much, maybe you should build a big bunker in an isolated mountain somewhere.
Well I can imagine for critical data and large companies that are still working in different approaches because they still need to ensure privacy and security.
Well totally true, we're very good in cleaning up the messes that come from earlier decisions. It's simply the state of maturity really, I think now we're getting much better quickly but the concerns a few years ago were completely different. So you still have many old systems and that is probably the biggest issue nowadays.
The second thing is that we probably don't really have a good language to explain the problem from the ones who gather requirements, design it and it's ways to avoid problems, all the way to the ones who develop the system.
That problem has been overcome in other areas like electronics and the building industry. Clear standards for engineering approaches will already create more stability and safety.
Many times software developers say this is different and more abstract, well I don't think it's different we just didn't found the best way to explain things and communicate the ideas. You notice that in the building world there's a clear delineation between engineer and architect but you usually don't get buildings being build upside down. That's more likely to happen in IT. Even tools and materials are very different in programming. Often the developers use their own tools and standards and make choices because they have an own preference but not for any good reason.

Allright, ok to continue a little bit on the blockchain. One part of the blockchain is the consensus algorithm, are you familiar with the Paxos algorithm?
Yes, I'm indeed. That algorithm has been around quite a while now. That's very different from the proof of work or proof of stake consensus. It's mostly used for private blockchains where the parties are known.
Exactly, I think you can somehow compare Paxos with shared ledger technology where you can make sure different physical locations always store the same data.
Indeed, and also there's a concept of Byzantine Fault Tolerant, so if one node gets untrustworthy, then the others will still come to consensus. But it's not thinking about consensus in massive skills where you might have a lot of untrusted parties. This is where the incentives like proof of work and penalty system comes in.
Yes indeed, the incentives are not that and probably also not as much the validation of the values. Like in the Bitcoin everyone can validate the values, but with Paxos you can't.
Indeed, something similar would be used by Hyperledger. But there's also a part of Hyperledger that is really just a message queue for ordering transactions, because you can trust everyone in the network. It's really about storing distributed facts and storing data, so it's a much more enterprising view.

Ok, and as last something about machine learning. Already this is being used in cybersecurity. How far is your knowledge in machine learning?
Well, in here, we don't use ML in cybersecurity, but I acknowledge completely that it's valuable there. We mostly use ML for medical diagnostics. I do believe that it helps to discover patterns in behavior. This has already being used for a while for example in preventing e-mail phishing and junk e-mail. Over time these algorithms behind for example Hotmail got smarter over time in distinguishing junk email and genuine email. At some level they relied on users to classify junk mail correctly, but for the system as a whole this turned out to be very helpful, because it learns how junk email looks like. From my experience now you automatically get a lot less junk email than a few years ago.
Have you heard of complex processing?
Yes, that's also one of the machine learning approaches right?
Indeed, it's really about a system where you have a lot of events going on and you try to determine behavior. So you have certain nodes of operations that have been identified in the past as malicious, then you could use machine learning to quarantine that user in your system. I think that could be a good way to deal with cybersecurity, I think way more likely to be successful than blockchain. Because that's basically already what were been doing.

Exactly, I agree that recently more and more people realize that it's a hype and the essentials are useful to some extend but not a single solution. For this research I also focused on just the consensus part of the blockchain and not on the other aspects like hashes and encryption and proof of work.

Indeed, so as I know from the last couple of years that people are well aware of security technology and are making good improvements in that. But if you're not well aware of security technology, then blockchain becomes somewhat the buy word for security technology. So people say all the amazing things that we can do, but the reality is that people don't realize that we can do these things already for many years. And then you see experts saying that it really is nothing new, but I guess the answer is in the middle.

It's not completely old or new or a single solution for everything, but if you look closely, then you will see that there're a lot of opportunities there. I think that you're right that when you need a broader network were you can't specify who will connect with whom, then you need some system to guarantee that the owner of the data makes the decisions who gets the data and who don't in an open way. That's the key difference and change with blockchain I think. What it will prompt is data sharing between different sectors because people start to believe into the technology what we already had before.

If we can create a system where anyone can verify the source of the data and guarantee that you're still in charge of your own data, this might open up the silos of companies and industries now. This data sharing aspect will become valuable I guess.

Yes, and with standardized ways in storing and sharing you already create a better secured environment.

Yes, it could be just another piece above of the current TCP/IP (the normal protocol currently). Somewhere in this communication stack or protocol a form of blockchain could work and be valuable that automatically checks and verify data. Then you only know that it's there when something is wrong. When you can bring it to that level, the use will be wide spread but at the same time more important how we standardize our design and development of systems.

At the same time stay safe and secured, but there's a lot of work to do still.

Yes, if you're interested you should check the company called Guardtime. Because they're actually doing this on industrial scale. They are an Estonian company and have worked on this for a while. They have created the security hardware to do the consensus and provide a distributed time stamp creation system with signatures and hashes. You could get a node from them and then the system simply can guarantee and verify the data source.

It's called a blockchain, but in reality it's called a data integrity engine. They have no ledger, however they have been doing some creations with ledgers like Corda on top.

Thank you, I'm definitely going to look into that company.

Well just a few more questions about a scenario of an industrial process or a company like the hospital. If you have for example 4 nodes that would function as the center of the network. It's a secured closed network and Paxos would run just to make sure the data is stored in those different locations and be consistent. If then the nodes can learn what is happening in the network and let them learn what is supposed to happen, then you can already make it better secured?

To start a set of rules can be determined about the actions that can be done, but most actions simply can't be verified. But if the nodes learn who's in the network and if they behave similar, could you already make it better secured? Is that happening already?

No, I believe that wouldn't happen today. There're some companies that claim they can do something like that. I think they can at a certain level, but probably not as good as we think they can. Because the systems require a lot of training and time to collect enough data to know what you're protecting and what behavior you're protection yourself against. You might be able to identify some of the behavior, but hackers are very clever. So they will come up with something similar to normal behavior and that wouldn't be detected.

So what you want is something that monitors effectively the vital signs of your systems and that can detect as a deeper level, similar actions as we know to be malicious. I believe this would start to make it a lot harder for hackers.

Imagine you got a system that is corruptible, so what stops a hacker from corrupting the AI system that's overseeing your system? So either that has to be independent in some way, but then the problem is that they could cut connectivity.

I'm not sure, I get your point, but I guess that's also the problem from machine learning in general because it's centralized, from the cybersecurity department experts.
Exactly, what if that system gets corrupted, if the hacker can get in there, than they can do everything they want. But this is somewhere where I see the integrity engine being useful, because you could imagine that we know that you can monitor the systems that are running and hash the current state of their system, that whenever some hacker can modify some code to their advantage on a node, than that hash would be different and immediately identified. In this way you can guarantee that your monitoring system isn't compromised. Right now this wouldn't happen.
I believe indeed that you somehow need to look at such a scenario.
Indeed like you said what if the node responsible for the security of the network would be compromised, you have a big issue. But what if all the nodes in the network are connected and they have a consensus algorithm running that handle the data. Is it possible that those nodes can also detect each others state and reach consensus about the fact that someone is compromised and isolate that node?
I think that might be ideal indeed. What you're saying is that you have 4 nodes with different administrators, and one is compromised that the others can rule him out. In some way that's Byzantine Fault Tolerance.
Exactly
So the other nodes would come to a consensus and quarantine the malicious node.
So that's indeed a form of security, could someone attack all four nodes, I guess they could because it's just 4 nodes. The strength of the public blockchain is that there're thousands of nodes, and therefore impossible to attack that.
Sure, I understand, but on the other hand, it's hard to determine that now. Because 4 might indeed be not as safe, could we make it 10 nodes, I guess we could and would that be already much harder to attack. I guess the higher safety you want, the more it will cost. But if we keep in mind a critical infrastructure like a water supply system or electricity grid, this would already make it much better secured because at the moment they only have the normal fault tolerant system.
When the network can verify each other in the network, than you have to attack all nodes at exactly the same time, because it's a closed network.
Indeed, I think what you're saying is also about insider threats. And the AI approach assuming that you are secured and your AI system is not tampered with, that you can overlook your system indeed. In that case it wouldn't just apply to hackers, but also inside attacks. If you're able to train such a security data model to detect such behavior it indeed should be effective.
Ok, so you're still talking about a centralized ML of cybersecurity model or node in the network?
Yes, I mean you probably could distribute that as well, but that would come with cost. Distributing is one way, but you could also use the tamper proof hardware, this makes it a lot harder to tamper with the software that's running inside it. So over the years we will find the best solution, and then I believe it will be highly adopted. But we're by far not there yet.
Yes, that's also what I face in this research. It's obviously just an exploratory research, essentially I want to look for an answer on the question if a network could be better secured if it's linked with a consensus algorithm that can verify the trustworthiness of the nodes in the network as well.
Yes, I agree that currently the most systems will have the normal fault tolerant networks. Devices can have an identity in the network, but the question comes about the integrity of the device. Can you trust the data that's coming at you from that device. So you know the identity but somebody changed the chip or something, how do you detect that. Especially on inexpensive devices.
If you can detect that something is tampered with and quarantine that device, that's fine. But I believe we still have some distance to reach that on a price point before that's really deployable. I believe indeed it will go such a way.
Ok, but I can imagine indeed that at a higher level it would already help. If you have those 4 nodes connected and let them check each other, then it would be much better secured.
Yes, I believe though ML works very well for things like junk email. If you can train that at the right level and share that learning across the network, and the system is continuously learning, then it's adaptive to threats indeed. The difficulty is that hackers would slightly change their attacks. There're so many attacks that are not detected because they're just slightly different. I believe you would need a lot of people checking new

scenarios and classify those threats correctly. But indeed it would be better because at the moment those things get all checked manually. Essentially you're already doing that when upgrading your security software. It could be better automated maybe in this way.
Yes, that's the biggest advantage of machine learning. But if you have such a standard set of rules without machine learning and you let this run on a current network, for example the hospital again. Then the protocol can also make sure all the nodes keep their security level up to date? So you don't rely on your staff to update the computer but they simply can't connect anymore if their security level is not correct?
Absolutely, I think it should be helpful in both ways indeed. Especially when you have connectivity between many nodes, and you work together with another companies and you know they're honest and the staff can be trusted. You now need to rely on their word that they're running the right software. It might just be that even though they're honest, they might just don't care about an update. So at some level, you can then verify that the people you communicate with are having the same standard as I have. This is very useful that you indeed can do with the blockchain because you can set these rules and let them be verified. So I indeed can see an architecture like this could help, but there're so many different buts and maybes about the standardization about this to make it valuable, if you don't have them all right it's not going to be valuable.
Ok, so essentially you're saying that it's valuable but probably very hard to bring in practice. It would also make it easier to share information about different attacks among different companies.
Yes, exactly there're already companies though that collect data about different attacks and share that knowledge with other companies.
Ok, thank you very much for your time. I think we agree that it definitely could work, but that it's probably very hard to introduce this.
Yes, indeed. I think in practice we first need to experience a full stop before we can justify these better secured solution. Companies who would now make a claim that they can secure such a network optimally with new technology are probably just making a false claim.
And to make sure, one last question, at the moment critical infrastructures are not secured on this level, only the fault tolerant networks.
Yes, they do try to improve the physical security in a cost effective way. But what a security architecture will often say is that we can build you a system that is very very secured, but it will come with a price.
Ok, but I can imagine that if you have sensors in the network where you can see that it's been tempered with you already have a better secured network.
Indeed, if one sensor is attacked and the others can detect that, it will help. But that will have network and communication cost, so we have some time to go before that's realistic. Will it happen, absolutely, but before we're there I think that will take some time.
There's a lot of work to do indeed. Probably a few more breaches and cost need to happen before we can justify the cost of better secured systems indeed.
Yes, it will take some time before all the things come together, but you're looking at a very interesting space, that's for sure. I wish you the best with this, and I hope you'll come a step further with this.
Thank you very much for your time. I'll definitely have a look into the GuardTime company.
Not a problem, let me know when I can help.
Thank you, we'll keep in touch.
Thank you Denny, bye.

Interview 3

Date: 02-10-2018

Introductie

..

kunt u aangeven wat u weet van Internet of Things?

Dat is uiteraard een algemeen breed begrip. Het gaat om een aantal machines, maar ook mensen die aan het internet hangen en daar communicatie mee voeren. Iemand die allemaal chips en apparaten en chips in zijn lichaam heeft b.v. voor medische redenen hoort daar ook bij.
Klopt inderdaad, met name de communicatie van al die kleine apparaten op grote schaal. Chips en sensoren die overal gebruikt worden.
Ja inderdaad, en je kunt het breder nemen. Je kunt het verengen tot een communicatie maar niets sluit uit dat er samenwerking tussen die machines plaatsvindt en dat ze ook besluiten kunnen nemen. Dan kom je misschien in de buurt van de blockchain.
Ik kan me voorstellen dat je uiteraard voorzichtig moet zijn hoe ver je daar mee wilt gaan. In de laatste jaren is ook een begrip ontstaan rondom Industrial Internet of Things. Heeft u daar iets over gehoord?
Daar weet ik eigenlijk weinig van.
Geen probleem, Industrial Internet of Things is eigenlijk het verlengde van IoT maar dan op Industrieel vlak (zoals de haven van Rotterdam of kritieke infrastructuren). Dus machines met sensoren en chips in het hele netwerk voor monitoren en optimaliseren van het netwerk. Echter is er een groot verschil dat het netwerk in principe privaat is en dus beperkt is voor specifieke machines binnen dat netwerk. IoT gaat juist over de openheid van alle apparaten die met het internet verbonden kunnen worden. Echter hoeft een IIoT netwerk niet van een bedrijf te zijn, het kan ook van een samenwerking tussen bedrijven zijn.
Als ik het goed begrijp onderscheiden ze zich omdat ze een dedicated taak hebben?
Juist en er zitten andere financiële aspecten aan vast uiteraard.
Gelukkig weten we dat ook weer.
Altijd fijn uiteraard nieuwe dingen te horen, sinds 2014 is die term eigenlijk omhoog gekomen. Je zou ook kunnen stellen dat het een trend is die waarneembaar is. Eerst begon het met de consumenten die zonder na te denken eigenlijk alles aan het internet verbonden en met elkaar communiceren. Nu zie je dat de industrieën eigenlijk ook inzien dat ze er misschien iets mee kunnen, op voorwaarde dat het allemaal beter beveiligd is. Het gaat dan wel om een privaat netwerk, maar waarin alles verbonden is maak je ook het risico groter dat als 1 component is aangevallen, de rest gelijk ook in gevaar is.
De belangen zijn uiteraard groter
Inderdaad, en dit onderzoek richt zich met name op dat probleem. Dan wil ik nog een paar vragen stellen over cybersecurity. U zei net al dat tijdens uw opleiding en huidige functie er al wat cybersecurity komt kijken. Zou u in het kort nog even kunnen aangeven wat uw expertise is met cybersecurity.
Nou we hebben verschillende projecten gedraaid op het gebied van cybersecurity. Maar volgens mij kan je het op verschillende niveaus bekijken. Dit begint bij de laagste tussen de machines. Al die machines communiceren namelijk ook al met elkaar en er gaat erg veel data heen weer. Je zou dus kunnen kijken als je die data bij elkaar brengt en vergelijkt, of daar uitschieters tussen zitten. Je hebt de zogenoemde Intrusion Detection Systems (IDS) zie allerlei dingen zitten te checken. Die kunnen bijvoorbeeld zien of men dezelfde soort vragen aan het systeem stelt etc. Als er dan bepaalde dingen afwijken van de vaste patronen wil je dat combineren met weer andere gegevens om te kijken of er iets aan de hand is. Bij DDOS aanvallen zullen ze bijvoorbeeld een systeem overbelasten. Dan krijgt het systeem dus ineens heel veel data, dan stopt het weer en op het moment dat het bijna onder controle is probeert de aanvaller weer enorm veel data te sturen. Je hebt natuurlijk een aantal strategieën om dit tegen te gaan maar om die mogelijkheden in kaart te brengen moet je dus de data tussen de componenten verzamelen en analyseren. We hebben dus met name naar de data van de IDS gekeken.
Dan kijk je dus met name naar de trends? Dus dan ga je ervanuit dat er een afdeling is die de data moet verzamelen en daar analyse over doet om verbeteringen te kunnen ontdekken?
Juist en in kaart brengen wat bijvoorbeeld nieuwe DDOS strategieën kunnen zijn. Je kunt een DDOS namelijk op verschillende manieren uitvoeren. Die veranderen ook in de loop der tijd, en dat zou je dus dan in de gaten willen houden.
Maar andere dingen zou je ook kunnen waarnemen, een virus bijvoorbeeld ontstaat niet van de ene op de andere dag. Wat je ziet is, net als in de biologie, dat er allerlei componenten zijn die men hergebruikt om weer een nieuw virus te maken. Dat zijn een soort mutaties, en die zou je natuurlijk ook willen zien aankomen. Zoals bijvoorbeeld Flame en Stuxnet, dat was niet helemaal vanaf scratch opnieuw gemaakt.

Dat is op het laagste niveau, maar we zijn bijvoorbeeld ook geïnteresseerd in hoeveel aanvallen er zijn geweest en welke typen. Wellicht in kaart brengen of er nieuwe criminaliteit of virussen ontstaan, daar kijken we ook naar.

Ik kan me ook voorstellen dat het stelen van data bij jullie ook gevoeliger is dan b.v. een DDOS aanval waarbij het systeem gewoon even plat ligt.

Precies, bij een DDOS aanval gaan ze niet in je systeem. Het is veel erger als ze in je systeem weten in te breken. Als men bijvoorbeeld rekening nummers of saldo's kan veranderen of data kan stelen dan is dat inderdaad een groot probleem.

Dat is dus wel waar we ook binnen onze systemen naar kijken.

Gebruiken jullie dan ook al machine learning in jullie cybersecurity?

Nou kijk machine learning is wel aardig, maar het werkt alleen maar als je heel veel voorbeelden hebt want daar moet hij van leren. Als je net op zoek bent naar upcoming trends, dan heb je niet zoveel aan machine learning. Een andere mogelijkheid is als je al een goed model hebt en waarbij nieuwe dingen toegevoegd kunnen worden die zijn gedrag wat kan aanpassen. In alle andere gevallen werkt ML niet zo goed voor trends.

Niet echt in de cybersecurity dus wat dat betreft.

Nee, wat mij betreft niet. Daarbij heb je ook nog het probleem met die curse of dimensionality in ML, wat ook niet erg goed is opgelost.

Is dat, dat je veel foute meldingen krijgt van dingen die eigenlijk goed zijn?

Nou kijk wat je hebt is dat in drie dimensies kunnen we ons wel een voorstelling maken. Stel dat je een classificatie probleem hebt, kan je classificeren op basis van drie criteria. Als je dan een nieuw punt hebt, kan je makkelijk uitrekenen bij welke klasse die behoort. Op het moment dat je dat moet doen op basis van 4000-5000 kenmerken heb je niet alleen het probleem van overfitting en heb je veel data nodig, maar een ander probleem is dat je doet in hoge dimensie, dan is ons afstandsbegrip niet toereikend omdat alles veel teveel op elkaar lijkt.

Ok, ik begrijp dat je dat dan lastig kunt schalen en vergelijken inderdaad. Dus je ziet op dit moment nog veel dat een cybersecurity specialist door de data moet scannen op zoek naar onregelmatigheden.

Ja, maar die gebruiken wel tools hoor, en ze leren hier uiteraard sneller doorheen te gaan. Kijk waar je ML kunt toepassen, moet je dat vooral doen.

Uiteraard, ze worden er steeds beter in en wat nu niet kan, is wellicht wel mogelijk in de toekomst. Wat je wel ziet is dat veel aanvallen er inmiddels ook al gebruik van maken, dus dan is het alleen maar logisch en wellicht noodzakelijk dat je er aan de defensieve kant ook gebruik van gaat maken.

Juist, en kijk bij security moet je er vooral ook op letten dat mensen proberen in te breken. Een van de meest voorkomende redenen dat dit lukt is omdat we onze systemen ook niet goed testen. Als een programma 2 gehele getallen goed moet tellen, dan stoppen we heel veel hele getallen erin en kijken of het juiste antwoord eruit komt. Maar we testen heel slecht op non-functionele requirements. Wat op zich te begrijpen is want de klant betaalt ook juist voor de functionele requirements, maar die non-functionele requirements daar zitten de lekken in.

Uiteraard, die zijn ook belangrijk.

Juist, dan zie je bijvoorbeeld dat er iets net niet gaat zoals het moet en dan breng je het systeem in de war. Maar belangrijker is dus dat aanvallers hier vaak naar op zoek zijn.

Dus dan zouden de developers inderdaad meer daarop moeten testen, monkey testing wordt dat wel eens genoemd volgens mij.

Ja inderdaad.

De vraag is inderdaad of dat met machine learning geholpen kan worden, dat zal wel lastig zijn. Om door te gaan naar een volgend onderwerp, zou u in het kort kunnen aangeven wat u weet van blockchain technologie en de belangrijke componenten daarvan?

Ja, blockchain zie ik hetzelfde als big data want het zijn beide container begrippen. Volgens mij is het een verzameling van unieke technologieën die nodig is om een specifiek probleem op te lossen. Natuurlijk zitten er wat kenmerken in zoals security, consensus etc. Bij dit soort dingen zijn vaak een hoop definities.

Begrijpelijk, inderdaad merk je dat er nog veel verschillende blikken zijn op het begrip.

Juist, maar er zijn wel een aantal dingen centraal zoals distributie, consensus proof-of-stake (POS), zijn wel essentieel.

Inderdaad, en is dat in uw opzicht wel anders dan gedistribueerde databases?
Ja, kijk dat is wel anders. Want een gedistribueerde DB is natuurlijk niets nieuws. Het probleem wat bij de blockchain wel is opgelost is bijvoorbeeld wel het probleem van de updates. Bij een gedistribueerde DB heb je dezelfde informatie op verschillende plekken, als de data op een punt veranderd wordt moeten de andere locaties worden geüpdatet. Deze updates duren lang dus alle systemen moeten gelogd worden. Dergelijke aspecten komen bij de blockchain minder voor want je slaat alles overal gelijk op. Die update in een gedistribueerde DB zijn overigens vaak dure operaties.
Eigenlijk is het niet helemaal eerlijk misschien, want die update verplaats je een beetje naar voren. Als ik namelijk in een DB iets aanpas, dan gaan we na een bepaalde periode zeggen dat dit in de andere systemen ook aangepast moet worden.
Bij een blockchain heb je ook wel die aanpassing, echter moet iedereen er wel consensus over hebben. Dus dat toetsing moment is naar voren geschoven.
Juist, daardoor kan je de historie niet aanpassen op 1 locatie, je kan alleen via consensus iets toevoegen als nieuwe waarde.
Klopt, voor sommige toepassingen zal de blockchain dan ook nooit werken, of is het erg onwenselijk. Wij hebben bijvoorbeeld te maken met het recht op vergetelheid, waarbij je dus het recht hebt dat de overheid je compleet vergeet. Dan moet je dus dingen wel definitief kunnen weggooien, en dat kan hier weer niet.
Dat is inderdaad een interessante situatie waar ik niet bij stil gestaan hebt.
Ik ben dan ook geen enorme fan van de technologie, maar ik ben ook niet degene die het afschiet.
Ja, u geeft gewoon aan dat het in sommige gevallen wel nuttig kan zijn. Dit is overigens ook zoals ik op de blockchain kijk. U gaf net ook al aan dat distributie en consensus toch wel de belangrijke componenten zijn. Proof-of-stake kan je uiteraard op verschillende manieren opvangen.
Dat kan inderdaad van standaard tot hele geavanceerde methodes en alle manieren zullen verschillende kosten hebben.
Zeker. Bijvoorbeeld als je iedereen in het netwerk eerlijk kan houden, dan heb je geen dure oplossing nodig. In de situatie waar ik onderzoek naar doe zie ik dat ook terug. Het gaat dan namelijk over een privaat netwerk waarin je ervan uit kan gaan dat iedereen in principe eerlijk is. Daarvoor heb je dan wel verschillende andere security maatregelen, maar daar zitten incentives niet in verwerkt zoals proof-of-stake.
Ja daar zullen de aanvallen weer meer van buiten komen.
Klopt, een van de lastige aspecten is dan ook ten koste van wat gaat het dan.
Dat hebben we overigens hier ook gezien, we zijn ontzettend goed om een virus buiten de deur te houden, maar stel dat het lukt, dan zie je dat het zich heel snel verspreid en er intern geen controle meer is. Het is net als de internet firewalls, die houden alles tegen, maar als je er dan eenmaal doorheen bent is er niks meer dat je zal stoppen.
Precies inderdaad, want dan ziet het netwerk al alsof het te vertrouwen is.
Juist, en dan zijn er geen andere analyses meer die checken of iets niet klopt. Om een voorbeeld te geven, daar zal machine learning ook niet echt werken denk ik. Menselijke kennis zal daar vaak effectiever bij zijn. Bij een bedrijf wat ik heb meegemaakt is zoiets gebeurd, waar op den duur wel een virus was maar dat is heel lang niet herkend. Totdat iemand zo slim was om te zien dat er inderdaad iemand ‘s avonds heel laat veel updates doet, maar hoe kan dat nou want er werkt bijna niemand om 3 uur ‘s nachts. Toen ze dat verder bekeken bleek het inderdaad een virus te zijn. Dat is gekomen omdat iemand gewoon naar de werklast heeft gekeken en met name hoe laat.
Ja tussen 09:00-17:00 zal dat wel heel normaal zijn, maar het gaat juist om meerder componenten die met elkaar vergeleken moeten worden. Dan is het maar de vraag of het systeem zelf of ML dat zou kunnen herkennen.
Inderdaad, dan zou het systeem misschien kunnen denken dat alle batch operaties even stilgelegd moeten worden, die juist wel ‘s avonds plaatsvinden. Daar heb je een soort onderzoekers mind voor nodig die meer dingen kan beredeneren op logica, daar zal ML niet zo gek veel kunnen helpen denk ik.
Nee inderdaad, zeker niet om daar om te beginnen achter te komen. Wellicht als die algoritmes al een tijdje draaien zal die misschien wel kunnen zien dat er op een rare tijd data wordt verzonden.
Juist, als je veel data beschikbaar hebt en een model al hebt, dan kan je dingen misschien herkennen.

Na een bepaalde tijd zou het dus wel kunnen maar het blijft een investering. Om terug te gaan naar het onderwerp blockchain. Zoals u net al zei, een van de kenmerken is het consensus algoritme. Daarvan zijn er verschillende versies, een daarvan is Paxos. Bent u bekend met Paxos?
Ja, ik heb van Paxos gehoord en veel verhalen gehoord, maar kan je het me nog een keer uitleggen?
Heeft u veel gehoord over Paxos specifiek of meer over consensus algoritmes in het algemeen?
Jazeker, er zijn in de wiskunde natuurlijk heel veel consensus algoritmes. Als je kijkt naar bijvoorbeeld verzamelingen leer. Als jij iets uitdruk in A, B, C en ik in A,G,E,F dan hebben we consensus over A. Er is dus niet 1 consensus algoritme.
Nee inderdaad, consensus is dus eigenlijk een overeenstemming van dingen?
Dat kan een definitie zijn, ik kan je ook overtuigen van B, dan hebben we ook consensus.
Ja dat is waar, en in de blockchain weet u dat consensus betekent dat de verschillende databases overeenstemming moeten bereiken over nieuwe waarden?
Ja inderdaad, alleen die consensus wordt bereikt door het stemgedrag en niet zozeer de rationale erachter. In het voorbeeld van net zit er een rationale, we zeggen allebei A en begrijpen dat dan ons consensus is. Maar bij de blockchain is het puur dat er wel gestemd wordt, maar de rationale erachter is er niet. Dat maakt het voor mij altijd lastig om er een duiding aan te geven.
Bedoelt u daarmee dat er geen waarde oordeel wordt gegeven?
Juist waarom je tot een bepaalde stemming komt. Als we beiden iets anders zeggen, zoals jij geeft akkoord en ik niet akkoord, dan weten we beiden niet waarom we dat doen of de redenen van de ander.
Ja, dat is inderdaad binnen het consensus algoritme lastig op te nemen. Het algoritme Paxos dat ik voor dit onderzoek heb onderzocht is beschreven door Leslie Lamport. Hij geeft daarin ook een aantal requirements die gelden om het systeem te laten werken, ten eerste dat je iedereen moet kunnen vertrouwen en ten tweede dat je geen waarde oordeel kan geven over de voorgestelde waardes. Dat is ook niet nodig omdat je iedereen in het netwerk kan vertrouwen en de waardes dus per definitie goed zijn. De voorwaarde is dat er genoeg andere nodes getuige moeten zijn en als ze online zijn dan ook per definitie "ja" stemmen.
Maar het is wel altijd een meerderheid van stemmen neem ik aan?
Ja, dat klopt wel. Maar die meerderheid is op basis van of de meerderheid wel of niet online is (bereikbaar). Ze kunnen niet tegen de waarde zijn, tenzij het tegenspreekt met een eerder voorstel. Ik kan me voorstellen dat ze ook nog kunnen kijken naar bijvoorbeeld beschikbaarheid. Als machines in een netwerk bijvoorbeeld een verzoek krijgen dat een bepaalde machine een hoop kracht nodig heeft voor een bepaalde tijd (rekenkracht of elektriciteit etc.) en een volgende machine een zelfde verzoek heeft, dan kunnen ze vast consensus bereiken dat ze het verzoek even moeten weigeren bijvoorbeeld. Ze kunnen in veel andere gevallen denk ik lastiger een oordeel geven over de waarde. Als het apparaat bijvoorbeeld vraagt of hij zijn apparaat naar 100 graden mag brengen, dan kunnen de andere machines waarschijnlijk lastig beoordelen of dat correct is.
Nou dat is precies wat ik bedoel. Als ik 100 voorstel dan kunnen we als mensen goede redenen bedenken waarom dat wel of niet 100 zou moeten zijn, maar de apparaten zullen wel consensus bereiken en akkoord gaan.
Juist, en akkoord is in dit geval een vreemde woordkeuze, ze zullen wel ja zeggen, maar akkoord dat weten ze niet.
Dus het is niet echt consensus.
Ja behalve dat ze wel allemaal weten dat het gebeurt en dit allemaal opslaan in hun database en ze zijn consistent daarin, welke uitkomst het ook heeft.
Juist, ze weten er in ieder geval van. Het is dus meer knowledge sharing dan dat het consensus is.
Klopt, en dat is dus het verschil met Paxos. Die gaat er eigenlijk vanuit dat als we ons kunnen beschermen en afzonderen, dan kunnen we ervan uitgaan dat die apparaten correct werken. Er zijn wel andere mogelijkheden en bijvoorbeeld Hyperledger maakt volgens mij gebruik van externe validatie. Dat betekent dat ze de waarde laten controleren door een beperkt aantal machines, voordat het naar het netwerk gaat. Daarmee beperk je dus de voorstellen die mogelijkheid zijn.
Zeker, dan heb je natuurlijk ook dat iemand het moet controleren en je ze dus een puzzel laat maken enzovoort. Dat zijn natuurlijk implementatie technieken.

Nou die puzzel komt uiteraard vooral uit de bitcoin blockchain. Dit heeft ermee te maken dat daarin iedereen zomaar voorstellen kan doen. Om een voorstel te doen moeten ze dus eigenlijk erin investeren.
Dat zijn dus allemaal implementatie technieken.
Ja, zo kan je dat zien. Om terug te komen op Paxos, daar ga je ervan uit dat iedereen in het netwerk te vertrouwen is en die voorstellen dus ook mogen maken. Ze zullen daarom transparant kunnen werken en data overal consistent opslaan. Je kan niet zomaar de data aanpassen want dat ziet de rest dan ook gelijk.
Dat begrijp ik, die transparantie draagt dus eigenlijk bij aan het vertrouwen.
Precies, dat is het idee van Paxos. Dan heb ik eigenlijk een vraag over een scenario van een netwerk binnen een bepaalde organisatie. Daarvoor heb ik dit simpele model gemaakt als voorbeeld. Er zijn verschillende manieren voor het netwerk om de machines erin te kunnen identificeren, bijvoorbeeld IPV6 of iets anders.
E wil dus nu tot het netwerk behoren?
Dat is mogelijk, het kan ook zijn dat andere nodes disconnected zijn en weer toestemming vragen erbij te horen. Het moet eigenlijk aangeven dat dat de eerste stap is om het netwerk privaat te houden. De rest zal dan inderdaad via consensus al vast stellen of die machine erbij hoort. Dat request kan uiteraard op bepaalde criteria worden getoetst (zoals persoonlijke security etc.), maar hoe dat precies gebeuren moet is niet echt onderdeel van dit onderzoek.
Als je vervolgens op deze manier het netwerk hebt ingericht, moeten de nodes in het netwerk via consensus alles naar elkaar meedelen. Uiteraard komen er dan ook acties in voor die wel iets makkelijker te controleren zijn aan de hand van bepaalde criteria, maar ook een aantal dingen zijn niet te controleren zijn, zoals we eerder hebben besproken. Uiteindelijk is het idee dat de nodes wel van elkaar een aantal zaken kunnen waarnemen en of er niet mee gerommeld is. Het idee dat je het daardoor beter beveiligd kan maken dan de huidige situatie. Kunt u zich dit zo voorstellen.
Ja hoor, daar kan ik me iets bij voorstellen. Stel er komt een request dat ze allemaal een afweging maken en met elkaar communiceren. Ik kan me wel voorstellen dat iedere node in dat netwerk zijn eigen criteria heeft.
Kunt u aangeven wat u daarmee bedoelt?
Dat zou ik wel sterker vinden, want als ze allemaal dezelfde criteria hebben, dan hoef je niet 4x hetzelfde te doen. Maar bij mensen zou het zo werken dat we allemaal verschillende vragen stellen, dan weten we weer wat meer over het verzoek. Als we allemaal dezelfde vragen stellen en die blijkt fout te zijn, zitten we er allemaal naast.
Als de verschillende nodes dus andere criteria kunnen hebben, dan maakt het uiteraard een stuk veiliger.
Alleen is de vraag uiteraard waar die andere criteria dan op zijn gebaseerd, en waarom je dan niet allemaal die volledige scan kan uitvoeren.
Ik zou zeggen als bijvoorbeeld D een node is met een andere dedicated taak dan B en ze kunnen beide iets leren van die taak, zullen ze ook andere vragen kunnen stellen.
Ok, dan zouden ze dus eigenlijk in elk geval moeten leren wat er met hun eigen netwerk en taken gebeurt.
Ja, dat lijkt me wel een denkbaar model.
Zeker, waar ik bij twijfel is dat als ze toch al alles met elkaar delen, ook hun eigen dedicated taak, zouden ze ook alsnog allemaal die criteria gelijk kunnen hebben.
Nou dat is waar, maar als alles gelijk is, ze delen alles en iedereen vertrouwt elkaar, dan reduceer je dat tot 1 en heb je weer niet al die netwerken nodig.
Dat is waar, maar dan komt de vraag naar boven hoe makkelijk je dan die ene kunt manipuleren die voor dat criterium moet zorgen. Daar kan ik zelf lastig zicht op krijgen.
Ja dat is zeker, als je die weet te beïnvloeden dan beïnvloed je iedereen.
Ik snap uw punt inderdaad. Maar mijn vraag is dan, als je als aanvaller een node kunt manipuleren en vervolgens aan die node vraagt om toetreding binnen het netwerk, zou dat dan mogelijk zijn. Dat zou uiteraard niet mogelijk zijn als het hele netwerk ook het criteria moet toetsen, ondanks dat het dus hetzelfde zou horen te zijn. Maar het is uiteraard een goed punt, ik zal eens kijken of die nodes wellicht op andere criteria kunnen komen. De kern beveiliging is de transparantie waarin de communicatie plaatst vindt en of dit consistent is met de historie. In dit protocol zou je dus allemaal opslaan wat er gebeurt en onder welke omstandigheden.

Ja dat vertrouwen vanwege die transparantie zou zeker beter worden, maar ik weet niet of dat hetzelfde is als beter beveiligd. Want ik kan uiteraard veel vertrouwen hebben, maar het kan nog steeds heel slecht beveiligd zijn.
Dat is zeker waar. Vertrouwen is echter wel terug te koppelen naar security als je de betrouwbaarheid kunt checken en kunt zien of er bijvoorbeeld niets raars met de machine is gebeurd.
Ja zeker, het is niet 1 op 1, maar het heeft zeker met elkaar te maken.
Ok, ik kan me ook voorstellen dat dit in grotere netwerken op dit moment nog niet van toepassing is. Wat je vaak ziet is dat als er 1 node in het netwerk wordt aangevallen, je het hele netwerk binnen kunt komen. Eigenlijk komt dit terug op wat u eerder zei over "als je eenmaal in het netwerk bent, zal niemand je meer tegenhouden". Het idee is dat met deze manier en transparantie je eigenlijk al beter beveiligd bent. Als 1 component wordt aangevallen of gecomprimeerd zou de rest dat moeten kunnen zien. Kunt u zich hier iets bij voorstellen.
Ja, maar dat zou betekenen dat zo'n node altijd stigmatiseert. Op het moment dat hij iets anders doet dan normaal maar volledig legaal, dan is hij al gestigmatiseerd. Dan zeggen de andere nodes, wacht even, wij verwachten van jou dat je mail verwerkt en stel dat er weinig mail is en hij iets anders gaat doen is dat al verdacht.
Ja daar heeft u gelijk in, dan zou je telkens moeten leren dat iets normaal gedrag is.
Maar die kans van leren krijg je dan niet. Want je verwerkt elke dag mail, dat leert de rest, op het moment dat je op een tijdstip ook documenten gaat verwerken word je geblokkeerd.
Ja, ik snap uw punt. Je geeft dus eigenlijk aan dat het wel beter beveiligd is alleen dat het misschien te beveiligd gaat worden.
Juist, die flexibiliteit ga je dan verliezen en heb je eigenlijk wel nodig en moet je erin laten denk ik. Maar goed, dat hangt wellicht van de applicatie af. Als binnen een applicatie die flexibiliteit niet nodig is, dan zou dit prima kunnen werken. Dus ik denk dat het goed is als je dit gaat ontwerpen, dat je eerst naar de applicatie kijkt en de flexibiliteit. Is het vertrouwen en transparantie belangrijk, kan je hiervoor kiezen. Maar ik kan me ook voorstellen dat die transparantie juist weer helemaal niet gewenst is. In militaire systemen wil je misschien weer niet dat alle systemen transparant met elkaar kunnen communiceren en dingen kunnen uitlezen.
Daar heeft u gelijk in. Nou is het wel weer zo dat als bepaalde communicatie en dingen te zien zijn voor andere nodes binnen het netwerk, dit nog niet betekent dat mensen dat kunnen interpreteren. De apparaten onderling zouden wel moeten begrijpen wat er gebeurt. Daardoor zou een aanvaller niet alle data uit de systemen kunnen halen en er gebruik van maken.
Dan ga je er vanuit dat je software gebruikt die niet te decrypten is.
Ja, wellicht is dat een requirement.
Maar de vraag is dan wel, als je software gebruikt die niet te decrypten is, hoe transparant ben je dan.
Dat snap ik, maar dan is de vraag of je kunt vertrouwen of het netwerk dat zelf kan en wij daar geen inzicht in hebben.
Ja dat is waar.
Heel interessant allemaal om te horen, nog in het kort geeft u eigenlijk aan dat in essentie er een mogelijkheid is. U schat in dat je dan wel veel moet inleveren qua flexibiliteit omdat je er anders snel uitgeknikkerd wordt. Ik kan me voorstellen dat in het begin daar veel werk in zit om dergelijke uitzonderingen te ondervangen, maar in de loop der tijd daar minder van voorkomen en het dus beter beveiligd is. Maar nog even ter bevestiging, in een dergelijk scenario kunt u voorstellen dat een aanval van buiten makkelijker tegen gehouden wordt?
Jazeker, dat kan ik zeker voorstellen. Als het systeem inderdaad verwacht dat iets standaard gaat en dat gebeurt niet, dan zal er vast wat aan de hand zijn en kunnen ze dat zien.
Zoals het voorbeeld van de update ‘s nachts, dat zal sneller worden gevonden. Uiteindelijk begin je hier met een oplossing zonder machine learning.
Ja hier stop je die kennis er expliciet in.
Juist, en dat moet je dan telkens veranderen als er nieuwe uitzonderingen bij komen. Alleen ik kan me ook voorstellen dat die machine learning gebruikt kan worden in alle componenten en dat ze zelf slimmer kunnen worden en die uitzonderingen zelf behandelen. De meest veilige optie zou zijn als dat op alle nodes gebeurt i.p.v. een centrale vorm.

Ja nogmaals vraag ik me af als ze alle vier dezelfde gegevens hebben en hetzelfde leren, dat je dan nog meerdere keren hetzelfde moet doen. In grote lijnen zullen ze wel hetzelfde leren als je ML op die verschillende nodes laat draaien met dezelfde gegevens. Als je die leerfunctie en criterium anders kan laten worden, dan is het zeker een sterker systeem. Overigens als ze wel hetzelfde leren zouden we ook een keer moeten uitproberen, want dat kan ik alleen maar schatten.

Juist en het voordeel wat je sowieso hebt denk ik, is dat die ML algoritmes op 1 node worden uitgevoerd dat je weer terug gaat naar je single point of failure wat je juist wilt voorkomen.

Klopt, het nadeel is dat je wel weer 4x hetzelfde doet. Dat is altijd wel de afweging die je moet maken inderdaad, het zal allemaal voordelen en nadelen hebben.

Klopt inderdaad, uiteraard blijft dit een theoretisch onderzoek en zijn we op zoek naar de mogelijkheid om het optimaal te beveiligen. Met name ook omdat dit wellicht op het moment qua kosten nog onpraktisch is, maar voor sommige netwerken waar miljarden in om gaan of infrastructuren die 100% beveiligd moeten worden, is het misschien zo gek nog niet.

Daar heb je gelijk in, misschien zou je ook een soort hybride versie kunnen inbeelden. Dat een deel wel op deze manier gaat en een deel via een makkelijkere versie.

Dat klopt, dat is nog een optie dat je het op de makkelijke manier doet, totdat er iets geks gebeurt.

Maar weet je, met dit soort dingen is het gewoon dat je het probleem moet pakken dat je wilt oplossen, een prototype bouwen en dan kijken wat werkt.

Dat kan ik me voorstellen inderdaad, ik hoop ook dat dit ooit gebouwd gaat worden, helaas zal dat niet binnen mijn onderzoek passen. Daarmee kunnen we denk ik dit interview gaan afsluiten. Als ik het goed begrijp geeft u wel aan dat u denkt dat het middels zo'n oplossing wel iets veiliger wordt dan de huidige situatie?

Ja, ik denk dat je zeker een goede richting hebt. 1 ding weet ik vrij zeker, met name als je kennis deelt dat je vaak tot betere inzichten zal komen. Ik denk dat zoiets wel geschikt is om die kennis te delen en het hele netwerk daar dan op gebouwd is. Je zou wel weer moeten afwegen wat je dan weer moet delen enzovoort om te voorkomen dat het weer overbelast zou worden.

Daar ben ik het volledig mee eens en dat zal weer afhankelijk zijn van elke situatie en de capaciteit van het netwerk. Echter is dat niet de focus van dit onderzoek en kan ik helaas niet veel over zeggen. Eigenlijk is het er nu vooral op gericht om te kijken of dat netwerk zichzelf beter kan beveiligen. Er is al veel werk in distributie en consensus gedaan omtrent failures en power outages, echter naar mijn idee nog niet veel met de achterliggende gedachte om een netwerk veiliger te maken tegen aanvallen. Door het feit dat je toelaat meerdere dingen te vergelijken, zou het wellicht veiliger worden.

Ja, ik denk het wel. Ik schat in dat het wel veiliger zou zijn. Alleen is het de vraag of dit het waard zal zijn. Daar zal zeker nog meer onderzoek gedaan moeten worden. Overigens worden die aanvallers dan ook weer slimmer uiteraard, maar met dergelijke oplossingen zullen ze wellicht sneller door de mand vallen. Het is dus zeker de moeite waard om te implementeren en uit te proberen om te kijken wat het oplevert.

Jazeker, nou dan wil ik u bij deze in elk geval hartelijk bedanken voor uw tijd en voor alle waardevolle input. Ik zal dit bericht documenteren en ter controle naar u opsturen.

Graag gedaan, ik ben benieuwd naar de afloop en het vervolg van dit onderzoek. Ik wens je uiteraard hier veel succes mee.

Nogmaals bedankt, ik zal u op de hoogte houden.

Interview 4

Date: 17-10-2018

Introductie

..

Duidelijk, om maar door te gaan naar het volgende onderwerp, IoT, je zei net al dat je daar iets van mee gekregen hebt in een project. Zou je in het kort kunnen vertellen wat je van IoT weet en hoe je ernaar kijkt?

Nou IoT in het algemeen is vooral meer van wat we al hadden. De telefoon was altijd al IoT, alleen zijn we nu doorgeschoten met sensoren en dergelijke waardoor het aantal apparaten exponentieel toeneemt. Dan gaan we het IoT noemen en komt er uiteraard vervolgens weer Big Data bij kijken want data hadden we allang al maar wordt het nu een veel groter volume. Maar goed het project wat ik gedaan had, gericht op Blockchain en IoT, dat kan je overigens ook teruglezen op onze website, dat is blockchain voor de foodsupply chain. We weten allemaal dat er in de voedselketen toch wat dingen spelen die niet altijd goed gaan, je hebt het ene na het andere voedsel schandaal zeg maar. Het wantrouwen in die keten is dan ook bijzonder hoog. Wanneer je het over wantrouwen hebt wordt blockchain toch vaak al relevanter. Onze partners waarmee we samenwerken hebben een oplossing gemaakt waarmee je animal protein op een blockchain kunt registreren en volgen. Dat komt dus uit de DNA van een dier, koe of varken, zodat het een unieke identifier heeft en kan worden geplaatst op een blockchain. Dit lijkt nog niet heel veel IoT, maar alle apparaten die daarin gebruikt worden is wel degelijke IoT. Dat hele proces zit vol met smart tech en smart scanners om het bloed af te nemen, naar een identifier te vertalen en vervolgens die dieren te kunnen volgen. Daar zie je dus een mooie toepassing van IoT en blockchain samen.

Daarnaast hebben we wel verschillende proof-of-concepts gezien die ook dergelijke combinaties kunnen maken. Smart meters die met smart contracts in auto's geplaatst worden en meer van dat soort voorbeelden heb ik wel gezien, maar de voornaamste ervaring binnen PWC hebben we dus wel met die voedselketen.

Oké, dus binnen die voedselketen en de blockchain daar doen die sensoren uiteraard een hoop werk om te zorgen dat die DNA in de blockchain komt. Dat hoeft uiteraard niet met een blockchain, maar dan neem ik aan dat die blockchain gebruikt wordt in de communicatie met de verschillende partijen die allemaal komen kijken bij dat proces.

Ja zeker, wat dat betreft hebben we er wel een hoop van geleerd. Zeker in termen van o.a. security alleen al komen daar natuurlijk een hoop aspecten bij kijken. Je moet natuurlijk kunnen garanderen dat wat er op die blockchain staat dat dat goed is. Een van de belangrijkste dingen waar je op moet letten is uiteraard zoals in elk systeem 'garbage in is garbage out'. Een blockchain die beschermt je daar ook niet heel goed tegen.

Nee inderdaad, de blockchain zelf kan niet valideren of iets goed of slecht is zeg maar.

Ja precies, dan zie je al snel dat de kwetsbaarheden ook weer terug te vinden zijn in de apparaten die de invoer verzorgen of de mensen daarvan. Het liefst doe je het sowieso automatisch met die smart scanners, maar dan nog is het niet waterdicht. Als de communicatie namelijk geborgd is via een blockchain, kan je zo'n apparaat nog steeds hacken.

Ja uiteraard. Maar de gegevens in de blockchain zijn inderdaad allemaal verspreid maar wel versleuteld en alleen beschikbaar voor degene die het moet zien.

Sowieso werken bedrijven alleen maar met afgeschermde blockchain, dus de inzage is al beperkt, en wat er op een blockchain terecht komt zijn inderdaad versleutelde gegevens. Zeker in het kader van teveel of te weinig transparantie, als je met verschillende leveranciers op een blockchain werkt wil je niet verschillende inkoopprijzen zomaar transparant maken. Dus er zit weer wel een zekere waarde dat informatie nou eenmaal niet transparant is.

Maar ook als je bijvoorbeeld vervoer service verleent en dat staat op de blockchain. Dan kan je dat misschien weer terug herleiden naar de persoon die dat vervoerd heeft, maar dat zijn weer persoonsgegevens die niet zomaar daarop mogen i.v.m. privacy. Gelukkig doe ik geen juridisch werk, maar ik begreep wel dat dit soort dingen nog steeds een issue is.

Oké, ik kan me voorstellen dat het lastig is en ook nog in de kinderschoenen staat wat nou het beste werkt.

Zeker, mede omdat er nog maar erg weinig van dit soort systemen in productie zitten. Pas als het in productie is genomen loop je weer tegen een hoop aspecten aan waar onder de juridische kant. Vaak zie je dat er met

een proof-of-concept gewerkt wordt op kleine schaal met test gegevens maar pas als er op grote schaal gewerkt wordt met verschillende organisaties en echte gegevens komt er toch weer een andere kijk op.
Uiteraard, maar die blockchain wordt wel weer op veel verschillende plaatsen opgeslagen.
Ja, dat is een beetje de natuur van de blockchain, het wordt op verschillende plekken opgeslagen en vervolgens met het consensus algoritme gegarandeerd dat het op iedere locatie ook exact hetzelfde is. Verder maakt het weer niet veel uit welk consensus algoritme je dan gebruikt, veel krijgen we de vraag van hoe zit het dan met dat minen. Maar je hoeft niet perse te minen om tot consensus te komen.
Nee inderdaad, en kan iedereen in het netwerk dan weer wel alle gebeurtenissen binnen het netwerk zien?
Nou om te beginnen wel, omdat je er vanuit gaat dat niemand binnen het netwerk elkaar nou ook echt vertrouwt. Daarom zullen ze wel de hele historie en alle gegevens moeten kunnen zien. Maar daar heb je alweer varianten op als je wat meer privacy wilt, zoals zero knowledge proof, waarbij je dus wel een transactie kunt bewijzen maar niet de details nodig hebt. Volgens mij heeft Ripple daar ook al een keer een proef voor gemaakt voor 20 banken waarvoor privacy wel erg belangrijk is. Uiteindelijk hebben ze daar wel een hoop omwegen voor moeten maken en ongeveer 300 subledgers gemaakt. Dat bleek daardoor ook niet helemaal goed te werken, maar het geeft wel aan dat er nog aan gewerkt wordt.
Oké en bij die zero knowledge proof dan moet je dus eigenlijk echt het netwerk volledig vertrouwen dat het goed werkt omdat je er zelf geen inzage meer in hebt.
gpt, en dat is design technisch ook weer een extra uitdaging, maar goed.
Nou dat is duidelijk, laten we maar doorgaan naar een volgend onderwerp, ben je toevallig bekend met Industrial Internet of Things of Industrial Internet?
Is dat niet gewoon een fancy term voor Industrie 4.0?
Nou dat zit wel in de goede richting. Zoals je al zei een supply systeem voor de voedselketen waar je een hoop sensoren hebt die van alles kunnen meten en kunt verwerken in het netwerk.
Ja inderdaad, alhoewel de meest wilde ideeën hierbij ontstaan. We kunnen uiteraard alles automatiseren met robots, en als er dan een order verwerkt wordt kan dat automatisch worden geladen in de zelf rijdende trucks. Dit alles zou met sensoren dan weer geregistreerd worden en zo. Dat soort ideeën zal het wellicht wel naar toe gaan in de toekomst, maar het moet wel met stappen. Het klinkt allemaal super en dan moet je ook nog eens een systeem hebben die dat allemaal goed managet en de data kan verzamelen etc., maar dat is allemaal nog wel een grote stap. Zeker alles wat niet start-up is daar kom je nog veel oude operating software tegen zoals veel Windows XP maar dan wel het idee hebben gelijk over te stappen naar top level.
Precies, die zouden ook met kleine stapjes moeten beginnen.
Inderdaad, maar dat komen we vaak tegen. Wat je ook vaak ziet is dat bedrijven AI willen gaan doen, maar als je dan vraagt naar de data, dan staat dat nog op papier.
Dat is inderdaad ook een veel te grote sprong.
Ja, voor ons ook altijd weer even een reality check dat er toch nog een hoop bedrijven zijn die gewoon met alles nog op papier werken.
Inderdaad, mijn onderzoek is overigens ook een beetje die kant op gegaan. Namelijk grote netwerken zoals powergrids, watersupply systems en dergelijke blijken toch allemaal erg oude systemen te hebben. Het is ook wel lastig dat allemaal up-to-date te brengen, maar daardoor wordt het alsmaar meer complex.
Nou inderdaad, breek me de mond niet open. Met name heb ik dan wat ervaring met de energie sector. Aan het begin was ik daar wel heel optimistisch over, totdat ik iets meer leerde hoe het allemaal werkt. Daar zitten zoveel partijen tussen, daar is geen lijn meer uit te halen. Een van de dingen die speelde was het creëren van een soort energie marktplaats voor mensen die energie genereren met zonnepanelen en dat vervolgens met smart contracts onderling kunnen verhandelen. De energie leverancier zou je daarvoor niet nodig hebben want die betaalt toch bijna niks voor de energie die je oplevert. Dan wordt er weer gedacht aan blockchain om dat te regelen, maar dat wordt wel erg complex.
Juist en ik kan me voorstellen dat grote energie bedrijven die je dan juist eruit wil halen er niet voor zouden betalen, dus wie dan wel.
Inderdaad, een mooie use case die je wel eens hoort is het kadaster, de eigendomsregistratie van grond en huizen. Dit zou je wellicht op een blockchain kunnen doen, maar dan is altijd de vraag van wie bouwt het. Het kadaster zelf heeft er niet een groot belang bij om het te doen.

Maar bijvoorbeeld de voedselketen daar zie je wel meer belangen zoals bijvoorbeeld de supermarkten die wel echt klaar zijn dat ze telkens de schappen leeg moeten halen omdat er eerder in de keten iets is mis gegaan bijvoorbeeld.

Dat kan ik me voorstellen inderdaad, overal waar wat meer financiële belangen bij zijn dat men dan wat sneller overstapt of i.i.g. gaat kijken naar de mogelijkheden.

Ja inderdaad, als de supermarkten zeggen dat ze het willen dan gebeurt het over het algemeen wel, want die hebben wel een hoop macht. Bij andere groepen zie je soms weer dat er niet zozeer wat gedaan wordt met blockchain maar meer dat het gebruikt wordt als argument dat het ook anders zou kunnen om de kosten een beetje te drukken.

Daar staat natuurlijk wel tegenover dat een blockchain ook niet zo makkelijk op te zetten is, maar je kan het wellicht gebruiken in de onderhandelingen dat je ook andere opties hebt.

Dat is ook weer een andere manier inderdaad. Nu hebben we het al een tijdje over de blockchain en met name de use cases. Zou je in het kort nog kunnen aangeven wat voor jou een blockchain is met de kern componenten of karakteristieken?

Ja, we zeggen altijd dat in essentie een blockchain een berg aan informatie is op veel verschillende plekken die overal aan elkaar gelijk is. Daar komen dingen bij kijken als validiteit, authenticatie, onwijzigbaarheid en consensus. Dat is kort samengevat denk ik een blockchain.

Juist, dus veel verschillende locaties waar je consistentie tussen kan garanderen.

Ja en we zien het dus echt als een enabling technologie, oftewel een goede blockchain zie je niet eens.

Ja ik begrijp wat je bedoelt, eigenlijk moet het zo goed achter de schermen zijn geregeld zodat het die extra veiligheid en betrouwbaarheid kan waarborgen.

Klopt, ik vind het dan ook niet echt een wondermiddel voor IoT als extra security laag. Juist omdat uiteindelijk hou je dat die apparaten de zwakke schakel zijn voor een blockchain, en kom je toch terug op garbage in is garbage out. Die apparaten zijn gewoon nou eenmaal kwetsbaar en dat lost de blockchain niet op. Het is wel zo dat wat er op die blockchain staat, dat is beter beveiligd dan in de huidige situatie met een gecentraliseerd systeem. Fraude in de blockchain is dus wat lastiger omdat je de gegevens niet meer kunt aanpassen, aan de andere kant als je met de gegevens kunt rommelen op die apparaten dan is het nog steeds onveilig. Dus wat betreft alle problemen die het IoT gaat opleveren dan heeft blockchain daar nog geen antwoord op.

Dat snap ik inderdaad. Wat je zelf al stelt is dat de blockchain die informatie niet kan valideren. Daar zullen we zo nog wel op terug komen. Eerst nog even terug naar die consensus algoritmes, zoals je al stelde staan die wel centraal voor een blockchain. Ben je toevallig bekend met het algoritme Paxos?

Nou niet echt nee. Ik weet dat in de praktijk veel gebruik wordt gemaakt van proof-of-work middels ethereum, alleen binnen een bedrijfsomgeving is dat een beetje stom. Dan is het advies ook vaak om dat op een andere manier te doen zoals wellicht hyperledger of multichain. Zo wordt er dan vaak gewerkt binnen zo'n netwerk met een lijst van vertrouwde nodes, maar dat doen private networks over het algemeen.

Precies, als je weet wie er in het netwerk zit en hun kan vertrouwen hoef je geen moeilijke mechanismes zoals proof-of-work te gebruiken om te bewijzen dat jij iets mag uitvoeren.

Juist inderdaad, intussen zie je al een hoop varianten met proof-of-stake, proof-of-space, proof-of-time, proof-of-possession en weet ik veel wat allemaal.

Klopt, er zijn een hoop varianten en alles heeft zijn voor- en nadelen.

De kern is eigenlijk dat je een soort random selectie moet doen. Maar een random selectie in een gedistribueerd netwerk waar ook een hoop kwaadwillende partijen deelnemen is een grote uitdaging. Maar in een gesloten netwerk kan je over het algemeen die kwaadwillende partijen al uitsluiten. Dan wordt het al wel een iets ander verhaal, desondanks moet je wel in zekere mate tolerant zijn voor het geval iemand toch besluit iets verkeerd te doen. Een mooie anekdote daarover over de Internet Service Providers, toen bleek dat een deel van het internet verkeer gewoon gestolen werd. Daar bestond ook wel een zekere vorm van vertrouwen binnen dat netwerk, maar bleek dat daar heel makkelijk iemand tussen kon zitten en zei stuur al het verkeer maar naar mij waar vervolgens niemand iets van zag. Dus netwerken met volledig vertrouwen zijn wat dat betreft alsnog vrij gevaarlijk.

Juist inderdaad, daar zullen nog een hoop haken en ogen bij komen kijken. Dan wil ik ook nog even een kleine stap maken naar de cybersecurity kant en de machine learning die gebruikt wordt. Heb je ervaring met machine learning?
Ja zeker, alleen ik heb het idee dat wat we nu machine learning noemen, dat noemden we vroeger gewoon statistiek. Mensen vergeten dat als je een machine iets leert, je alsnog een bepaalde error in en afhankelijk van hoe je traint creëer je dezelfde bias als degene die de informatie kiest wat erin komt. Als een mens een bias heeft en bepaalde data classificeert zal die machine vervolgens dezelfde fouten blijven maken.
Daar komt toch weer hetzelfde terug van garbage in is garbage out.
Ja, daarom heb ik ook zoiets van allemaal heel mooi dat machine learning. Maar je ziet altijd dat de mens toch weer de zwakste schakel is en je toch nodig hebt al is het maar om die machine te leren en de algoritmes opstellen en trainen.
Ik kan me voorstellen inderdaad dat we daar nog lang niet zover mee zijn dat we kunnen garanderen dat die machines dat zelf kunnen.
Ja, en de AI is volgens mij nog niet zo intelligent dat hij zichzelf van alles kan leren.
Dat zal vast nog wel wat tijd nodig hebben.
Het is vooral een middel denk ik om dingen sneller te doen. Kijk de mens maakt fouten, een machine zal dan dezelfde fouten maken, alleen een stuk sneller.
Ja dat kan ik me wel voorstellen, maar goed binnen cybersecurity kunnen ze wel weer bijvoorbeeld dingen die niet horen snel detecteren. Maar goed, zoals je net al zei dat de blockchain binnen zo'n gedistribueerd netwerk niet de validatie kan doen op de gegevens. Binnen dit onderzoek kijk ik eigenlijk naar een scenario dat je die verbondenheid hebt en verschillende apparaten met een consensus protocol hebt verbonden. Die waardes zullen ze niet valideren maar de vraag is of die apparaten bijvoorbeeld wel kunnen zien of er geklooid is met een van die machines. Kan je voorstellen wat ik bedoel?
Nou, in een blockchain zie je dat nogal makkelijk, als er eentje afwijkt van de rest zien ze gelijk het verschil en moet hij de waarden van de andere weer overnemen of je krijgt een splitsing in het netwerk.
Precies, maar dan spreek je van de waardes of die afwijken.
Inderdaad, dat er dus gegevens op een blockchain staan waar iemand probeert zijn eigen blockchain te updaten en veranderen. Als de rest dat niet doet, dan zien ze dat gelijk.
Ja dat punt snap ik, als ze niet meer consistent zijn, dan zien ze dat heel snel.
Dat zie je dan meteen inderdaad, alleen niet als het zou lukken om het hele netwerk te veranderen, maar dat is een stuk lastiger.
Uiteraard, maar even wat anders, ik kan me voorstellen dat zo'n node informatie kan versturen en het netwerk niet ziet dat hij verkeerde informatie verstuurt.
Klopt, zolang die informatie voldoet aan de voorwaarden die opgesteld zijn kan dat prima ook verkeerde informatie zijn en zal het hele netwerk dat overnemen.
Precies, dan is wel de vraag of er op een andere manier aan die sensor of node gezien kan worden dat hij veranderd is en dus niet meer betrouwbaar.
Dat ga je denk ik niet met een blockchain vaststellen. Dat kan je wellicht wel op het apparaat zelf vaststellen dat er op een bepaald moment activiteiten geweest zijn, maar de blockchain kan dat niet zien.
Oké, dat is eigenlijk de vraag die naar voren kwam met dit onderzoek. Met name als je dus kijkt inderdaad naar grote netwerken waar die waarden niet meer te controleren zijn en eigenlijk het aantal apparaten ook dusdanig groot is dat je dat niet meer kunt beveiligen. Dan zul je op een andere manier moeten kijken hoe je dat kan beveiligen en wellicht is dat mogelijk door te kijken of het netwerk kan garanderen dat er niet met de nodes geklooid is. Als je weet dat er niets raars is gebeurd met die machine, dan kan je wellicht de waardes vertrouwen ondanks dat je dat niet kan controleren. Dat is dus een beetje het idee, wat vind je daarvan?
Dat klinkt interessant, ik denk alleen dat het erg lastig is dat met een blockchain te borgen. Simpelweg omdat op zo'n scanner naast de blockchain nog iets als operating software is dat eerst opstart. Ik vraag me af of een aanvaller dat niet gewoon kan aanvallen zonder dat de blockchain dat kan zien. Je kan het operating system weer niet op een blockchain laten draaien bijvoorbeeld.
Klopt, daar ben ik het zeker mee eens. Uiteraard is een tweede vraag natuurlijk hoe je dat kunt maken, er zijn wel indicaties die denk ik het wel mogelijk maken. Ik kan me wel voorstellen dat er zo meteen situaties

zijn waar we zoiets nou eenmaal nodig hebben als het inderdaad een hogere mate van betrouwbaarheid zou kunnen creëren.
Ja uiteindelijk zou je hashes kunnen laten maken van zijn gehele toestand waardoor als er iets verandert in zijn toestand die hash weer anders is en de blockchain dat kan zien. Een aanvaller zou dat wellicht niet kunnen vermommen want er moet nou eenmaal wel iets anders zijn aan het apparaat.
Nou dat is eigenlijk precies waar ik tijdens dit onderzoek ook op uit kwam. Stel je zou dat binnen een privaat netwerk doen waar apparaten zich al identificeren met bijvoorbeeld IPV6 o.i.d. Je kunt daarnaast niet definiëren wat die apparaten allemaal mogen en horen te doen, want dat is niet bij te houden in een groot netwerk. Even los van hoeveel het kost en je het precies zou inrichten, als die apparaten eigenlijk aan het netwerk kunnen tonen dat er niets aan hunzelf veranderd is, dan kunnen we vertrouwen dat hij goed werkt. Zou dat dan een betere beveiliging creëren.
Nou dat klinkt zeker aardig, maar ik ken nog geen partijen die daar naar kijken of dat proberen op te zetten. Los van de vraag of het überhaupt al mogelijk is. Maar op de blockchain zijn we nu de gegevens ook al aan het hashen en vergelijken, als er ook maar een spatie anders is dan ziet het netwerk dat al. Op dezelfde wijze kan je misschien de consistentie van dat apparaat of misschien de meest cruciale dingen pakken, waarna je er een hash van genereert en op een blockchain zet. Als er dan iets verandert dat je meteen ziet dat er iets niet goed zit. Dan krijg je wel de vraag wat wil je daar weer allemaal in opnemen en is dat te doen voor een groot netwerk en in hoeverre draagt dat bij aan de gehele veiligheid.
Daar heb je zeker gelijk in. Maar in het kort geef je wel aan dat je er een mogelijkheid in ziet. Wellicht dat het heel ingewikkeld is of duur etc., maar daar is nu uiteraard geen concreet beeld op te vormen.
Inderdaad, en sowieso gebeuren er veel dingen op dat apparaat zoals updates en zo en hoe ga je daar dan weer mee om. Aan de andere kant weet je dan weer dat er iets gaat veranderen en is dat weer te managen. Je kan ook nog controleren als je een update doet of iedereen dat doet en of die dan zelfs de juiste hash genereren die je verwacht of zo. Dus daar zitten zeker nog wel uitdagingen in, maar er zijn nog geen partijen die dat aan het doen zijn, dus het is nu heel moeilijk om te stellen in hoeverre dat effectief is en zo.
Zeker, dit onderzoek is daarom ook erg theoretisch. Omdat zoiets nog niet bestaat kan je de effectiviteit en zo ook niet onderzoeken. Vandaar dat ik juist met veel experts van verschillende achtergronden wil sparren om te kijken wat die ervan vinden.
Een van de eerste stappen denk ik sowieso al is dat je in een consensus protocol kunt opnemen dat er een aantal voorwaarden zijn waar iedere machine aan moet voldoen om überhaupt mee te doen. Zoals je net al aangaf met het voorbeeld van Windows XP, zou je het netwerk al beter beveiligen door te stellen dat je alleen maar mag deelnemen als je up-to-date bent met je security standaarden.
Dat is waar, zolang je daar geen valse signalen over kan krijgen, maar inderdaad dat zal al een mate van extra veiligheid geven. Dus met bepaalde mate zal het wel werken, zolang een apparaat niet kan liegen dat hij op Windows 10 draait maar eigenlijk op Windows XP bijvoorbeeld.
Klopt, dan blijft weer de vraag hoe ver wil je gaan en hoe beveiligd wil je worden.
Maar het voorbeeld wat je net gaf over die sensoren, ik kan me voorstellen dat het wat makkelijker is om die consistentie daarvan te borgen.
Inderdaad, ik heb ook iemand gesproken die vertelde me over bijvoorbeeld powergrids dat er een hoop sensoren zijn over het hele land. Maar als iemand daar fysiek of digitaal aan gaat klooien, dan hebben we daar geen idee van. Hiermee zou je dat wellicht al ondervangen.
Ik denk inderdaad dat je wel gelijk hebt dat de blockchain niet helpt met de gegevens controleren maar je op die manier weer een focus kan leggen op de individuele apparaten waar de gegevens vandaan komen.
Inderdaad, hier kunnen we zeker nog langer over praten.
Ik denk dat we het afgelopen uur wel stappen hebben gezet en ik vind het idee wel erg interessant, daar ga ik zelf ook nog even naar kijken.
Zeker, hartelijk bedankt voor jouw input. Ik zal uiteraard dit gesprek volledig uittypen en jou toesturen ter controle dat we dat ook inderdaad besproken hebben.
Oké, en ik ben ook wel benieuwd naar jouw eindverslag. Ik vond het een interessant gesprek. Veel succes nog met jouw onderzoek.
Hartelijk bedankt, dat zal ik zeker doen. We houden contact.

Interview 5

Date: 29-10-2018

Introductie

..

Om kort door te gaan op een ander onderwerp. Namelijk het Internet of Things, een veel besproken onderwerp wellicht afgelopen jaren. Zou je in het kort kunnen aangeven wat je daarvan hebt meegekregen en wat jouw kennis en expertise hierin is?

Nou IoT is totaal niet mijn expertise gebied. Ik kan wel een antwoord geven. Wat ik ervan weet is dat het een container begrip is, en dus veel dingen kan zijn. Het wordt volgens mij vaak geassocieerd met kleine devices, met weinig capaciteit die met elkaar gelinkt zijn. Dat zou mijn korte definitie zijn.

Precies, dat is zeker waar. Belangrijk is denk ik ook dat die kleine apparaten allemaal ook met elkaar verbonden zijn en kunnen communiceren. Ze zullen allemaal data uitwisselen en hier kan dan ook weer veel analyse op gedaan worden. Dan neem ik aan dat Industrial Internet of Things ook geen bekend begrip is?

Nee, maar ik neem aan dat het een verlengde daarvan is.

Ja, dat klopt uiteraard zie je dat daar ook steeds meer met sensoren etc. gewerkt wordt om alles efficiënter te maken. Een belangrijk verschil is wel dat dit dus een netwerk is waar niet iedereen zomaar bij mag komen en de apparaten met elkaar meer onderling verbonden worden en communiceren en ook beslissingen en handelingen kunnen uitvoeren.

Oké, maar even hardop denkend vraag ik me af wat dan het vernieuwende is van het Internet of Things. Kleine apparaten konden al heel lang met elkaar kletsen. Waar het denk ik om gaat als je die apparaten allemaal met elkaar connect dat je ook een grotere data stroom krijgt. Uiteraard dan ook de vraag, hoe wordt deze data verwerkt met name als je naar een decentrale omgeving kijkt. Dan loop je tegen beperkingen aan van die devices in de vorm van te weinig opslag en processor capaciteit hebben. Dat je dus eigenlijk het slachtoffer bent van je eigen succes.

Juist, dat je heel veel kan maar het nog niet kan verwerken en coördineren.

Ja, daar kan ik me wel iets van voorstellen.

Die kleine apparaten zullen daar inderdaad op het moment nog te weinig kracht voor hebben. Daarnaast denk ik dat dit ook consequenties heeft op de veiligheid van die netwerken.

Zeker, dat is natuurlijk de droom geweest van iedere hacker dat die apparaten zomaar worden verbonden. Een van de dingen hierover die ik interessant vind is wireless security. Als ik thuis een pineapple heb staan (een grote antenne) dan kan je de hele buurt auditen maar je kunt er ook andere dingen mee doen.

Ja dat kan wellicht goedschiks of kwaadschiks.

Inderdaad, en zo'n klein device kan dan niet op tegen de antenne van 2 meter. Die kleine devices kan je dan gewoon wegdrukken of overnemen.

Ja inderdaad, daarmee heb je eigenlijk ook al de volgende vraag beantwoord namelijk wat dan de consequenties zijn. Voor industriële netwerken waarin veel apparaten worden verbonden komen security vragen wat sterker terug. Dit in tegenstelling tot IoT waarin consumenten toch wel sterk de neiging hebben alles maar te verbinden zonder erbij na te denken. Met name de connectie van zo'n netwerk ook in industrie brengt wel met zich mee dat je het onveiliger maakt.

Ja, aan de andere kant is het uiteraard een afweging. Als je bijvoorbeeld als bank zijnde je primaire processen zoals de betaalstraat van je klanten een soort IoT structuur van maakt en dus kwetsbaar maakt, zo'n stap zal een bank nooit nemen. Dus uiteindelijk komt het er een beetje op neer wat het risico profiel is van zo'n omgeving. Als het gaat om medewerker gegevens die een gebouw binnen komen, dan maakt het niet uit als dat een keer een dag eruit ligt omdat iemand dat gehackt heeft.

Daar heb je zeker gelijk in. Ik kan me ook voorstellen dat het ervan af hangt hoe ver een hacker kan komen als er een simpel device gehackt wordt en welke gegevens hij kan bereiken.

Ja en vooral de vraag wat zijn de consequenties daarvan. Voor degene die eigendom heeft van dat apparaat.

Jazeker, duidelijk. Laten we nu doorgaan met het onderwerp cybersecurity. Je gaf net al aan dat je een tijdje bij de hebt gewerkt.

Ja dat klopt.

Zou je in het kort kunnen aangeven wat je ervaring is met cybersecurity?

Nou dat is eigenlijk ook zo'n container begrip. Dat is al lastig te definiëren. Dan kom je vaak uit op dat netwerken veiliger moeten worden en zo. Maar het is vele malen breder dan dat. Mijn rol toentertijd was in het Intelligence team. Dit betekent dat we vooral moesten kijken naar wat gebeurt er nou in de buitenwereld. Dit zijn publieke bronnen en minder publieke bronnen. Vervolgens kijken of we daar informatie uit kunnen halen dat duidt op dreigingen voor ons of voor andere bedrijven. Bijvoorbeeld of andere bedrijven al worden aangevallen, hoe gaat dat dan en verwachten we dat dan ook bij ons. Dat was veel meer informatie verzamelen en analyseren, threat intelligence werd dat ook genoemd. Daarnaast heb je binnen cybersecurity een hoop andere vlakken zoals netwerken beveiligen maar is er ook een snijvlak tussen security en cybersecurity. Bij cybersecurity zal je veel meer kijken naar de volledige en met name externe keten. Lockheed Martin heeft ook zo'n model gemaakt waar is gekeken vanuit de aanvaller perspectief. Wat gebeurt er nou eigenlijk en waar is de aanvaller het om te doen, welke informatie in welke stappen kan waardevol zijn voor de aanvaller.

Oké, de cyber kill chain van Lockheed Martin bedoel je toch?

Juist, die inderdaad.

Daar keken jullie dus toen inderdaad ook naar, dus met de gedachtegang hoe een aanval eruit ziet en wat een aanvaller ermee kan.

Juist, het woord om mensen bang te maken is Advanced Persistent Threat (APT) aanvallen. Hier hebben we dan een aantal aanvallen van in kaart gebracht, maar dan blijkt dat ze helemaal niet zo advanced zijn. Het bleken vooral simpele tools te zijn en met name de oorzaak was dat de firewall niet helemaal goed werkte bijvoorbeeld. Cybersecurity is dus een breed begrip maar ik merkte toen wel dat het nog redelijk in de kinderschoenen stond.

Ja precies, dit geeft wel een duidelijk beeld inderdaad. Zelf heb ik uiteraard vooral onderzoek gedaan naar de theorie en online documenten. Dan kom ik eigenlijk ook tot dezelfde conclusie. Vaak merk je dat we veel maatregelen en technieken om ons beter te beschermen al wel hebben. Echter het probleem is dat we het vaak niet updaten of dingen überhaupt niet toepassen, dan maak je jezelf op den duur uiteraard onveilig. Binnen grote netwerken die op het moment draaien bij bijvoorbeeld civiele infrastructuren denk ik dat je wel kunt stellen dat deze erg oud zijn voor cyber begrippen. Uiteraard dit updaten zal lastig zijn en geld kosten maar goed, dat heeft weer consequenties.

Juist, en de zwakste schakel blijkt altijd de mens te zijn. Bij alle bedrijven waar wij toen contact mee hadden bleek dat zo te zijn. Als je bijvoorbeeld gewoon 50.000 phishing mails uitstuurt, is er altijd wel eentje die klikt en dan ben je binnen. Vooral het menselijke aspect van cybersecurity is denk ik een groot probleem.

Ja, dat probleem wordt nu alleen maar groter denk ik. Als achter de schermen het netwerk alleen maar groter wordt, en je kan via elk component binnenkomen, is het lastiger dit te beveiligen. Met name als die componenten te beïnvloeden zijn door mensen of medewerkers die niet precies weten wat de gevolgen zijn en verkeerde dingen aanklikken heb je al een probleem uiteraard.

Ja.

Oké, tot zover genoeg over cybersecurity, dan wil ik doorgaan naar blockchain technologie. Daar doe je uiteraard een hoop mee op dit moment. Zou je kunnen aangeven wat je zelf ziet en wat de karakteristieken zijn van een blockchain.

Je bent een van de weinigen die die vraag stelt, maar ik denk dat dat een goede vraag is.

Ik zal alleen proberen het in het kort te beantwoorden. Blockchain is niets meer dan een technologie, een vorm van database. Blockchain technologie lost 1 enkel probleem op, en dat probleem is hoe kun je in een groep van mensen die elkaar niet kennen, toch consensus bereiken. Voor blockchain technologie lag die vraag er ook al en konden we die beantwoorden zolang die groep van mensen bekend was en beperkt tot een vaste set/aantal. Echter een onbeperkt aantal mensen die deel kon nemen om consensus te bereiken over die database of ledger kon niet. Blockchain heeft een voorstel gedaan voor een oplossing. Helemaal opgelost wil ik namelijk niet zeggen, er zijn nog genoeg issues met blockchain namelijk. In mijn optiek is dat de essentie van blockchain.

Precies, en zoals je al aangeeft is het een oplossing maar zijn er weer verschillende varianten en mogelijkheden van gemaakt die allemaal verschillende voor- en nadelen hebben.

Ja en blockchain is ook meer een set aan technieken die bij elkaar zijn gehaald wat bij elkaar tot een ander inzicht/oplossing heeft geleid.

Oké, en welke karakteristieken en componenten zie je dan essentieel binnen een blockchain? Je geeft net als bijvoorbeeld consensus, zijn er nog een aantal die je nodig hebt omdat je anders geen blokchain hebt?
Nou het is uiteindelijk allemaal gebouwd rond het consensus algoritme. Daarnaast worden er allerlei technieken toegevoegd, publieke en private sleutels en hashes, maar daar is niets nieuws aan.
Jazeker, en het gedistribueerde aspect zal er uiteraard ook wel voor nodig zijn zoals al eerder aangegeven. Hashes en dergelijke zullen wellicht niet altijd nodig zijn bij elke vorm van blockchain, zolang je maar consensus bereikt binnen de groep.
Nou dat weet ik niet zeker, die hashes heb je namelijk wel nodig. Namelijk als je een rij aan blokken achter elkaar hebt, en er ontstaat een fork, dan moet je wel weten vanaf welk punt dat ontstaan is. Als je niet al die hashes hebt verzameld kan je op een willekeurig punt forks creëren oftewel de history data aanpassen. Die cryptografie is denk ik wel een vereiste daarvoor.
Oké, en als er in een scenario binnen een netwerk consensus wordt bereikt via een consensus algoritme en dit wordt opgeslagen op alle ledgers, inclusief data wanneer dit is opgeslagen en aangepast, en we vervolgens daarop volgende waardes precies op dezelfde manier opslaan. Dan vraag ik me af of je dan eigenlijk al zonder hashes dezelfde uitkomst kan bereiken. Namelijk als er iets aangepast wordt in de historie kan je dat ook zien en dan zullen de andere ledgers de juiste waarde nog steeds kunnen vinden.
Nou hier doe je een aanname over de tijd en dat die tijd op iedere node hetzelfde is. Als je bijvoorbeeld kijkt naar het Bitcoin netwerk, dan is dat niet zo. De tijden worden wel gesynchroniseerd, maar dan wordt het gemiddelde genomen van alle connected nodes. Het kan namelijk ook zijn dat blokken een hoger bloknummer hebben, dus later in de tijd worden gegenereerd, maar een timestamp hebben die eerder ligt dan het vorige block. Dit omdat die klokken niet helemaal gelijk lopen, dus die aanname in de tijd kan je niet zomaar nemen.
Oké, dat begrijp ik inderdaad. Dit komt volgens mij voort uit het artikel Time, Clocks, and the Ordering of Events in a Distributed System van Lamport, klopt dat?
Nee, dit is gewoon hoe het Bitcoin protocol werkt. Sowieso aannames over tijd in gedistribueerde systemen lopen vaak niet goed.
Omdat die apparaten dus niet altijd dezelfde tijd hebben en berichten ook later aankomen neem ik aan.
Ja klopt.
Oké, tot zover duidelijk. Zojuist gaf je al aan dat consensus algoritmes centraal staan in de blockchain, maar dat we al voor de blockchain dergelijke algoritmes hadden. Een van die consensus algoritmes is Paxos, ben je bekend met Paxos?
Ja, uiteraard ben ik het tegengekomen en heb ik het doorgelezen. Het valt voor mij onder de Byzantine Fault tolerant type consensus algoritmes. Dit tegenover de proof-of-work en proof-of-stake, meer Nakamoto type consensus algoritmes.
Ja inderdaad, daar heb ik voor dit onderzoek dan ook iets dieper naar gekeken. Met name omdat in dit consensus algoritme wellicht niet een hoop moeilijke en zware technieken nodig zijn. Een van de requirements is echter wel dat iedereen bekend is binnen het netwerk en kunt vertrouwen.
Nou, je moet twee delen vertrouwen volgens mij.
Wat bedoel je daarmee precies?
Nou, het staat me bij dat je binnen het Paxos protocol 2/3 van de deelnemers moet kunnen vertrouwen en dat dan het protocol nog goed werkt. Als dat niet zo is en er zijn meer nodes die niet eerlijk zijn, dan zou het protocol niet meer werken.
Ja, daar heb je gelijk in. Je moet uiteraard een netwerk hebben dat je kunt vertrouwen, en als een klein deel malicious is kan je die nog wel compenseren of eruit gooien, maar dat kan maar tot een bepaald percentage uiteraard.
Ja, inderdaad.
Als we hier iets verder op in gaan, dan moet je je voorstellen dat we een netwerk hebben van 4 nodes waarop Paxos kan draaien en dus een gedistribueerde ledger hebben en BFT zijn. Dan is eigenlijk de vraag of die nodes in dat netwerk van elkaar bepaalde gegevens kunnen zien binnen het consensus protocol om de betrouwbaarheid te verhogen. Met andere woorden, kunnen de nodes zien onder welke omstandigheden een node bepaalde handelingen en beslissingen neemt?
Ik begrijp de vraag niet helemaal. Dus we hebben een Paxos protocol?

Ja, we hebben 4 verschillende nodes. Dit zijn geen simpele camera's maar geavanceerde computers. Die zijn met dat Paxos protocol verbonden en dan is eigenlijk de vraag wat zo'n node van andere in het netwerk kunnen waarnemen. Wellicht kan er zoiets opgenomen worden in het protocol, er kan bijvoorbeeld al wel opgenomen worden dat de nodes zichzelf moeten identificeren.
Ik ken Paxos niet helemaal uit mijn hoofd, maar je zou verwachten dat de identiteit van de nodes bekend is. Op het moment dat ik iets teken met mijn private sleutel, dan kunnen de andere drie nodes zien dat ik dat ben geweest. Maar de vraag die je stelde wat kunnen ze dan nog meer zien. Het nadeel van Paxos is dat er ontzettend veel berichten verkeer in moet plaatsvinden. Het staat me bij iets van 9 per transactie voordat er consensus wordt bereikt. Dat zal overigens wel te zien zijn en de data waarover consensus moet worden bereikt is uiteraard ook te zien. Volgens mij is dat wel zo'n beetje wat nodes van elkaar zien.
Juist dus die verschillende berichten en uiteraard de data waardes zelf. Overigens wat je al zei is dat wellicht ook de reden dat er veel naar andere mogelijkheden dan Paxos wordt gekeken omdat er misschien veel verkeer in nodig is. Hier gaan we zo nog iets verder op door, maar eerst even een kleine tussenstap over een ander onderwerp. Vandaar de vraag heb je ergens al ervaring met machine learning of iets over gehoord?
Ik heb werkelijk geen idee, alhoewel ik me er uiteraard wel een voorstelling van kan maken.
Geen probleem, dat is wel makkelijk uiteraard.
Ik ben wel benieuwd eigenlijk vanwaar je vraag over Paxos, want er zijn ook andere protocollen zoals RAFT en Istanbul BFT. Vanwaar Paxos?
Eigenlijk omdat dit onderzoek veel componenten bij elkaar brengt, zoals IoT, cybersecurity en blockchain. Toen mijn onderzoek begon bij blockchain, kwam ik ook al snel tot de conclusie zoals jij al zei overigens, dat consensus toch wel centraal staat. Toen ik hier dieper op in ging en naar de historie hiervan keek, kwam ik op Paxos uit als een van de eerste consensus protocollen voor gedistribueerde netwerken. Het protocol stamt eigenlijk al uit 1989 beschreven door Leslie Lamport. Als je uit gaat van de requirements die daarin gegeven zijn namelijk dat je iedereen in het netwerk moet kennen en kunt vertrouwen en de historie niet kunt aanpassen, dat het dan goed zou werken. Later zijn wellicht een hoop variaties ontstaan die het algoritme wel of niet beter maar wellicht ook moeilijker maken. Daarbij heb ik gekeken waar IIoT netwerken waar alles maar aan elkaar wordt verbonden en vooral gekeken wordt naar de use cases, maar in mindere mate wellicht naar de cybersecurity kant. Dat als je alles met elkaar verbindt je ook een soort kaartenhuis aan het bouwen bent. Deze aspecten bij elkaar genomen, dat dus eigenlijk ruim 20 jaar geleden er al een algoritme bestond die de betrouwbaarheid zou verhogen en het netwerk beter kan beschermen. Nu zijn er inmiddels wel andere technieken met proof-of-work etc. om een netwerk te beschermen, maar dit heeft ook weer nadelen. Daaruit is dus het idee voortgekomen om te kijken of misschien de simpelere versie van 20 jaar geleden, toen ook nog niet veel computerkracht bestond en blijkbaar wel mogelijk was, of dat niet gewoon voldoende is om bepaalde netwerken te beschermen. Het kijken vanuit een security perspectief en dus of die nodes van elkaar kunnen zien of er eentje wordt aangevallen en daarover consensus bereiken wordt naar mijn weten nog niet ergens beschreven. Geeft dit een klein beetje een helder beeld.
Jazeker, ik ben erover aan het nadenken, maar je maakt wel wat grote sprongen in de lijn.
Als je vier machines hebt en eentje wordt aangevallen en komt in het bezit van jouw private sleutel dan kan ik dingen doen. Dan beheer ik jouw computer, maar de rest van de nodes die zien dat niet, die denken op basis van de private sleutel dat jij dat bent.
Ja inderdaad, daar wil ik wel even op aanhaken dat er wel al mogelijkheden zijn volgens mij die dat kunnen. In theorie kan je bijvoorbeeld als node de volledige software status van jouzelf hashen. Als een aanvaller namelijk wil binnendringen of wil aanvallen zal er wellicht toch iets veranderd moeten worden binnen dat apparaat. Als binnen het consensus protocol is opgenomen dat dat apparaat telkens zichzelf moet identificeren maar bijvoorbeeld ook die hash moet laten zien en kan garanderen dat hij nog steeds hetzelfde is, kan je wellicht wel een hogere mate van veiligheid bereiken. Kun je je zoiets voorstellen?
Ja hoor, zoiets kan ik me wel voorstellen. Hier moet ik ook weer even over nadenken, want ik ben nog geen software tegen gekomen die zoiets kan, op cryptografie. Dan zul je dus inderdaad toch een soort hash moeten maken, en als je die hash weet kan je die gewoon injecteren in datgene wat de node verstuurt.
Oké, en anders gezegd in een huidige situatie kan een node zich inderdaad wel identificeren met b.v. IPV6 o.i.d., alleen is dan de vraag als een aanvaller die node dan compleet kan overnemen zal hij er binnen het

netwerk nog steeds hetzelfde uit zien. Eigenlijk als ik naar dit consensus algoritme kijk waar je er vanuit moet gaan dat iedereen te vertrouwen is, moet je dat wel kunnen garanderen.
Misschien zit het er niet zozeer in dat de nodes worden aangevallen, maar zegt het of het protocol in stand blijft als er minder dan een bepaald percentage eerlijk is. Volgens mij is dat het uitgangspunt van BFT protocol. Zolang 66% eerlijk is, kan je ervanuit gaan dat het protocol blijft functioneren.
Ja dat is waar.
Volgens mij probeer je nu iets anders te beschrijven, namelijk dat als er een van de nodes in het netwerk gecompromitteerd is.
Daar komt het inderdaad wel een beetje op neer denk ik, dat je eigenlijk gelijk al ondervangt wanneer een component binnen het netwerk veranderd is. Die 66% klopt inderdaad, maar ja als niemand alarm slaat als 1% anders is en ook niet daarna 2%, dan heeft de aanvaller zo gezegd bijvoorbeeld veel tijd om 34% te halen. In de huidige situatie zie je bij aanvallen volgens mij, dat als een aanvaller binnen een netwerk kan komen, hij al vrij snel zich kan verspreiden. De gedachte hier is dus als je een industrieel netwerk hebt, een privaat netwerk, bijvoorbeeld de haven van Rotterdam of een andere industrie waar een aantal apparaten met elkaar verbonden zijn, dat je eigenlijk al met het protocol dergelijke aanvallen kunt ondervangen. Wellicht dat je daarmee wel een hogere mate van veiligheid kan creëren.
Ja, dat zou zeker kunnen inderdaad, maar wellicht dat je dan wel een hogere mate van complexiteit toevoegt. Dat is over het algemeen nooit gewenst, want als de complexiteit omhoog gaat, wordt het risico ook groter. In dit geval probeer je de compromittatie van de node te ondervangen door het te stoppen in het consensus algoritme. Ik kan me ook voorstellen dat je dit wel kan gebruiken in een soort security techniek en niet in de consensus. Dat je dus eigenlijk een soort tweede laag maakt. Als de node wordt gecomprimeerd dan krijgen we daar dus gelijk een melding van maar het consensus algoritme blijft gewoon draaien. Dit maakt namelijk dan ook niet uit, want die zou sowieso goed moeten blijven werken omdat we nog meer dan 66% honest nodes hebben.
Daar heb je inderdaad gelijk in echter hoe kan je dan garanderen dat er wel een melding komt dat een van de nodes aangevallen wordt als de rest daar dan niet naar hoeft te kijken. Binnen het consensus algoritme zou je dat als het ware moeten garanderen.
Ja maar je beperkt je daardoor ook weer tot het consensus algoritme zelf. Daarvan ben je dan ook afhankelijk, op het moment dat het consensus algoritme niet werkt of je kijkt er bijvoorbeeld buiten, dan zien ze het ook niet. Maar je kan bijvoorbeeld misschien wel naar netflow data kijken of de machine zelf. Wellicht kan je in jouw netwerk protocol wel opnemen, maak inderdaad maar iedere dag een hash van het apparaat en vergelijk het maar. Hierdoor kan je wellicht naar andere dingen kijken, dan alleen in het algoritme zelf.
Ik begrijp inderdaad wel wat je daarmee bedoelt, maar als ik het goed begrijp bedoelje dit met de gedachte dat er ergens een cybersecurity afdeling is die dit kan controleren.
Ja, kijk om te proberen security in een consensus protocol te stoppen is hetzelfde op een tafel en een stoel proberen te combineren en er tegelijk op te willen zitten en aan eten.
Ik snap je punt inderdaad, wellicht uiteindelijk blijkt het niet praktisch. Maar goed vandaar ook een beetje dit onderzoek, namelijk zie je vaak dat er veel gekeken wordt naar hoe we die apparaten met elkaar kunnen verbinden maar het cybersecurity perspectief erin wordt vaak vergeten. Vandaar de vraagstelling of we dat nou juist wel in dat protocol kunnen opnemen, zouden we dan een hogere mate van veiligheid creëren. Kijk ik kan me zeker voorstellen dat je het wellicht complexer, duurder of misschien zelfs onpraktischer maakt, maar dat kan ik uiteraard met dit onderzoek niet beantwoorden. Vandaar eigenlijk met een theoretische blik gekeken of dit ten eerste mogelijk is en of er toch een betere veiligheid kan worden bereikt als het netwerk zelf al kan zien dat er iets veranderd is en gelijk ook die node kan afschermen. Nu hebben we het dan ook over 4 nodes, maar wellicht werkt dit hetzelfde als het op 10 nodes of meer draait en je dus kunt stellen dat het netwerk zichzelf in stand kan houden. Dan komt daar nog een vervolg vraag op, maar dat is niet meer onderdeel van dit onderzoek. Als het netwerk op die manier zichzelf in stand kan houden, misschien dat dit dan een oplossing is in grotere netwerken met bijvoorbeeld IoT devices. Als daar minder geavanceerde apparaten alleen maar hun huidige status kunnen aangeven en het netwerk kan zien dat er iets anders is, hoeven ze dat niet zelf te doen maar mogen ze van het netwerk even niet meer mee doen, totdat dit probleem verholpen wordt. Dat is uiteraard nog even verder nagedacht, maar dat geeft misschien weer een iets beter beeld van het huidige onderzoek.

Ja, ik snap het en vind het zeker een leuk idee, ik probeer alleen wat tegen gas te bieden.
Heel graag zelfs uiteraard, hoe meer kritische blikken hoe beter.
Ik denk dat bottomline, zeker als je naar IoT gaat kijken het nog lastig is omdat zo'n Paxos protocol bijvoorbeeld al heel veel capaciteit vraagt van een device. Je blijft maar berichten sturen naar elkaar voordat je het eens bent over een simpele transactie. Als je daar nog meer aan gaat toevoegen, zoals bijvoorbeeld de huidige status, dat gaat nog meer capaciteit vragen en dat hebben IoT devices nog niet. Dat zou mijn voornaamste gedachte zijn over het voorstel.
Ja, dat kan ik me zeker voorstellen. Aan de andere kant als we bedenken dat het Paxos protocol rond het jaar 1990 is beschreven en de meest geavanceerde computers al minder computerkracht hadden dan een huidige smartphone, is het wellicht wel het overwegen waard. Daarnaast stijgt dat ook alleen maar en is iets wellicht nu nog onpraktisch maar over 5 jaar weer helemaal niet.
Je hebt wel een punt, alhoewel ik van mening ben dat je vergelijking niet helemaal op gaat, omdat IoT devices echt nog niet te vergelijken zijn met smartphones. Daarnaast kun je volgens mij bij BFT protocollen niet meer dan 20 devices aan elkaar knopen. In het Istanbul BFT protocol kunnen geloof ik 30 devices gecombineerd worden. Dat zou wel echt een groot probleem zijn in IoT met honderdduizenden devices, maar ook al in industriële netwerken.
Jazeker, dat is overigens een beetje de reden waarom het voor dit onderzoek nog klein gehouden wordt met 4 nodes, die op zich al geavanceerd zijn. Echter heb ik er wel over nagedacht, en ik kan me voorstellen dat als dit concept werkt op een kleine groep je wel verschillende groepen zou kunnen creëren. Bijvoorbeeld die 20 apparaten fungeren als het centrum, die weer met 20 andere kleinere apparaten verbonden zijn en die vervolgens weer met andere apparaten is er weer iets mogelijk. Hier kan je nog veel andere vragen over bedenken en uiteraard ook complexiteit etc. maar als de apparaten in het netwerk met zo'n structuur alleen maar moeten garanderen dat ze zelf niet zijn aangevallen is het wellicht denkbaar.
Ja wellicht krijg je als je weer gaat werken met subsets dat je een soort centraal component weer terug krijgt. Als je in dat principe weer de centrale set aan nodes weet te vinden en je kunt daar iets mee, dan kan je ook gelijk weer de rest onderuit schoppen. Maar goed, dat maakt het niet minder interessant.
Wat dat betreft staat het uiteraard nog maar in de kinderschoenen. We kunnen hier lang over praten, maar als blijkt dat er een kans bestaat dat dit werkt zullen we het toch moeten bouwen en tegen praktische zaken aanlopen.
Jazeker, en zoals net al gezegd zou je het ook als een additionele laag kunnen gebruiken. Cybersecurity wordt sowieso vaak in lagen opgebouwd. Als door een stuk beveiliging in het protocol toe te voegen, voegen we daarbij een additionele laag aan beveiliging toe. Binnen het scenario wat je schets, zoals beperkt aantal devices en bepaalde setting zou dit meer waarde kunnen hebben. Dus in andere woorden, in plaats van Paxos te upgraden naar Paxos+ of Paxos secure kan je het ook anders zien. Volgens mij is de essentie dat de nodes niet alleen overeenkomen over een bepaalde waarde of staat van de database, maar ze komen ook overeen of bereiken consensus over de veiligheid van het netwerk.
Nou dat vind ik inderdaad mooi verwoord. In essentie is dat wel waar je naar kijkt, omdat de waardes binnen zo'n netwerk kunnen niet meer gecontroleerd worden. In tegenstelling tot de waardes van bijvoorbeeld financiële transacties in de Bitcoin die wel gecontroleerd kunnen worden. Binnen een industrieel netwerk zal een machine bijvoorbeeld zeggen dat hij zichzelf naar 100 graden moet brengen en het kan niet gecontroleerd worden of dit wel juist is door andere machines. Met een consensus protocol kunnen ze wel overeen stemmen dat het gaat gebeuren en dit wel opslaan, maar daar creëer je niet een extra veiligheid of dat juist is. Maar als je dus consensus kan bereiken of het netwerk nog veilig is, los van wat die nodes dan allemaal wel niet doen in het netwerk, kan je wellicht toch een hogere mate van veiligheid maken.
Ja inderdaad, dat lijkt me de essentie van wat we net besproken hebben.
Nou dan wil ik je uiteraard bij deze hartelijk bedanken voor alle input. Ik ben er zeker een stukje verder mee gekomen. Zijn er nog dingen die je wilde toevoegen of wilde vragen?
Nou graag gedaan, ik wil nog wel vragen als je scriptie klaar is, mag ik daar dan een kopie van?
Jazeker, sowieso zal ik dit gesprek volledig uittypen en naar je toe sturen. Dan heb je uiteraard de mogelijkheid om aan te geven of er dingen zijn die je er liever niet in hebt uiteraard. De transcripties zullen geanonimiseerd in mijn eindverslag komen. Uiteraard wel een lijst met namen en functies en

achtergrond van de personen die ik heb gesproken, maar die zijn niet te linken naar welke transcriptie erbij hoort. Mocht je zeggen als je de transcriptie leest dat je het liever helemaal niet terug ziet in de publieke versie, dan is er nog de mogelijkheid dat het alleen naar mijn begeleiders gaat en er volgens niks meer mee gebeurt. Als laatste uiteraard als het verslag helemaal klaar is stuur ik het graag op naar iedereen die het in wil zien, te beginnen bij iedereen die heeft meegeholpen middels een interview.
Nou ik ben heel benieuwd. Een interessant onderwerp en ik vond het ook een leuk gesprek. Ook eens iemand die het van een andere kant bekijkt, en ik ben heel erg benieuwd naar je scriptie.
Dat is erg leuk om te horen, nogmaals hartelijk bedankt voor je tijd en je zult zeker nog van me horen.
Graag gedaan en tot ziens!

Interview 6

Date: 31-10-2018

Introduction

..

OK, well as I said this research is also focusing on how you could use blockchain technology in Distributed Networks, but mainly how this can be used to better secure the network. Could you tell me in your own words what you think is IoT and your experience with it?
Let me think of a short definition of it. We have on the one side a third Industrial Revolution where the internet came up and made it possible to send email and other documents much faster etc. On the other side we had the operational technology (OT) where machines got part of the production processes and got automated. So the main goal would be to have a high security and continuity features and machines wouldn't break down, because that would lead to high costs. So we had the two worlds of IT and OT, I think we're now getting in the fourth Industrial Revolution where those two worlds are getting combined into the IoT. So now we have the possibility that we have the physical words, the things, working around and then we have the platform tier were we can gather data, do data analytics etc. Then also we have the enterprise tier were we have all the ERP systems and production systems, basically all the systems that we tried to automate in the third Industrial revolution. Now we have the possibility with the IoT that the fusion of getting data from the physical world and gather it and analyze it. Out of these analyses we get much deeper insight into what's going on in my production, but also what's going on in the streets, what's going on in the offices and everything. Based on that we can make better decisions and can even run machine learning algorithms and automate, improve and support more and more. So this is kind of the IoT, the fusion of the internet with the operational technologies that were built in the third Industrial Revolution. Based on the fusion, new things are evolving, innovations are possible. In the oil for example, data is getting more and more important, because based on that I can make better decisions.
Yes, I understand you can do big data analyses on the data gathered from all different devices.
Yes, so based on the devices I can gather more data, I can get a deeper insight into what's going on in my business or operational environment. Based on this deeper insights I can make better and more precise decisions. For example, yesterday I spoke to a company focusing on big data analytics, based on the data they're gathering, they're making better analytics. They worked with a company that's selling furniture. On the beginning of the year, they prognosed that at the end of the year green sofas and couches will be the trend. They advised the company to develop a few green couches, put it on a fair in October. Based on that the revenue increased a lot, and people indeed really bought those green couches. That's what I mean with better decisions.
Yeah indeed, I can imagine that would be helpful. And of course with your background in the IIoT consortium, you are already talking a lot about IIoT and the benefit in industrial processes with all the machines and sensors you can add to gather more data.
Yes, indeed. The definition I gave was in general IoT, because that would also apply to smart homes, smart watches and so on.
Yes, exactly I understand. It's clear that you know a lot about these subjects and also do a lot of research still. Well let's move on to the subject cybersecurity, what is your experience and expertise in cybersecurity?

Well my focus is not on security, but what I know is that there's a framework, called the security framework. That framework speaks about the goal is to create a trustworthy IoT. Like I said we had OT and their goals like continuity and safety, but on the other site we have the IT where privacy, security and interoperability is a focus. By now combining those IT and OT to IoT, also the security will be an important aspect. When I'm gathering data from my devices on the production site and put it in the platform, there's for example the data privacy aspect. In order to create trustworthiness over this IoT system, I need to also combine the security aspects of both IT and OT. This will require new mechanisms and methods in order to guarantee this trustworthiness. What I also wrote in a paper is about IoT and the integration of the blockchain in the IoT. This includes the question what trustworthiness aspects are guaranteed or supported by the blockchain. We came to the conclusion that blockchain will enable and support the aspects like trustworthiness.
Trustworthiness is a buildup of 5 aspects, this is privacy, security, reliability, safety and resilience. We came to the conclusion that blockchain can enable privacy (although not in the whole part, but in some use cases it can), security and reliability. Safety, that means to ensure that the worker who works with the machines are in a safe environment, blockchain would not be useful. Also resilience, that means that when the system breaks down or has to adapt to new environment, would also not be supported by blockchain. On the other side on privacy, with the private and public key system it can enable more data privacy. It can enable more security by the usage of a distributed system instead of a central server. Of course reliability because the data would always be available, also because of the distributed system. I don't go more into detail, but in the conclusion we also stated that it might be a good field to look into if blockchain can guarantee trustworthiness. Because if you see the news and people say that blockchain is guaranteeing trustworthiness or trust between partners, I think there're other aspects that also need to be considered. It has to be the whole system that can guarantee this trustworthiness.

Yes, in different use cases you have to look at what's suitable.

So considering more into cybersecurity, I looked into cryptography. And as I said in the beginning, with the fusion of IT and OT existing aspects of both have to be combined in order to guarantee a trustworthy IoT system. Cybersecurity is looking at all this different methods to guarantee this trustworthiness over the whole system.

OK, very clear. You're now looking at the blockchain side but you don't have experience with current cybersecurity principles in industrial networks.

No, this is not my focus.

Sure, no problem. Well just hop on to the subject of blockchain, and you already said something about it, but could you in short tell me in your own words what a blockchain is and the characteristics or components are?

OK, yes. So I'll try to structure it in three layers. We have the distributed ledger, that's the principle layer. It provides all the principles that are required to implement concepts. The second layer are the concepts, on this layer we have blockchain tangle, hash graph and so on. Distributed ledger provide the principles for example cryptography. In this cryptography we have hash functions that are used, tree structures and the usage of private and public keys and aspects like zero knowledge proofs that just came up recently. Then we also have game theory, one problem of the game theory that the Distributed Ledger technology is solving, is the Byzantine Generals Problem. Furthermore we have craft theory, so in one concept linked list to describe the blockchain tangle and so on. Then in tangle or IOTA we have mark of chain or Monte Carlo algorithms to kind of decide which transactions to validate. Then we also have another component which is digital economy, for example this is about the double-spending problem and is solved by the bitcoin. That means that a transaction can't be executed twice. Then we have a lot of cryptocurrencies that are one of the first use cases that are enabled by the concept of blockchain. Then we also have networks, that's another component like for example peer-to-peer networks or distributed networks on which the concepts of blockchain are based on, to have not the dependency on 1 central server. This is kind of the principle layer that I described, it are not all the components, there might be more.

Yes, I understand there're much variations.

Yes, and of course if you look at one protocol, we say the third layer is the protocol layer, there we have Bitcoin, Ethereum, IOTA and so on. They are using concepts like blockchain tangle, hash graph and so on. Protocols are implemented and can be used for your system and so on. I don't know if this is enough. I go

more into detail about the blockchain concept. Blockchain is using all these distributed ledger principles and describe what the processes are to get new transactions. So they describe how they will find consensus in this peer-to-peer system. It also describes what cryptography mechanisms and algorithms are used. Then they let the network generate blocks that are connected via hashes to build a one dimensional blockchain. In comparison to tangle that are using a graph that's maybe more dimensional. On this concept layer I define the differences of the different concepts. And on the protocol layer we have the implementations. With every variation of implementations there're different communities of developers that try to further develop it.
Well that's a long story, it's clear you know a lot about blockchain. You already mentioned short the consensus protocol, what does that do in the blockchain?
So the main purpose of consensus algorithms are to find a consensus on a value. We're talking about a peer-to-peer network, so everyone has the same rights and responsibilities. When transactions come into the network, for example 1 bitcoin is transferred from A to B. Now in this network of various peers we need to find an agreement, so that we can say that this transaction is valid. In order to do that, you can use different consensus algorithms to get to this consensus or agreement. When the agreement is found, the transaction is saved in the blockchain and can't be changed anymore. Like I said there're various consensus algorithms like proof-of-work, proof-of-stake, proof-of-lapstime, BFT's and so on.
Yes, to agree on a new value basically. Very clear that you know pretty much everything about the blockchain that you can know. One of the consensus algorithms though is the one that I studied more into detail for this research is the Paxos algorithm. Have you heard of this?
Yes, I've heard of it. I stumbled over it a while ago, but I don't know into detail what it actually is. I think Paxos is used in Hyperledger and Corda, but I'm not sure. I don't know much more into detail.
Well, no problem. You're right indeed, I think they are using variations of Paxos in Hyperledger and Corda. I'll explain a little bit about it, first of all they don't have the proof-of-work and don't really do the validation on the network. The basic assumption is that they can trust everyone in the network. If everyone can be trusted and works how it should, then you can trust the network is still correct. With the proof-of-work you have a system implemented where you can guarantee that it will work even if people are malicious. Paxos has often been looked at, as being a normal fault tolerant consensus algorithm. This means when somebody fails like power outage or a breakdown, then the network will agree that somebody else will take it over. But like I said they don't really look at the values.
OK, but where is it mostly used? Is it more in private networks, or more in public?
Private networks, because one of the requirements is that you know everyone in the network and can trust everyone who's in the network. Nodes however still can fail, can drop, can disconnect and come back but the network would still reach consensus.
OK.
We'll go a little bit more into detail about this later on, but first one aspect I want to ask is: what's your experience with machine learning?
Well at the moment and mostly recent months we're building up knowledge about machine learning and Artificial Intelligence.
Is that when you're gathering data from the different devices and do analytics on that data?
Yes, so at the moment we're mostly creating slides to get main knowledge about the AI. This includes data analytics but also deep learning. Basically we say that AI is divided into artificial and intelligence. Artificial means that something is taken over by something else than a human being, so like a computer and so on. Intelligence is a term not defined yet, but it combines things like thinking, making decisions, being autonomous in a way. In one paper we wrote, we described the features of ML into 7 fields, learning is one feature, predictions, rewarding, detections, optimizations, decision making and inference. By looking at different literatures we took out, or created features to describe what is machine learning and what are the features of machine learning. And based on that, we described these 7 capabilities or features. But in AI we have narrow AI and more general AI. The field of machine learning is part of AI, within machine learning you have deep learning approach, predictive analytics. What I always find important is to differentiate between data analytics and AI. Data analytics I describe as big data that you gather in your data warehouses. With this historical data you run algorithms and do data analytics, then you have the possibility to do descriptive things, so you describe something that is already existing. You do the predictive things, based on the historical things, you

can predict something or find expected behaviors or outcomes. On the other side you do the prescriptive things where you try to forecast outcomes based on the data you have. And AI in my definition is going further than that. For example when you see a robot that is gathering historical data but also real time data and data that's in a certain context and comes from different origins, it will make its own decisions and influence its processes. It's working autonomously like human beings are behaving. To do that, ML algorithms are used, like deep learning for example. Deep learning is using neural networks that are layered on top of each other. Based on this layers it's possible to get deeper insights and more precise predictions about the data I have in my database. Based on this data that I can gather and using the deep learning algorithms I can make decisions that influence my process steps and can make a robot behave for itself. So creating autonomous cars for example that decide by itself. This is a fuzzy differentiation, you can't say this is data analytics and this is AI or ML. But they're differences that we currently try to separate from each other. Now we have AI and more data analytics. On the other side I hear that the experts in the field really don't like the definition of AI because it's more a marketing term to describe a new trend. I believe all the things that are now being deployed were developed in the past, but now we have the power of CPU etc. to also implement it.

Yes.

This is just a side note, but some people also speak about augmented intelligence, that means to use AI to support the person that's working somewhere.

I can imagine.

This is what I meant with narrow AI, it's used and should be used to optimize processes and support workers and so on. The goal is to go to the general AI where AI replaces human beings and everything can work autonomously. Then I would say we're at the definition of AI.

Yes, I can imagine that ML can be used in different fields. One of them is AI, but also more in data analytics and probably more fields. Essentially we're talking about the algorithms that learn about the data. It's good to know that you're already…

One more thought is, but it's just an idea. It would be great that with AI we keep in mind the autonomous assets that are developed and can decide by themselves what data source they're going to use or need to make specific decisions. At the moment we provide them with a data lake and this is an area and amount where the ML algorithms are deployed. On the other side autonomous assets should have the possibility to create its own data source and decide what data it needs to have. Then it needs to be made open to also other data sources. For example autonomous cars, they have the possibility in the morning to access weather conditions or street cams and tell me that we should go half an hour later because the conditions will be better. So the car would tell me based on the data it can gather how to do the trip from house to work.

Yes, currently they already go pretty far because they can see the outside temperature and see when you wake up or at least normally wake up so it will ask you to increase temperature already.

Yes, indeed.

Wow, also a very detailed description about what you think of ML. Now getting back to the industrial networks what we just discussed. Basically this research is about those networks, but not the use cases but the security. Let's imagine we have 4 nodes in the network and create a distributed ledger between those nodes. We use a consensus algorithm, in this case Paxos, to combine the nodes, communicate and agree on certain new values. In this network, like an electricity grid, you know all the machines in the network and it's closed for machines that shouldn't connect to it. Then obviously you need to make sure it keeps running if something fails like breakdowns, but also defend yourself against attackers. If we have such a network could those networks also secure the network as a whole. So instead of just agree on a value, it needs to see who's in the network and determine if they can still trust every node in the network. Can you imagine the scenario that I try to explain?

Yes, so we have 4 nodes, that is for example an industrial system or electricity system. They make decisions decentralized, it looks like autonomous assets, they make their own decisions? These decisions influence the network in total or whatever. Now you say what happens if one gets compromised would it still work?

Well something like that. At the moment we see that more and more machines get connected. This is also due to the fact that people tend to look a lot to the use case and benefits of getting more machines connected. Basically what I'm wondering now is, if you have such a network connected and in this example 4 nodes. They already communicate a lot with each other and their database is synchronized. Although they

do their own tasks individually they broadcast it to the network. Can you imagine that if we include in the protocol that they need to identify themselves including data like their security level for example. Would you maybe increase the security level with it?
Ok, well what I know is used in blockchain. When I send a transaction from A to B, the transaction is broadcasted into the network and then get verified first. The nodes will look if I exist as an account and have enough coins.
Yes, but hold on. The problem in this scenario is a bit different because I don't talk about any coins or cryptocurrency in this network. It's a private network so there's no point of adding coins. All the actions that go through the network like increasing their temperature etc., those values can't be checked on whether or not it should happen. So we have to look at a different network where you can't always verify the actions that are taken in the network. What I try to discuss now is that maybe the network can verify that the machine proposing the new value is still legitimate and trustworthy.
OK, I understand. So it's not possible to verify the actions. The question is how to still verify that this machine is still trustworthy. Well I haven't heard of anything like this, but what I can imagine is a trustworthy level. That based on maybe past behavior etc. But when you cannot verify what the machine is supposed to do, it's hard to determine that he did good in the past also. So you need to observe this machine over time and if the behavior would be beneficial for the whole system or not. Basically when a machine needs to verify it will check, "did this machine in the past support us or not". If I think about multi agent systems, then the agent looks at the other agents and I can calculate based on my data that they supported me in the past so you have a certain trustworthy score. Then I can also ask the other agents and based on that I can decide to work with the node or not. I think you will need more historical data though to make a trustworthy score.
Maybe you also need to send back and forth some messages, based on this messages I can check something as well. Like we do in the normal world, when I meet someone new, I try to speak with him and try to get a feeling if he's trustworthy or not and then decide to do business with him or not. If I for example know someone for a long time, and thus have some historical data it makes it easier. I think in the system what you explained something like this will be necessary to decide if I can trust it or not.
Yes, it's funny that you're saying trustworthy score because that's how I called it myself as well. So indeed it will kind of look the way you say, although I'm not sure if you need historical data. Of course I think it's better if you can compare as much as possible, but maybe at the beginning you can start with simple data. This could be the identification of the node and the current safety standard they have implemented. Also at the next level, they can show that they're not compromised.
So the question or challenge is to make this identification possible. You need to have a central party that you can trust that gathers all the identifications that are currently working in the network.
Well, I can imagine that you don't need to do that centralized. I can imagine that the network in general knows that, so they all know who should be in the network. They can reach consensus on who can be trusted or not.
OK, yes. When you have such a distributed network we can have a decentralized party. But if we talk about a blockchain where everyone in the network can trust each other, I don't know if we really need then something like that. If the basic is that the nodes trust each other.
You mean that you don't need any other security features.
Yes, then you don't need anything. Why would you use a trustworthiness score if you can trust everyone.
Well, good point. But you see with some of the recent cyberattacks that happen on a network. In the network the nodes all trust each other and are connected, but when an attacker can infiltrate in one of the nodes, like a simple component. Then it can enter the whole network because it's already in and the rest trusts each other. If so, then the attacker can infiltrate the whole network and do much damage.
OK, then why isn't the principle that you don't trust each other.
Yes, well I understand what you mean. Maybe you're right and you can say that they still have to verify that they can still trust each other. This is obviously very theoretical, but maybe then you don’t need very expensive mechanisms to keep the network safe. The idea is that you have a "simple" form of connectivity and they communicate via a consensus protocol. The nodes can identify themselves, so you have a first version of trust, but you still want to see when you can't trust his actions anymore.

OK, so then you have two points. At the one side you have the basic principle that you don't trust each other and can develop mechanisms to enable transactions between the parties who don't trust each other. On the other side you have a network where the basic principle is that we all trust each other, but we need to secure this network from outside attacks. For that you need security mechanisms that secure the network itself like a firewall around it that makes it impossible to go in this network. So I imagine we have a fortress with people inside it and the wall around it protects the people from outside attackers. This fort will still have a door that enables the entrance but it's guarded by people that verify the people that want to come in. They decide on the trustworthiness of the new people based on mechanisms that can determine this trustworthiness.
But then the data that is saved in the blockchain also need to be guaranteed to be secured. Also data that's coming from outside, so outside the fortress need to be verified. The big question is how to secure the data on those machines before it gets into the blockchain.
Yes, I understand what you mean. I think what you mean could be something like external validation used by Hyperledger where they also look at how to verify data before it goes into the blockchain. But I think you're talking about transactions that can be verified and checked. But the problem again with the scenario I try to describe is that you can't really verify the data itself. It might be just actions like "I want to increase temperature to 100 degrees". The other nodes in the network will now say yes, ok we record that in the database, but they don't know if 100 degree would be good to do. We need a certain way to determine that there's not an attacker that tries to tell that machine that he should go to 100 degrees.
If you keep such a scenario in mind, then maybe we need to look at a different feature of consensus, so they can reach consensus about that they're still secure as a network and all the machines in the network are still trustworthy. Eventually maybe this comes a bit back to machine learning about what can machines learn about each other or at least see from each other. But simply put this consensus protocol looks to the identification of the node, the fire wall is up to date and maybe physical locations and whatever other data you can think of. This maybe already makes it better secured.
OK, I think it's an interesting thought. But when I have this picture in my mind with the fortress, with the people inside the fortress, how does this help to secure the network? It could be over the time that one party tries to fool the network because for this node it's a higher benefit to behave malicious in comparison to participate in the network. Do you also focus on that?
I do understand what you mean. I'll try to illustrate it with the fortress in mind. It maybe sounds a bit stupid, because we're talking about people and actually mean machines, but let's keep it that way. Let's for example say that one of the people in the fortress gets a psychosis. So he gets crazy but is already in the network, so the rest trusts them. We check people at the gate if they're good and we can trust them, but now when they're in the network we don't do the verification. So if this person who gets crazy or malicious or attacked via airplane or whatever. The rest of the nodes should see that he's different if he wants to do a certain action. If you have such a scenario but then in a network of machines, where you essentially can trust them but you can't verify the actions that it's supposed to do, but still want to guarantee that you can trust the actions that he wants to do. Could you then basically use data about the node that proposes the new action to confirm he's trustworthy. For example he maybe can show he has still the right security level or maybe in a very advanced state he can show that his software is still the same as yesterday. I heard of a way where machines can hash their complete current software state for example. Then every time when this machine wants to perform an action, it will ask to the network can I go to 100 degrees and that machine will also show its current state so the rest can verify that he can perform the action. Not based on if 100 would be good or not, but we can see that your software is not changed yet so we can trust you.
Well the question would then be if we include machine learning, is it possible to create some predictive security or something. Say for example, but I don't know it may sound stupid, this agent could become malicious in one week because of historical data etc. Maybe you could detect and predict future malicious nodes.
Well maybe not future, because I can imagine attacks happen suddenly in a few seconds. Maybe you just need to know in the network that you can still trust everyone and even the node that did good for years might still get compromised suddenly. As far as I know currently it's already possible that when a cybersecurity specialists looks closely to a certain machine, he can already see that something is wrong.
Yes, indeed.

Well with that idea, if you can implement that in the network, that they can see from each other if they're compromised or not, it might help to secure the network. Can you imagine what I mean?
Yes, but now you said that manually the cybersecurity expert needs to check the machines.
Well that's the current way I think.
So if you think about smart cities where you have 1000 of cars autonomously etc. In such a system it's very difficult to manually check if all the cars are still right.
Yes, exactly that's what I mean. In my scenario, all the cars in the network need to verify that other cars in the network can still be trusted. That's the idea. All those cars are in the fortress and running around and we can trust them, but we still need a mechanism to make sure that they can check and verify each other's actions.
Yes, I agree. Then it needs to be some mechanism where the cars can give each other scores and based on this score they connect to that particular car or I leave it and don't trust it or something like that.
Yes something like that.
That's very interesting to be honest, and I can imagine you need something like that if you think about smart cities or connected cars and other things like that in supply chains. They need to be secure and some mechanisms be in place that guarantee that the parties are trustworthy. Especially when new parties come in, how you calculate the trustworthy score then. I think that's an interesting thing to look at.
Yes true, I guess the network has some standard requirements that the network can use to check, like identification and security status. Then the network knows it's a new node and probably can't trust it as much yet, something like that.
Very interesting to look at this into more detail.
That's what this research is about.
Cool.
Well I'm actually wondering, do you think something like this is already happening? Because you have a lot of experience with IIoT and blockchain etc.
I haven't heard of anything like this I have to say. I think on a technical level they look into how to make sure that only someone in the network can encrypt and send data into the network, but that's not really the same. I haven't heard of any other developments into this direction.
Well, that's good to hear.
Basically it's not good enough to have a secured network, but you also propose some kind of security protocol or second layer that guarantees the trustworthiness between the assets.
Maybe eventually it could use machine learning, but for the simple version do you think it could work?
Yes, it's very interesting, I would be very interested into your thesis if you can share it that would be great.
Definitely I would! Thank you for your input into my research.
No problem, I hope it was helpful.
For sure it was. As I said I recorded the conversation and will make a transcription of it. Then I'll send it so you could check and confirm that this is indeed what we spoke about. Then when I'm finished, I'll send the full report to everyone with whom I did the interviews with. So I will definitely send it to you.
That's great, I'm looking forward to it.
We'll keep in touch, have a nice day.
You too, bye.

Interview 7

Date: 05-11-2018

Introductie

..

Oké, interessant met welk onderzoek u zich voornamelijk bezig houdt. Zoals ik net al aan gaf zijn er een aantal onderwerpen die binnen mijn onderzoek aan bod komen, de eerste daarvan is Internet of Things (IoT). Zoals u al zei komt er veel data uit de verschillende sensoren en doet u daar al analyses op, dus ik kan me voorstellen dat u daar veel kennis van heeft. Kunt u toch aangeven wat u verstaat onder IoT?

Wat ik zie onder de IoT. Ik zou zeggen dat het een heel breed begrip is, en bijna alles tegenwoordig data opslaat en naar de cloud stuurt. Het heeft ook een vorm van intelligentie, dus algoritmes draait die data interpreteert etc. Dus het IoT gaat zo breed worden dat vrijwel alles, behalve misschien hele simpele dingen zoals een bekertje, data intensief en een vorm van communicatie en computation in zich gaan hebben. Wellicht zelfs dat bekertje om efficiënter te recyclen etc.

Juist, we willen alles weten.

Inderdaad, je wil gewoon alles weten. Dus dat gaat zo pervasive worden, dat we dat niet meer merken. Alles gaat computationele communicatie mogelijkheden hebben. Gewoon omdat het interessant is dat je efficiënter kan werken etc.

Inderdaad, zeker als het makkelijk kan en het weinig kost om dat te doen, waarom ook niet zeg maar.

Ja inderdaad, ik denk dus ook dat de IoT dus ook de nieuwe computational power van de wereld gaat worden. Het gevaar is natuurlijk, wat gebeurt er dan allemaal met die data enzovoort.

Precies, daar komt de data analyse weer terug en wat kunnen bedrijven of wie dan ook er allemaal mee.

Ja, en wat je dikwijls ziet dat data opslaan wel makkelijk is, daar hebben we genoeg technische oplossingen voor. Data analyseren dat valt vaak tegen, daar heb je mensen voor nodig die de data begrijpen en de kennis van techniek hebben.

Dat zal inderdaad nog een grote uitdaging zijn.

Dat blijft inderdaad een uitdaging denk ik.

Als je kijkt naar data analyse zijn er ook al veel mogelijkheden, maar hier komt inderdaad wel zoveel data bij kijken dat is niet meer te overzien.

Juist, er komt zoveel data bij kijken en er zijn al veel analyse mogelijkheden die niet echt veel interessante informatie opleveren. Meestal moet je wel iets weten over de data en begrijpen. Ik heb nog maar weinig keren gezien dat je met vlugge enkele commando's interessante dingen eruit haalt. Meestal moet je er toch echt induiken, dat vergt veel kennis en investering van je tijd.

Zeker weten en dat komt bij IoT veel kijken.

Dit onderzoek heb ik eigenlijk meer gericht op de Industrial Internet of Things. Kent u die term ook toevallig?

Ja, wat je ziet is dat daar natuurlijk de grote winst is. We hebben samenwerkingen met bijvoorbeeld grote energie bedrijven. Alles wordt gevolgd, alles wordt voorzien van sensoren en efficiënter gemaakt. Maar ook daar zie je, dat ze heel veel data verzamelen, maar het verwerken daarvan blijft nog altijd een bottleneck. Ze hebben de data wel, maar weten niet goed wat er nou daadwerkelijk in die data te zien valt. Dikwijls zijn ze ook niet voorzien van genoeg personeel daarvoor. Grote ingenieurs bedrijven hebben uiteraard veel ingenieurs die werktuig bouwkunde of elektronica enzovoort hebben gedaan, maar die hebben geen idee wat je met die data moet doen.

Ik was onlangs bij een meeting, daar was een hoofd ingenieur die zei "Ja, ik heb ook wat gelezen over data analyse en weet dat er supervised en unsupervised analyse bestaat", dat was het ongeveer. Dat was echt een hoofd of manager van een bepaalde afdeling.

Die hebben hele andere expertise en zijn daar vast niet mee bezig.

Die hebben hele andere expertise inderdaad. Die bedrijven hebben hun personeel geselecteerd op die andere expertise.

Ik kan me voorstellen dat ze wel een hoop data hebben en kunnen opslaan maar om die eruit te halen en vooral begrijpbaar te maken, dat is natuurlijk lastig.

Dat is een hele andere tak van de sport.

Zeker weten inderdaad. Dergelijke dingen komen zeker terug bij IIoT alleen een groot verschil met IoT is denk ik dat je dan vooral praat over gesloten netwerken binnen een bedrijf of samenwerking tussen bedrijven. In tegenstelling tot IoT waar uiteraard alles zomaar verbonden wordt aan elkaar. Echter het probleem met een enorme hoeveelheid data en de analyse wat we er vervolgens mee kunnen doen komt wel bij beide terug uiteraard. In elk geval is het duidelijk dat je erg op de hoogte bent wat er speelt op het vlak van IoT. Dan heeft dit vooral te maken met de data analyse kant, heeft u ook ervaring op het gebied van cybersecurity?

Nee, ik heb niet zoveel expertise op het gebied van cybersecurity. Het is overigens wel heel belangrijk en heel sophisticated. Je hebt een soort wapenwedloop, oftewel de hackers worden gewoon steeds slimmer. Ik zie het wel als een mogelijk groot risico. We hebben dus meerdere projecten lopen bij bijvoorbeeld smart grids. Ik denk wel dat er een disaster is waiting to happen. Het is gewoon wachten tot de eerste keer een of andere groep, dan wel land of gewoon een paar schooljongens, het land even plat leggen. Dat gaat gebeuren, met dergelijke grote ingewikkelde systemen en netwerken waar al die informatie doorheen loopt, is het wachten totdat er vroeg of laat een lek is. Volgens mij zijn er daar al veel dingen van mogelijk en oefenen bepaalde groepen ook om dat te gebruiken. Er zijn ook al rapporten dat er gecoördineerde aanvallen en try-outs plaatsvinden om te kijken waar verschillende zwakheden zitten enzovoort. Zoals volgens mij al gebeurd is in Oekraïne of Estland ofzo waar een aanval is geweest waarbij verschillende banken en andere belangrijkere netwerken aangevallen werden.

Dat is dus een groot gevaar, maar die afwegingen moeten we nemen. Als je kijkt naar bijvoorbeeld grids, je wilt al die sensoren en technieken inbouwen om het efficiënter en efficiënter te maken. Efficiëntie gaat dikwijls gepaard met het kwetsbaarder maken, omdat je redundancy schrapt en je moet centraal kunnen sturen en zo. Dat maakt het weer kwetsbaarder want je hebt gevaarlijkere punten van failure enzovoort.

Juist, heel duidelijk gezegd. Dat is wat ik tijdens mijn onderzoek ook vaak zag terug komen inderdaad. Juist door die connectiviteit en alles maar verbinden omdat het efficiënter wordt, maken we het heel erg onveilig. Eigenlijk zijn we steeds een soort kaartenhuis aan het bouwen.

Exact ja, je krijgt een soort ketting reactie. En die efficiëntie klopt, maar in spel theorie heb je zo gezegd de price of anarchy. Ben je daar mee bekend?

Nee, wat is dat precies?

Een heel simpel voorbeeld, als je twee steden verbindt met twee wegen. De ene weg heeft gegarandeerd een uur reistijd, de andere heeft een reistijd van maximaal een uur maar hangt af van de hoeveelheid verkeer. Als er bijvoorbeeld maar 50% van al het verkeer langs die weg gaat, is de reistijd maar een half uur. Als je dit centraal kan organiseren, kan je ervoor zorgen dat 50% langs de eerste en 50% langs de tweede weg gaat, dan is de gemiddelde tijd 75% van de reistijd. Maar als je dat niet coördineert en iedereen zijn gang laat gaan, zal iedereen bedenken als ik route A neem, heb ik sowieso een uur reistijd, langs de andere weg heb ik hooguit een uur reistijd en is dus de betere optie. Iedereen zal die weg kiezen waardoor iedereen alsnog een uur onderweg is.

Het punt is dat je dat qua efficiëntie centraal zou moeten aansturen, maar als je dingen online centraal wil aansturen heb je weer een groot probleem want dat kan je hacken enzovoort. Dat is in netwerken met twee nodes met twee connecties, in grotere netwerken zit het vol met dit soort problemen.

Ja, en dan zou je het efficiënter kunnen maken als je dat van een groot punt kunt bekijken en analyseren.

Ja, daar moet je een balans tussen vinden.

Vaak in een industrieel netwerk zal er op dit moment met name worden gedacht aan die centrale vorm met de voordelen hoe we het zo efficiënt mogelijk kunnen maken en wellicht minder over de security daarvan.

Juist, dat is denk ik mogelijk een groot gevaar. Ik denk dat het wachten is totdat een grote disruptie gebeurt.

Daar wordt inderdaad al mee getest. Niemand kan daar ook veel aan doen omdat er nog weinig wetten zijn, vooral internationaal wat wel en niet mag online.

Dus ik denk dat die cybersecurity erg belangrijk is, maar ik vrees dat we daar eigenlijk altijd zullen achterlopen. Je ziet dat trouwens nu met high frequency training. Binnen de grenzen van de wet wordt er echt uitgetest wat kan. Elke actie van bijvoorbeeld regelgevers wordt gevolgd door allerlei tegenacties die nieuwe loophols proberen te vinden. Dat is met cybersecurity precies hetzelfde.

Wellicht nog makkelijker dan in de fysieke wereld waar we wel weten wat de mogelijkheden zijn. Binnen het internet kan je met wetgevingen dat niet allemaal meer beheersen. Weer duidelijk zoals u ook aangeeft

dat er binnen IIoT een groot probleem kan ontstaan vanwege die verbondenheid. Tegenwoordig zien we dan de blockchain technologie een beetje opkomen waarin eigenlijk een netwerk heel erg verbonden is en allerlei dingen zelf kan regelen en schijnbaar vrij veilig gebeurt. Wat weet u van de blockchain technologie?
Ik weet het algemeen principe. Het is een vorm van gedistribueerde ground truth die je opzet. Er zijn een aantal beslissingen en acties die op verschillende manieren zijn beveiligd. Een manier daarvan is cryptografie, de blockchain wordt namelijk met hashes aan elkaar gebonden en de hashes bestaan uit deels het oude en deels het nieuwe blok, dat stapelt zich op. Daardoor is het zo goed als onmogelijk om iets eraan te veranderen zonder dat het gezien wordt. Dat is een vorm van beveiliging, de tweede is het feit dat het gedistribueerd is en iedereen een copy heeft van de database. Op die manier creëer je een vorm van trust die als het ware in het netwerk zit. In een klein netwerk dan werkt het niet, maar op een bepaald moment wordt het netwerk zo groot en is het praktisch ondoenbaar om er iets aan te wijzigen. Daarnaast weet ik wel dat er een hoop problemen zijn. De klassieke blockchain is gebaseerd op het principe van proof-of-work, waarbij je een cryptografische puzzel moet oplossen. Dat is dus een vorm van leader selection, je hebt een toevalligheid die jou toelaat om nu even iets toe te voegen. Maar ja die Bitcoin miners verbruiken samen wel een hoop energie, ik hoorde iets als dat ze tegen 2050 de aarde met 2% opwarmen als ze zo bezig blijven.
Ja, energie verbruik bij de Bitcoin is een groot probleem.
Dan heb je natuurlijk wel een hoop alternatieven, zoals proof-of-stake en dat soort zaken.
Veel varianten inderdaad.
Alleen die zijn momenteel nog niet zo populair als de eerste dacht ik. Maar goed, ik kan me voorstellen dat bij sommige applicaties deze technologie heel waardevol is. Aan de andere kant vrees ik dat de blockchain opnieuw weer een hype is waar iedereen op springt. In veel gevallen zal je niet echt een blockchain nodig hebben, maar ik kan me voorstellen dat het bij bepaalde gevallen heel nuttig kan zijn. Ik denk bijvoorbeeld als je naar onderwijs kijkt. Ik denk dat dit heel snel grondig zal veranderen, waarbij de klassieke diploma's aan waarde gaan inboeten. Ik kan me voorstellen dat we over 10-15 jaar niet eens meer naar de Universiteit gaan, maar hier en daar een cursus volgen en hier en daar weer een diploma op doen. Als gevolg daarvan moet je wel een soort bewijs hebben dat je dat allemaal gedaan hebt en dat moet internationaal waarde hebben en bereikbaar zijn. Maar dat moet wel veilig zijn, dus ik kan me voorstellen dat de studenten over een aantal jaren een soort blockchain certificaat hebben en daarmee kunnen aantonen wat ze allemaal hebben gedaan.
Interessante gedachte.
Het belangrijkste is dat je zeker weet dat die informatie betrouwbaar is.
Juist, u zegt ook met name waar bepaalde dingen internationale betrekkingen krijgen, waar niet zomaar 1 land dat mag beheren dat blockchain wel waardevol kan zijn.
Ja, ik denk ook wel dat bedrijven daar een rol in gaan spelen. Stel bedrijven huren een ingenieur in, dan heeft die persoon zijn/haar diploma als bewijs. Ik kan me echter voorstellen dat bedrijven het niet zo belangrijk meer vinden wat je op de Universiteit hebt gedaan maar juist wel dat je bepaalde andere specifieke dingen hebt gedaan.
Eigenlijk alle informatie die je niet centraal wilt opslaan omdat er verschillende partijen bij komen en toch de data betrouwbaar wil blijven.
Juist, dus ik denk dat het bij bepaalde situaties wel waarde heeft maar op het moment juist weer nep toepassingen zijn.
U bedoelt dat iedereen denkt dat het een geweldige oplossing is voor alles maar dat er toch kritischer naar gekeken moet worden. Maar goed de blockchain is misschien wel een soort eye opener geweest en dat mensen zich beginnen te realiseren dat we bepaalde dingen ook anders kunnen regelen.
Ja, dat klopt zeker en vast. Er zijn interessante technieken die we tegenwoordig allemaal kunnen gebruiken.
Inderdaad, de blockchain is overigens ook gebaseerd op al bestaande technieken.
Ja exact, voor zover ik weet zat er niet echt iets nieuws in maar was het een nieuwe combinatie van bestaande technieken.
Zoals u net al zei zijn de centrale technieken daarin denk ik wel dat het gedistribueerd en niet te veranderen is. Een ander belangrijk punt is denk ik consensus bereiken binnen het netwerk. Uiteindelijk gaat het erom dat je met elkaar overeenstemming bereikt over de waarheid, en met name nieuwe waardes. Of je die waardes vervolgens opslaat met hashes of hoe dan ook maakt misschien niet heel veel uit. Heeft u wel eens met consensus protocollen gewerkt?

Ja, ik weet ervan maar niet de details hoor. De vraag is waartegen je consensus protocol bestand moet zijn. Is dat tegen het uitvallen van de nodes of dat je ook bestand moet zijn tegen actieve aanvallen van vijanden. Daar bestaan allerlei resultaten over of het al dan niet nodig is, maar de details weet ik verder ook niet echt.
Ik moet zeggen dat u er al een hoop erover weet.
Het is in elk geval ingewikkelde materie. Ik weet dat er resultaten bestaan over het niet bestaan van mogelijkheden. Ik dacht dat het zelfs zo was, als je meer dan 2-3 nodes hebt en er zijn malicious attacks mogelijk en je hebt geen deadline/expiring date, dat het dan niet mogelijk is om tot consensus te komen. Dus het kan zijn dat je eeuwig blijft wachten op die berichten. In zeker zin heeft de Bitcoin geprobeerd daar een mouw aan te passen want die wachten niet. Je stimuleert ook de nodes om zich op een goede manier te gedragen.
Door de incentives inderdaad.
Juist, dus ik kan me voorstellen dat er een hele familie is aan protocollen die in de ruimte van de mogelijkheden optimale niches vinden, zoals hoe betrouwbaar wil je zijn of hoe snel etc. Dat gaat altijd weer ten koste van andere gebieden.
Juist, allemaal hebben ze weer verschillende kosten en voordelen.
Dat is wel zo'n beetje alles wat ik ervan weet.
Nou, dat was al een erg duidelijk verhaal! U geeft inderdaad ook aan dat er verschillende varianten zijn, ook omdat het nog vrij nieuw is en we nog niet de optimale gevonden hebben denk ik. Voor dit onderzoek heb ik eigenlijk naar een van de eerste gekeken namelijk beschreven in 1989, dat is Paxos. Daarvoor was het nog een groot probleem zeker met 2 verschillende fysieke locaties om consensus te bereiken met individuele berichten. Heeft u iets gehoord van Paxos?
Ja, Paxos is van Lamport zeker?
Klopt inderdaad!
Ik dacht dat die wel een lastige is omdat je er vanuit gaat dat malicious attacks mogelijk zijn. Je wilt toch consensus bereiken.
Juist, u bedoelt het Byzantine Fault Tolerant problem ook beschreven door Lamport. Dan worden er inderdaad regels toegepast zoals dat je inderdaad binnen een bepaalde tijd moet reageren en met signed messages bijvoorbeeld. Het apparaat kan zich dus identificeren en het bericht tekenen. Als ze dat binnen een bepaalde tijd doen en versturen naar iedereen kan je ze vergelijken en zien dat er iets niet klopt. Bij Paxos is het wel zo dat ze uit gaan van een netwerk waarin de nodes te vertrouwen zijn. Wellicht ook omdat eind jaren 90 nog niet heel erg werd nagedacht over die aanvallen. In het kort gaat hij dus uit van een scenario waarin je weet wie er in het netwerk zitten en je kan ze in principe vertrouwen en de data die je opslaat niet kan veranderen. Dat komt dus al wel erg in de buurt van een industrieel netwerk. Als er nu een hoop sensoren aan zo'n netwerk worden toegevoegd weet je eigenlijk nog steeds wie erin zitten en horen. Alleen de aanname dat je het netwerk kan vertrouwen is vanuit een cybersecurity perspectief niet zomaar te doen. Je kan wel weten welke apparaten er in je netwerk zitten, maar dan moet je alsnog weten dat dat apparaat niet is aangevallen. Dus laten we voor het gemak 4 nodes in gedachten nemen die verbonden zijn met zo'n consensus protocol en dus dezelfde informatie hebben en consensus bereiken over nieuwe waarden. Maar ze kunnen binnen een industrieel netwerk niet meer controleren welke waardes goed of slecht zijn, wat je over bijvoorbeeld financiële waardes wat beter kan. Bij financiële transacties heb je wel of niet geld op je account en mag je dat opsturen en is dus makkelijker te controleren. Bij het netwerk wat ik probeer te schetsen heb je dat niet, want daar mag een apparaat bijvoorbeeld naar 100 graden of een sensor geeft een bepaalde waarde aan. De rest van het netwerk kan niet controleren of dat klopt. Zodoende kwam dus de gedachte of er een andere manier is om te garanderen of dat apparaat nog juist is omdat er niks veranderd is van buitenaf. Dus de essentie is, kan zo'n netwerk door zijn verbondenheid zien of een component misschien veranderd is. Kunt u zich dit scenario een beetje voorstellen?
Ja, tot zover wel.
Eigenlijk gaan we ervan uit dat het netwerk goed werkt als het niet aangevallen is. Alle acties die ze doen sturen ze naar het netwerk en dat kan iedereen dus zien en slaan ze gedistribueerd op zodat het ook niet meer aan te passen is etc. Alleen het probleem ontstaat dat als een van die apparaten fysiek of digitaal is aangevallen of dat dan te zien valt door de rest van het netwerk. Begrijpt u wat ik bedoel?

Oké, nou ik probeer het me even voor te stellen. Je hebt inderdaad 4 sensoren die hun waarden spuwen. Maar stel je voor dat de ene acces krijgt op een sensor en die stroom van data kan manipuleren, hoe zou je dat dan kunnen weten?
Nou het idee is dat er altijd software in zo'n apparaat zit. Om die stroom van data te veranderen of dat apparaat binnen te komen, zal je toch iets moeten veranderen in die software. Ik kan me voorstellen dat een node binnen dat consensus protocol een waarde wil toevoegen aan de database en daarbij ook zijn huidige status aangeeft, waardoor iedereen kan zien dat is hetzelfde als je gisteren was, dus we kunnen je vertrouwen.
Dat klinkt wel aardig, maar ik kan me voorstellen dat je bijvoorbeeld de software van zo'n apparaat niet zo snel kunt controleren op kleine veranderingen.
Nou ik ben geen expert met dergelijke technieken, maar ik heb wel technieken gezien waarin het bijvoorbeeld wel mogelijk is om een hash te maken van je hele status. Dat kan wel heel snel, maar als er maar een klein ding verandert, dan is die hele hash anders. Ik kan me voorstellen dat als de node die nieuwe waarde plus die hash bijvoorbeeld toont dat het al extra beveiligd wordt.
Oké, maar dat betekent wel dat die huidige status bijvoorbeeld niet afhangt van de tijd die sowieso verandert.
Goed punt, dat durf ik niet te zeggen. Ik kan me voorstellen dat de waarde zoals tijd of hoeveel graden het is niet opgeslagen is in de software. De software is denk ik hetzelfde alleen de output is anders.
Stel dat elke sensor de data bij zich houdt en de timestamp bewaart enzovoort. Bijvoorbeeld een CO2 meter wat afhangt van de temperatuur, dus die moet ook weer de buitentemperatuur weten dan gaat die buitentemperatuur weer mee in die machine voor de berekening. Misschien heb je ook bijvoorbeeld de frequentie van elektriciteit toevoer wat je moet meten en varieert. Dus ik kan me voorstellen dat zulke veranderingen niet vergeleken moeten worden en het lastig is dit te vergelijken. Wellicht dat je zoals eerder aangegeven het hiermee extra kan beveiligen maar er toch weer met een andere weg omheen gewerkt kan worden, want dan kan bijvoorbeeld de input van de temperatuur weer veranderd worden. Die wapen race is wel heel lastig.
Dat zeker, goed punt. Maar goed, stel theoretisch kan je wel bepaalde essentiële stukken software hashen en vergelijken, kunnen we dan misschien toch al iets beter het netwerk beveiligen? Als je bijvoorbeeld kijkt naar een electricity grid in zijn centrale vorm is vrij onveilig. Wat je vaak ziet is dat als een aanvaller via een zwakke schakel binnen komt, vaak het hele netwerk kan binnen dringen. Dat is door een verandering in de software en in een centrale vorm waar je security specialists hebt die dat moeten controleren, dat lijkt toch vrij onmogelijk. Wellicht moeten we dan toch wel kijken of het netwerk dan zelf kan zien wanneer een node aangevallen wordt. Het apparaat hoeft bijvoorbeeld al niks zelf op te slaan misschien, als hij maar gewoon eerlijk is.
Eerlijk in zijn communicatie inderdaad, ja.
Juist, eigenlijk ook transparantie. Die node zegt gewoon naar het netwerk, dit is de waarde die ik geef en dit is hoe ik eruit zie, dan mag het netwerk bepalen of ze dat vertrouwen.
Ik denk dat ik me zoiets wel kan voorstellen. Daardoor kan je misschien ook kijken naar de biologie bijvoorbeeld, hoe gaan complexe ecologieën daarmee om. Of hoe werkt het immuunsysteem in ons lichaam bijvoorbeeld.
Juist, die werkt ook ongeveer zo.
Ja inderdaad, waar komen vreemde boodschappen vandaan. Soms werkt dat goed. Ik denk dat het nuttig is daarnaar te kijken. Hoe weet het lichaam dat dingen tot zichzelf behoren en andere dingen vreemd zijn. Misschien dat je zoiets wel kan gebruiken in computer netwerken. Ik denk niet dat er overigens 1 oplossing is voor alles maar dat je partieel iets af moet dekken. Als je genoeg overlap hebt met die maatregelen dat je genoeg zekerheid hebt over de stabiliteit en veiligheid.
In het immuunsysteem hangt het ook af van een aantal mechanismes. Sommige zijn voorgeprogrammeerd, andere aangeleerd. Heel primitieve immuunsystemen doen iets als iets zich voordoet, andere passen zich aan en hebben een hele bibliotheek aan mogelijkheden. Als we naar dat soort computer netwerken kijken zullen we dus ook verschillende lagen nodig hebben, ten eerste niet alles centraliseren maar juist compartimenten hebben die afgesloten kan worden van elkaar.
Ja zeker.
Maar ik denk inderdaad dat dat uiteindelijk wel nuttig kan zijn.

Klopt, dat is ook wel een beetje waar ik heen ga. Binnen cybersecurity zal je zeker altijd verschillende maatregelen moeten blijven houden. Ik kan me voorstellen dat we bepaalde dingen kunnen ondervangen, want je wilt eigenlijk weten binnen een netwerk wanneer er iets anders gebeurt dan normaal.
Wat ik me wel af vraag is dat je veel netwerken hebt die erg dynamisch zijn. Wat ik bedoel is dat je netwerken hebt met 100 miljoen nodes maar elke minuut zijn er weer 10 miljoen die komen en 10 miljoen die gaan. Denk aan netwerken van mobiele telefoons bijvoorbeeld.
Als je in de context van IIoT kijkt heb je bijvoorbeeld de leveranciers die af en toe komen aanrijden met hun trucks en even deel zijn van het netwerk. Dus oplossingen die ervanuit gaan dat je een bepaalde configuratie hebt en daarmee kan blijven werken worden misschien ook juist weer kwetsbaar.
Ja, dat zeker. Wellicht dat het alleen maar op je kritische delen valt toe te passen omdat daar niet veel zou moeten veranderen misschien. In eerste instantie is dat ook het idee dat je ipv de huidige centrale vorm naar een decentrale vorm gaat waarbij je gelijk zo'n consensus protocol hebt die kan checken wanneer op een van die apparaten iets is aanpast. Als de rest van het netwerk dat gelijk kan zien en even kan afschermen is dat wel prettig. Maar goed, zoals u al aan gaf is het de vraag of elke kleine verandering die wel normaal is gelijk de alarmbellen laat af gaan en het stukje flexibiliteit wellicht een issue wordt.
Ja, het zal een balancing act worden dan.
Inderdaad, maar even hypothetisch als in een bepaalde vorm die machines in het netwerk wel van elkaar bepaalde dingen kunnen zien en wellicht veranderingen kunnen zien. Denkt u dan wel dat het een van de lagen zou kunnen zijn die de veiligheid kunnen verhogen?
Ja, dat denk ik wel. Het zal daarna weer nieuwe uitdagingen oppoppen.
Dat zonder meer. Maar goed, we waren het er net al over eens dat het op het moment heel onveilig is en dat we toch wel iets moeten bedenken en dingen proberen.
Dat zonder meer, het moet hoog op de agenda staan.
Juist. Overigens met uw kennis van machine learning. Mocht er veel van die data verstuurd worden binnen het netwerk, denkt u dat een machine learning algoritme daaruit dan zelf kan leren en het veiliger maken?
Ik denk het wel, naar de toekomst toe denk ik dat het zelfs wel gaat gebeuren. Ik denk dat we dat nu nog niet zien, maar dat toekomstige innovatie daar zeker voor zal zorgen. Dat zal wel een punt zijn waarop we onszelf serieuze essentiële vragen moeten gaan stellen. Het is helemaal niet evident dat AI op dat netwerk leven om de zaken in de gaten te houden.
Eigenlijk de ethische redenen of we het überhaupt wel willen.
Ja of we het wel willen, alleen vrees ik dat het sowieso gaat gebeuren omdat er gewoon sterke economische drijfveren zijn om het te doen. Alles moet sneller en zo en bedrijven zullen uiteindelijk op allerlei vlakken AI gebruiken en zullen we op een punt komen dat we ook niet meer terug kunnen.
Nou inderdaad, in cybersecurity zie je al dat bepaalde aanvallen al met een bepaalde vorm van AI mogelijk is. Dan zou je vanuit de verdediging kant om het zo maar te zeggen er niet omheen kunnen om het ook te gebruiken.
Klopt maar zo is maar de vraag met AI wat ze allemaal kunnen doen en of ze dezelfde uitkomsten zullen hebben als we dat zouden willen. Dus dat zijn wel zaken waar we nu al over na zouden moeten denken. Zodat we kunnen zorgen dat het ons uiteindelijk wel blijft dienen. Het is best denkbaar dat we uiteindelijk machines maken die dezelfde denkwijze zullen hebben als wij alleen het vele malen sneller kunnen. Die kunnen de ervaringen die wij in een heel leven zullen opnemen in een paar seconden verwerken en zijn weer klaar voor de volgende gedachtes.
Dat zie je al met quantum computing wat alles weer eens zal versnellen enzovoort.
Inderdaad, we zien al veel tekenen en ontwikkelingen die we hebben om sneller en efficiënter te werken. Ik zeg niet dat het geheel verkeerd is, maar we moeten wel stil staan om te kijken of het nog wel de goede kant op gaat.
Precies, maar goed we kunnen wel stellen dat cybercriminelen niet zullen ophouden met aanvallen te verbeteren dus vanuit een security perspectief moeten we sowieso wel stappen gaan maken.
Dat zeker, en zonder dat je openlijk agressief bent kan je al een hoop dingen doen zoals bij de verkiezingen waarmee gespeeld wordt. Niemand kan het echt bewijzen, het is geen oorlogsmisdaad want er is nergens een bom gevallen. Als nu blijkt dat de Brexit gesponsord is door bijvoorbeeld Rusland en wat voor impact dat heeft, dat is niet niets.

Zo zijn er nog talloze mogelijkheden inderdaad. Hartelijk bedankt voor al uw input.
Graag gedaan, ik wens je ook veel succes met je onderzoek.
Bedankt, het grootste gedeelte is denk ik wel gedaan, vooral nog alles afronden.
Nou ik hoop dat ik wat voor je heb kunnen betekenen.
Zeker, ik vond het een fijn en nuttig gesprek! Ik zal het uiteraard ook allemaal uittypen en opsturen zodat u er even naar kunt kijken en bevestigen dat we dit inderdaad besproken hebben. Het gesprek in mijn uiteindelijke verslag zal wel geanonimiseerd worden en dat verslag zal ik uiteraard ook toesturen.
Oké, ik vond het ook een leuk gesprek en interessant onderwerp. We houden contact**.**
Zeker, fijne dag nog.
Hetzelfde.

Interview 8

Date: 01-11-2018

All right, well this research touches much with IoT. Could you tell me about what your expertise is with IoT?
What do you mean expertise in IoT?
Well, what do you know about it or what your experience with IoT is?
No, this is not something I can say. You can imagine I heard about it and I know what it is. I have experience with it but I don't know why you ask this question.
All right, I understand. Maybe I wasn't clear myself. This research touches the fields of IoT, cybersecurity and blockchain.
No, no, no blockchain. I do zero blockchain, I think blockchain is the most hyped thing in the world at this moment. So I know zero about blockchain.
No problem, I understand. This research just touches different subjects, therefore I speak to experts with different backgrounds. Because it's academic research I have to ask some questions to scale the knowledge of my interviewees. Then I can ask some questions that go deeper into detail about how to secure an industrial network.
Ok, go on.
Well, ok so you told me you know a lot about IoT and also the Industrial Internet of Things will be familiar to you.
Yes, industrial that's what I know something about.
Is that based on the fourth Industrial Revolution?
Some people call it fourth Industrial Revolution.
OK, but this is not your expertise probably more the focus on cybersecurity?
Well I'm an expert in monitoring security in Industrial Contact systems but I know the Industrial contact systems, you can call them Industrial IoT if you want.
All right, thank you, all clear. Let's quickly head more towards the cybersecurity, could you tell me in short what you see your expertise is in cybersecurity?
No I can't, look. It's too broad, it's too unprecise. It's like asking me what's my opinion about the world, you can't ask that.
I'm sorry, I understand what you mean. I know you have a lot of knowledge about these subjects. I hope you can understand that some questions just have to be asked to be useful for the research.
Seriously, for this kind of interviews I'm no use. If you have a specific question, than I'm happy to answer, but this is useless now. It's just too broad.
OK, well let's do it a little bit different then, I will just shoot to the core questions then.
For this I do need to know if you know something about consensus algorithms in distributed networks?
I don't think so. Can you tell me something about those algorithms, then I can tell you what I know, but maybe under another name.
Sure, of course. Well let's say you have a network of machines and they're all connected with each other. These machines all have a different location and database, but when new values need to be

saved, this needs to be done at all locations like a shared ledger. For this you need a consensus algorithm to make sure all nodes agree on the same value and all save the same values in their database.
Yes, I've heared about it, but I'm not an expert.
OK, no problem. Well this research is about the industrial networks (or critical infrastructures) and that at the moment they're usually organized in a centralized form. This gives a single point of failure, and most failures or cyberattacks can do a lot of damage, because if they hit the core or any part in the network they can infiltrate a large area of the network and take it down. Now more and more machines are getting connected to the network and also start to work more decentralized, for this you need a consensus protocol.
Well in IIoT, at this moment they have zero space for things that are not consensus. I mean it's all centralized. But I don't really understand what you mean. In the kind of networks that I work on, I'm talking about oil&gas, energy, power generation and manufacturing. In those cases, there's no agreement on things. There's one system, determining what all other systems are doing. Then there's a safety system checking that all systems are doing the right thing and there's a fallback system in case the initial machine is failing. So in that sense it's very much an architecture that is 20 years old. In these systems there's very little space for a consensus algorithm. They will laugh at you if you would come with something like that.
OK, I can imagine indeed especially because right now indeed the systems are already very centralized and it's hard to change that. From a security perspective, like you said they do have a back-up already for the case when something fails.
Well it's a safety feature, not a security feature. When something goes wrong, then you have a fall back, but it's not in case of a cyberattack, just in case when something breaks down.
Yes, indeed. But recently we see more and more attacks also on those infrastructures.
In that case we don't talk about safety features, we talk about security features. That's very different, in safety you don't have an enemy, in security you do have an enemy.
Yes, I understand. As you said in the traditional way when they developed these networks 20 years ago, they probably didn't have to think as much about security but more about safety features. Now you see they are connecting a lot of machines to this network but that also increases the risks in case of cyber-attacks. We've seen in the past when attackers can infiltrate in a part of the network, usually an old or smaller machine, they seem to be able to infiltrate the full network, is that correct?
Yes, that's correct. But I really don't see how a consensus algorithm, where you also have a redundancy and you have consensus about the value of things, could improve the security.
Exactly, I understand, let me explain. Because if you have a consensus algorithm and they agree on the values, that means they can also see certain things from other nodes in the network. First of all the machine has to identify itself to the network, but maybe also show other data like software data and maybe indicate that it's compromised. Then in the network they can reach consensus on the value, but also reach consensus about if a machine in the network can still be trusted. Can you imagine something like that?
Well I'm extremely skeptical about this. Because, it's a different world in IoT, it's all real time and then if you have things that have to get consensus on things, and when there's no consensus the things are probably breaking down already. Besides I wouldn't call it a security feature, but more a safety feature, because it's about when things break down.
Well, I understand that at the moment they use consensus algorithms to guarantee continuity when part of the systems breaks down, so they can go to a back-up. But this research is basically focused on how to make this consensus algorithm also a security feature. So they can actually see that one of the machines is attacked and the network reaches consensus that such a machine can't be trusted anymore.
Uhm, I don't know.
Basically the scenario that I can imagine would be that indeed those consensus algorithms can agree on certain values but currently they won't see.

Well look, you have an operator switching things on and off. So how do you want this when you have an operator switching things on and off. He's determining what the system is going to do.
One thing you could do, but I think that is already old as a solution, is having every system duplicated and when the duplicated system does not agree in the results with the original system, rather than having a consensus algorithm, it just says "hey, here we have a difference", then you go and look after the difference.
This is basically what you're trying to implement only by implementing a consensus algorithm. In my opinion you don't need a consensus algorithm, you can just duplicate the system and see when the back-up does not agree with the original one. In that case, it will say here is a difference, go and look for it. But no one in that world of OT would allow you to say that once there's a difference, we would activate a consensus algorithm. They're not even going to think about that. I know companies who have a full back-up system, then what happens is, the next day or the next month someone changes something in the operational system but doesn't change in the back-up because there's no time. Then so many times, we get in and look at the original and back-up system, and they don't match.
Yes, I understand what you mean.
So think about what would happen if you add a consensus algorithm. Btw, those people are already scared to death to implement any changes.
I can imagine indeed.
They don't want to change anything, we tell them here you have a bug, and here you have the patch. They don't implement that patch for years, because they just don't trust if that's going to make a difference and the system unstable. Think about a consensus algorithm and that could bring some instability, you cannot even start with that story.
I understand the idea, but it's just going to be an overkill. You just have to have a back-up system and check if they match.
Of course, like you said it are old systems and you won't convince anyone to change to something new. This also makes it harder to imagine that it could work. But it's not my research to find a way how to implement this. The question now is, would it theoretically be in any way better secured than. Like you said it's maybe a bit similar to a back-up system, on the other hand like you said the back-up system is not always up to date. And especially when the network is continuously growing, you don't want a full back up system. Even with the full back-up system they can't really detect when something is compromised right?
Well what you're saying with the consensus algorithm is exactly what you're saying by duplicating everything and checking if the values are the same. This is already proposed a long time ago, you're just putting another flavor around it.
I understand what you mean, and you're right that consensus algorithms already exist before the year 2000.
Yes.
I understand, and those consensus algorithms only look at the values that're in the system and if they match. They don't yet look at it from a security perspective, more a safety perspective like you said earlier.
That doesn't change, what you're doing is using a consensus to do monitoring on a certain system. Whether this is actually providing the right value. When you want to know when a system is compromised or not, you don't want to have a consensus on a system.
Well if you want to see when a certain part is influenced by an external factor, gets attacked, and when the others can see that because they're connected, work together and transparent. I guess at the moment they cannot really see that when you duplicate the network right?
Why not? Why not? Why not? It's the exact same thing, only you make it a little less centralized. But the principle is the same, you have someone watching over the shoulders of someone else. What you're proposing is everyone watches over the shoulder of everyone else. I think in real time systems, this is completely unfeasible. You actually shoot yourself in the foot because they might disagree because there's a latency in the network.
I understand your point that it might get very complicated.

Yes.
It might all depend a bit on how you implement this and the techniques you use. Just the theoretical question is the same, would it essentially be possible to let the network automatically see when they can't trust a machine that's already in the network.
Would your case do.
Well that's what I'm trying to discuss and am searching an answer to, if the other nodes in the network can see real time that something is different than it should, it can agree that they should put that node in quarantine for example. Basically the rest can agree, or reach consensus that one particular machine in the network can't be trusted. Do you understand what I mean with this?
Well I really don't see how this would be better than duplicate every PLC and every work stations and see if they react the same. When it doesn't react the same, then you can look at it. Well of course you can have a double duplication, then you have 3 of them and then you make an agreement thing that if 2 say A, and the other says B you put in quarantine the one that says B. It is something you can do, and you can reach some extra security with this, with the consensus algorithm you would make it only more complicated. Because the essence is already there. It would cost more money and is also less, because the more simple the better.
Yes, I understand what you mean with that.
You don't want a complicated solution to a simple problem. Especially you don't want a complicated solution if you already have a simple one. What I'm telling you I think is the simple version. I don't see how this would be worse than a consensus algorithm. If you want you can put 4 or 5 or whatever number of duplications, but I think that a consensus would add no extra benefit. In this case you want to rely on something and check if it's doing well. If you rely on those things agreeing with each other you bring a big instability in the system, that I think would never work.
In theory of course you can do that, and there are some cases in which it would improve the security. I can't deny that. But is it the best solution for the problem, I'm sure not. Because I think the one that I explained would be the simpler one and more reliable. I know you need to do this for your master thesis and you would like to hear "yes this would increase the security".
No, of course if it doesn't work the research can still be good.
I completely agree with that, negative results are very interesting as well.
But if I'm correct than you at least say that in some cases it might work and be beneficial, but in most cases it would be too complicated and expensive to do it.
Not only too complicated and expensive, but it would introduce more risks. I don't think it's suitable for IIoT.
But in an industrial network soon we have 100.000 machines working together. In a centralized version with a back-up where some things get detected. Or actually the focus now is on the safety feature that something breaks down and gets replaced quickly in the current situation. But that won't work with so many machines connected right? I can imagine that you need some kind of security feature as well that can automatically detect real time when an attack occurs, not only when they fail on a natural way.
I understand. Look, you can try. But I mean, I'm pretty sure that in some systems where you need security to be extremely high, like military systems or airplane systems, then you can use consensus algorithms. Then you have everything duplicated and you'll use a consensus algorithm. I do get that, in that case you do have a better security. But if this would be feasible for IIoT networks, that would be fighting a small problem with a big cannon. So I think the solution that you're proposing has value, that certainly. Only the place where you place the solution is probably not the most ideal place where you need it.
OK, point taken. As for example the attacks on the water supply system in America. They intruded the network via a component in the network and eventually could change the software on the machine that controlled the chemicals in the water. By changing it a little bit, the water was unsafe to drink. Now we can say it's too complicated and expensive to add extra security measures, but I can imagine it needs to be better secured anyhow.

Yes but intruders will get in and infiltrate in the whole network and compromise all the machines in there. By the way you mention water, but people handling water have zero money. Zero. Try to convince them to buy a Linux system and a Windows system, and then every time they have to reprogram it, they have to reprogram the Windows and the Linux system. They're never going to do it.

I understand, let's look at it slightly different. Let's say in the network protocol you have a security standard and need to update to even connect to the network.

Yes, but if you just duplicate the machine in there and someone is compromising it, it's just going to change the same values on all the machines. Because how does an attacker come in? He gets into the work station where the monitor person is working. Then it works from this workstations and changes some values. He does exactly what the person would do to change this values. Suppose that you have to change this values, then you have to change the values on all 3 machines. That's not going to work, because that takes time. But even then, the intruder would do exactly that. So it gets in the workstation he mimics the moderator and can change.

So he gets into that machine digitally right, not physical?

He gets into via phishing or whatever something.

So in the digital environment indeed.

Yes, he just changes the values just like a human person would.

All right, now keep that in mind, but the attacker is intruding a certain machine digitally.

It's too complicated! I mean what do you want, that a person is going to do it 3 times on different laptops?!

No, I'm actually not at all talking about duplicating. Essentially if the other nodes in the network can see that the machine or laptop is trying to change a number, but his software is different (and thus compromised), maybe he shouldn't allow this value because it might not come from the operator.

No, but look! It comes from the operator! It comes from the machine of the operator. That's what happens. Nobody can tell you "Ow this comes from an intruder, so watch out". They come via the operator.

Because the intruder can get into the operator system.

Absolutely, that's the way they get in. Phishing, spear phishing, Word documents, whatever they start from there.

Of course, they need to have a certain access point.

That's what they're doing.

All right, so they start somewhere and try to use it to enter the network, so they implement some software on a certain machine. But what if at that point the other machines in the network, can see that this machine is a bit different. Because for example they could all see what it was yesterday and could compare that to what it is now and see that it's different.

Yes, but that is not consensus.

Well if they can reach consensus maybe on that they are all still safe or not?

No, they can't. Look I'm the operator and need to be able to shut off the water, right.

Yes of course.

With your consensus system I need to tell to 3 people shut off the water. Then after consensus the water is shutting off. It must be possible otherwise the operator can't operate. An attacker does exactly this, it comes into the system, behaves as an operator and then tells to shut off the water.

Yes, and nobody can check if it's actually a good thing to turn of the water, that's right.

Exactly.

So indeed they would still reach consensus if an attacker tells them to turn of the water.

100%

I understand that. And as I saw online you have experience with intrusion detection in Industrial Control systems. So to get into the network, they have to get into and change the software.

Yes, but they get into the software at workstation level. They get into the workstation, and the workstation is normally the one that changes all the values all the time.

Yes that's normal. Well than the idea is that the other machines in the network can see also on that workstation that the software is changed a little bit.
Haha, if you have that, you'll become rich.
Well I don't say I have the solution. But when I did research about this matter there're indications that machines can identify them self and also prove about his software status that he's basically still the same as yesterday.
There're methods to do this.
Well if they technically can show that they are the same and thus not compromised. And because you also need to have a connection in the network then.
That's a different ball game. We could discuss about that, but I'm running out of time now. I hope this discussion was still useful.
All right thank you, I understand that you have other priorities as well. Thank you for your input, essentially you say that it might be better secured but won't be worth it.
Yep, ok look I'm going to do something else now. I wish you good luck with your research and thesis.
Thank you very much.
Bye.

Interview 9

Date: 09-11-2018

Introductie

..

U begon net al over IoT en wilt daarop gaan focussen, kunt u in het kort aangeven wat u verstaat onder IoT?
Ik kijk eigenlijk bij IoT niet naar de toepassingen maar naar de architectuur en protocol aspecten ervan. Ik kan me echter wel makkelijk een voorstelling van bepaalde scenario's indenken als we dat zo nodig hebben. Kijk we hebben het over steeds kleinere devices die van alles kunnen doen, maar ik vind het vooral belangrijk dat ze ook krachtig genoeg zijn om zich te beveiligen. Een mogelijkheid is wel dat je bijvoorbeeld sensoren hebt die alleen praten met een gateway en die doet het meeste werk.

Oké, u kijkt in elk geval meer naar de security, en dat is wel prettig want mijn onderzoek is daar uiteindelijk ook op gericht.
Overigens nog iets over die gateway, daar kan je veel security aspecten zien maar ik wil kijken of je daar ook privacy aspecten kan meenemen. Bijvoorbeeld de Toon thermostaat, vroeger pompte die alle gegevens naar een centrale server.

Inderdaad, dan kunnen ze van bovenaf alles vergelijken.
Juist, maar ik denk dat je ook goed moet nadenken wat nodig is om erop te versturen. Niet alles maar versturen, dat wordt weer privacy gevoelig. Dus je moet vanaf daar al data minimalisatie gaan toevoegen, dat komt meer van de privacy kant. Security experts die denken daar niet over na.

Nee, ik kan me voorstellen ook vanuit die bedrijven dat ze daar wat minder de focus op leggen. Die denken hoe meer we verzamelen hoe beter, dus stuur alles maar door.

Wat betreft privacy zou je toch meer moeten kijken wat willen we eigenlijk wel doorsturen.
Wat willen we halen inderdaad en die data vervolgens alsnog beveiligen.

Juist, laatst hoorde ik al het voorbeeld dat Philips tandenborstels heeft die verbonden zijn en data willen doorsturen. Dan ga je je toch sterk afvragen waarom willen ze dat, willen wij dat wel, maar goed.
Precies, privacy en security zijn erg belangrijk voor IoT denk ik.

Zeker, daar zijn we het over eens. Nu hebben we het vooral over IoT netwerken gehad waar je ook ziet dat die netwerken veel meer decentraal gaan worden. Je ziet steeds meer dat alles groeit en verbonden wordt maar dat dit ook niet meer vanuit een centraal punt te managen of beveiligen is. Heeft u ook ervaring met de cybersecurity van dit soort decentrale grotere netwerken?
Nou ik heb wel gewerkt aan 3G en 4G netwerken van telecom systemen en deze te combineren met wifi en bluetooth netwerken en hoe je overschakelt van de ene naar de andere maar niet echt in IoT. Interessant vind ik wel in jouw vraag dat er twee dingen zijn die van centraal naar decentrale distributie kunnen. Een is het management van het systeem met controle van de software updates bijvoorbeeld, het management aspect. In telecom is dat het control platform, dat alles controleert. Aan de andere kant kan je ook de data decentraal brengen, dus elke meting dat een thermostaat doet. Mijn vraag is welke heb je in gedachten.

Ik snap wat u bedoelt, uiteindelijk kijk je naar IoT met hele kleine sensoren. Om te beginnen denk ik aan grote netwerken maar wel gesloten binnen bepaalde organisaties. Dit kunnen bijvoorbeeld powergrids zijn, water supply systems.
Oké, dat soort netwerken ja.

Dergelijke netwerken worden ook steeds meer apparaten aan gekoppeld om dingen efficiënter te maken. In de literatuur wordt dit vaak beschreven als Industrial IoT, waar je dus een gesloten (privé) netwerk hebt. Op dit moment zijn deze vaak centraal ingericht, vaak ook omdat ze al heel wat jaren mee gaan. Tegenwoordig zie je dan wel weer dat aanvallers steeds meer de mogelijkheid krijgen om bij een zwakke schakel het netwerk binnen te komen en binnen het netwerk kunnen op klimmen naar een centrale control panel en veel schade doen.

Dit onderzoek is dan ook gericht hoe we zo'n netwerk eigenlijk beter kunnen beschermen door het decentraal te organiseren.
Met grid netwerken of SCADA systemen heb ik zelf niet veel ervaring, maar ik begrijp wat je bedoelt. Ik heb wel een jaartje gewerkt met een powergrid, wat je daar ziet is dat er veel switches zijn die aan en uit kunnen

gaan en van een afstand worden bestuurd. Daarvoor heb je ook een communicatie netwerk nodig om dat van een afstand te kunnen sturen. Toen was er eigenlijk geen internet en waren er weinig invloeden van buitenaf.
Precies, wanneer was dat?
In de jaren 1990-1991.
Ja, precies en wat ik veel in de literatuur terug las is dat die netwerken nog steeds op dezelfde manier werken, maar dat veel componenten nu verbonden worden en ook met het internet bijvoorbeeld.
Zeker, ik kan me jouw scenario nu voorstellen. Dat kan op het moment zeker mis gaan. Even een ander voorbeeld, hier tegenover hadden ze een project over het controleren van een aantal pompen, ik geloof 5000 pompen. Van afstand wilden ze die pompen controleren, maar dat is uiteraard ook niet erg veilig want ze wilden dat met een mobiel app besturen.
Precies, nou dergelijke dingen kan ik me goed voorstellen inderdaad. Binnen IoT is het al heel lastig omdat alles verbonden wil zijn en het is al heel lastig dat te beveiligen. Voor dit onderzoek kijk ik dus wel naar die industrial netwerken die eigenlijk al veilig moeten zijn zoals bijvoorbeeld zo'n netwerk van pompen. Wat je veel ziet met aanvallen zoals Mirai en Stuxnet dat ze via een klein component binnen kunnen komen en zo door het netwerk kunnen verspreiden zonder dat het opgemerkt wordt. Omdat er steeds meer machines verbonden worden neemt die onveiligheid alleen maar toe.
Dat zeker, ik begrijp de context die je bedoelt.
Super, dan wil ik hier zo even op door gaan. Eerst even een kleine sprong naar blockchain technologie. Heeft u hier al kennis van genomen of ervaring mee?
De principes weet ik wel. Je hebt bijvoorbeeld 5000 noden en elke gaat een transactie roepen naar iedereen, vervolgens gaan ze dan kijken hoe dat past aan het vorige block. De eerste die wint en andere kunnen bevestigen dat het klopt wordt genomen als de waarheid. Ik heb niet alle toepassingen bekeken, er worden allerlei fantastische dingen bedacht, maar daar ben ik niet echt van op de hoogte. Mijn visie hierop overigens is dat de blockchain eigenlijk een grote database is die veilig is. Je kunt bijvoorbeeld dingen die erin staan niet ontkennen dat het gebeurd is en ook niet meer veranderen. Dat biedt integriteit en betrouwbaarheid, dat is volgens mij het belangrijkste.
Juist, en wat betreft privacy waar u veel naar kijkt zal dat wel weer problemen opleveren omdat je soms juist vergeten wilt worden, maar goed.
Ja, ja zeker! Sommige mensen lijken blockchain te willen gebruiken voor alles, maar in mijn optiek is het een geweldige infrastructuur voor integriteit maar niet voor anonimiteit etc.
Precies, nou kan de blockchain weer op veel verschillende manieren geïmplementeerd worden met verschillende technologieën die allemaal weer zijn voor- en nadelen heeft. Maar de essentie is waar dat je over een netwerk praat met verschillende fysieke locaties die met elkaar nieuwe waardes moeten overeenstemmen. Vervolgens slaan ze het allemaal op, waardoor het niet meer aan te passen valt.
Dat is wat ik er inderdaad van begrijp.
Nou hebben ze dus eigenlijk altijd een consensus algoritme voor die nieuwe waardes en iedereen het erover eens is. Hoe je dat wilt doen, en hoe je het wilt opslaan etc. kan op verschillende manieren, maar de essentie is dat je wilt garanderen dat er maar 1 waarheid ontstaat. Dat is een consensus protocol, bent u wel bekend met consensus protocollen?
Ja hoor, in het kort eigenlijk vragen ze aan iedereen iets te bevestigen, als een meerderheid zegt ik bevestig dat, dan wordt het door iedereen aangenomen als waarheid.
Juist en voor het jaar 2000 waren er al consensus protocollen. Wellicht zoals bij die data fusie die u eerder in het begin zei kan ik me voorstellen dat zo'n vorm al gebruikt kan worden. Als je bijvoorbeeld drie sensoren hebben, zoals hoogte sensoren van een vliegtuig, als er eentje afwijkt zullen de andere twee zeggen wij hebben gelijk.
Ja, zoiets inderdaad wordt wel gedaan.
Oké, een van de protocollen die ik heb bestudeerd is Paxos, zegt dat u wat?
Nee, daar heb ik geen idee van.
Geen probleem, dat kan ik me voorstellen. In het kort is het eigenlijk een consensus protocol dat zegt "als je iedereen kunt vertrouwen in het netwerk en de historie kan je niet veranderen, dan kan je er vanuit gaan dat het netwerk nog betrouwbaar is". De uitkomst is dan dat alle apparaten overeenstemming bereiken en dezelfde waarden als waarheid zullen aannemen. Als we dat gebruiken in zo'n industrial network waar je

ook weet wie er in het netwerk zouden moeten, kan je dat beter beveiligen via zo'n consensus protocol. Bijvoorbeeld om terug te komen op uw voorbeeld met de pompen, dan zou eigenlijk zo'n pomp aan de rest van het netwerk moeten vragen of hij omhoog of omlaag wil.
Oké dus het scenario is dat een pomp zich naar boven brengt maar de anderen willen dan meten of hij dat dan ook echt gedaan heeft?
Nou, een pomp moet uiteraard soms naar boven of beneden, maar je wilt niet dat een aanvaller van buitenaf daar invloed op heeft en kan bepalen wat die doet. Eigenlijk wat je hebt in bijvoorbeeld 4 pompen is dat inderdaad zo'n pomp dat zal voorstellen aan het netwerk, zodat ze consensus kunnen bereiken of dat wel of niet mag.
Oké, maar die pompen kunnen elkaar niet altijd zien en hoe kunnen ze dan bepalen of een bepaalde pomp dat mag doen? Met bijvoorbeeld Bitcoin, wanneer je een nieuwe transactie hebt kan iedereen minen en komt daar uiteindelijk een oplossing uit en iedereen kan bevestigen dat het goed is of niet goed is. In het geval wat jij zegt, kunnen ze bijvoorbeeld niet controleren wat het water niveau is en niet checken of iets goed is en wat niet. Hoe zou een algoritme dat dan checken?
Heel goed punt, dat is nou precies de conclusie die ik tijdens mijn onderzoek ook had. Bij de Bitcoin inderdaad kan je wat makkelijker controleren wat er wel of niet moet gebeuren. Een transactie is relatief makkelijk te verifiëren, je hebt wel of niet geld en als je het hebt mag je het maar 1 keer versturen, dat kunnen ze controleren. Eigenlijk in het netwerk waar de machines een hoop dingen kunnen doen, maar de rest niet kan controleren of iets wel of niet mag, is het misschien mogelijk om met andere manieren te verifiëren of die actie betrouwbaar is.
De gedachte is dat een aanvaller volgens mij altijd de software een beetje verandert om binnen te komen.
Ja, dat kan ik me voorstellen.
Dus die andere pompen kunnen inderdaad niet zien hoe hoog het water staat, maar misschien wel zien dat die pomp met dat voorstel niet hetzelfde is als dat hij gisteren was. We zien dat er iets is veranderd in jouw software en dat is mogelijk een aanvaller geweest. Als het netwerk van pompen daar dus consensus over kan bereiken. Dus voor het scenario als een pomp een bepaalde actie wil doen, moet hij zichzelf identificeren aan het netwerk met het voorstel maar ook laten zien wat zijn status is. Om te beginnen bijvoorbeeld alleen al dat hij kan aantonen dat zijn cybersecurity up-to-date is, een firewall bijvoorbeeld.
Zo'n mechanisme kan je inderdaad wel maken denk ik. Wat je bedoelt is dat een pomp een aanvraag stuurt naar iedereen in het netwerk en de anderen moeten mijn aanvraag beoordelen en bevestigen dat het een goede versie is. Bijvoorbeeld met identiteit management kan ik me dit voorstellen, een node heeft een token dat zijn identiteit bevestigt, de aanvaller heeft dat niet ook al is hij binnen de software gekomen, hopelijk heeft hij dan nog niet mijn identiteit. In dit geval ga je de control unit distribueren omdat iedereen nu kan beoordelen of dat apparaat nog dezelfde identiteit heeft. In dat geval kan ik me voorstellen dat een netwerk dan consensus kan bereiken over de veiligheid, tenzij een aanvaller die identiteit kan vervalsen.
Oké, je zal inderdaad nooit ook maar 1 solution hebben en zal dus meerdere technieken moeten toepassen om de veiligheid te waarborgen. Nu kan ik me ook voorstellen dat omdat we
Nou identiteit met behulp van tokens kan inderdaad wel.
Is dat in de richting van IPV6?
Nou IPV6 is meer om punt tot punt communicatie te bevestigen. ID management is deel van je authorisation system. Als je bijvoorbeeld als student in Leiden een account hebt in Leiden kun je daar met het wifi verbinding maken. Als je vervolgens naar Delft gaat en verbinding probeert te maken, zal dat wifi netwerk zien, jij bent van Leiden en ik kan jouw verzoek doorsturen naar Leiden. Als Leiden bevestigt dat jij die student bent, dan krijg je via hun toestemming om op het wifi netwerk van Delft te komen. Dit is echter niet peer-to-peer, er zit wel een soort surfnet boven.
Oké, dat is een soort centrale vorm.
Nou er wordt een soort hiërarchie gecreëerd. Als je binnen Leiden blijft ziet het centrale netwerk dat niet, alleen als je naar Delft wilt, dan zal dat centrale punt in werking moeten komen om jouw ID te managen.
Juist, nou zie je dat we momenteel zelfs moeten gaan naar een transparante vorm waarin andere nodes in het netwerk kunnen zien of iedereen nog wel te vertrouwen is.
Nou is het wel zo dat het netwerk veilig maken wel een groot begrip is want er kunnen een hoop dingen mis gaan. Een pomp aanpassen kan je misschien wel op deze manier oplossen, maar bijvoorbeeld data

communicatie tussen twee pompen en een aanvaller die dergelijke berichten wil lezen en monitoren kan wellicht weer niet op deze manier beveiligd worden.
Zeker.
Daar moet je denk ik weer met een andere manier mee omgaan. Daarnaast kan ik me voorstellen dat om een juist apparaat te onderscheiden met een slecht apparaat je die token kunt gebruiken, maar checken of de software niet is aangepast kan je misschien ook wel een soort image van het gehele ding doorsturen naar iedereen zodat iedereen kan checken of het wel of niet oké is. Ik weet niet of dat mogelijk is, dat is een beetje fantasie wat ik me kan voorstellen.
Nou dat is erg scherp en ik denk inderdaad dat zoiets mogelijk is. Je kunt namelijk een hash maken van je huidige status. Die hash kan je heel makkelijk vergelijken met de status van gisteren, dat is eigenlijk precies wat u zegt. Je kan inderdaad op die manier een apparaat snel laten aangeven wat zijn huidige status is, in een hashvorm.
Dat is vergelijkbaar met een token inderdaad en kan je snel vergelijken. Om de status van jou door anderen te laten bevestigen is wel een goed idee. Om terug te gaan naar die pomp, iemand komt binnen en geeft een command. In de oude manier gaat de pomp meteen aan. Wat jij zegt is dat als dat command komt, dan stuurt die pomp dat naar andere pompen en creëren ze consensus. Die consensus wordt gestuurd naar de actie unit van de pomp en vervolgens gaat het pas aan. Dat kan denk ik goed werken.
Hij vraagt het inderdaad aan de andere pompen. Belangrijk is dat die pompen inderdaad die commands wel moeten kunnen uitvoeren wanneer dat nodig is. Het is dus noodzakelijk dat een pomp kan checken of die aanvraag wel terecht is. Als de rest misschien kan zien of er iets in de software is aangepast, dan heb je misschien een betere vorm van veiligheid.
De aanname is dat die hashfunctie mogelijk is van de status. Daar wil ik wel eens naar kijken, want dat weet ik niet. Als iemand wat van de code verandert kan je dat wellicht ontdekken, maar als iemand binnenkomt als een administrator, dan weet ik niet of die apparaten dat kunnen zien.
Dat weet ik inderdaad ook niet precies. Volgens mij is het wel zo dat vaak aanvallers binnen proberen te komen met bijvoorbeeld phishing of wat voor manier dan ook. Dan is hij nog niet administrator maar hij moet ergens binnen komen en plugt dan wat software in om een soort gate te creëren. Vervolgens proberen ze op te klimmen in het netwerk om meer macht te krijgen.
Als software geplugd wordt, kunnen ze dat misschien zien inderdaad. Maar als ze bijvoorbeeld toegang kunnen krijgen door het gokken van iemand zijn password zal dit misschien weer niet werken. Alleen mallware en dat soort dingen zullen wellicht wel zichtbaar worden. Alleen moet je dan wel kijken naar false positives en false negatives. Soms moeten legit mensen ook wel eens iets doen en dan kan die weer problemen krijgen.
Ja ook dat kan een issue zijn. Daarnaast ook uiteraard de vraag hoeveel computation power zal het kosten en dergelijken. In eerste instantie is het dan ook erg theoretisch, zou het in sommige gevallen een toegevoegde waarde hebben?
Ja, dat is dan een volgende stap maar wat denk ik belangrijk nu voor jou is of het wel mogelijk is in sommige scenario's.
Klopt, maar je ziet nu steeds meer in de centrale organisatie vorm waar we steeds meer aan koppelen dat het vanzelf best wel onveilig wordt. Misschien moeten we dan wel een dergelijk netwerk creëren die niet per se kan checken of iets wel of niet mag gebeuren, maar wel kan zien of iemand in het netwerk nog steeds hetzelfde is en dus te vertrouwen. Om vervolgens een stapje nog te maken naar machine learning, heeft u daar wat kennis en expertise mee?
Ja, dat zeker.
Oké, want uiteindelijk kan ik me voorstellen dat zo'n machine die wellicht weinig computation kracht heeft zichzelf lastig kan beveiligen. We spreken uiteindelijk misschien over allerlei sensoren en zoals het voorbeeld van net al die thermostaat of tandenborstel. Misschien door te zeggen dat die apparaten alleen maar naar het netwerk hun status laten zien wanneer ze iets willen doen. Hij weet zelf niet dat hij aangevallen is, daar heeft hij te weinig kracht voor. Maar de rest van het netwerk kan wel zien dat hij nu ineens anders is.
Ja, ja dat kan ik me voorstellen.
Nou dat kan wellicht in verschillende niveaus gedaan worden. Zo kan je bijvoorbeeld misschien software status vergelijken of beginnen met security software of die up-to-date is. Je ziet nu al in veel netwerken

waar mensen nog werken met Windows XP of een oude firewall, dat aanvallers dat kunnen gebruiken om binnen te komen. Misschien is het daar al nuttig om te zeggen, dat iedereen in het netwerk dingen mag doen als die software up-to-date is bijvoorbeeld.
Ja dat is zeer interessant. Die signature kan ook wel dergelijke aspecten meenemen. Ik zie daar een toegevoegde waarde, alleen moet je even kijken hoeveel bandbreedte je nodig hebt en hoeveel aantal nodes je nodig hebt om genoeg betrouwbaarheid te creëren. 3 nodes is wellicht niet genoeg bijvoorbeeld dus heb je minima nodig of zo. Overigens denk ik dat je in jouw onderzoek "netwerk veilig maken" een te grote claim is. Misschien moet je zeggen "ik maak de intrusion detection" veiliger oid.
Zeker, zoals we al eerder zeiden zal cybersecurity in verschillende lagen moeten werken. Als dit een klein deel kan helpen is het al een mogelijkheid. Uiteindelijk kan ik me voorstellen dat die apparaten in een netwerk consensus bereiken of ze nog wel of niet beveiligd zijn op basis van software status. Dan kan ik me voorstellen dat je een soort machine learning algoritme kunt gebruiken die de betrouwbaarheid alsmaar veiliger maakt. Misschien kunnen ze wel patronen zien van wanneer ze gebruikt worden, of de waardes consistent zijn en de locatie waar een bepaalde order vandaan komt. Want de administrator zal wellicht ook wel op dezelfde computer zitten maar een order kan niet geaccepteerd worden als daar niemand zit, noem maar op. Daar zou je een soort machine learning voor kunnen gebruiken.
Dat is ook een goed idee inderdaad. Alleen moet je rekening houden met de rekenkracht van die pomp. Het is denk ik lastig om dergelijke machine learning kracht per node in te bouwen. Maar het is inderdaad mogelijk dat algoritmes die patronen gaan zien, als er altijd tussen bepaalde tijden dingen gebeuren en ineens is dat anders, dan kan de rest dat wel zien. Dat is wel een goed punt.
Dat is wel een beetje het idee van dit onderzoek. We zien dat die netwerken steeds groter worden en in de huidige situatie met een control panel kunnen ze niet alles meer overzien. Misschien moeten we eigenlijk wel die bevoegdheid aan het netwerk gaan geven zodat het netwerk bepaalt wanneer iets niet helemaal klopt.
Nou is het wel de vraag of elke node de andere in de gaten gaat houden. De andere oplossing is dat dat centraal gestuurd wordt vanuit een grote machine. Als je bijvoorbeeld 10.000 pompen hebt, dan is de vraag of je wilt dat ze elkaar allemaal controleren of juist 1 centrale vorm waar ze allemaal naar moeten rapporteren.
Inderdaad, ik denk dat uiteindelijk je ook een soort tussenweg kunt maken. Inderdaad is het misschien niet nodig dat ze allemaal elkaar gaan controleren. Ik kan me voorstellen dat je bijvoorbeeld 10 centrale kernen hebt, maar niet 1 want dat is heel onveilig. Die 10 kunnen allemaal weer subgroepen hebben o.i.d. zo kan je beperken dat je enorme kracht nodig hebt en alsnog centraal werkt. Misschien hoeft er maar een klein groepje te bevestigen of een machine nog hetzelfde is.
Ja, een soort hiërarchie maken.
Wellicht heb je wel verschil in mogelijkheden want sommige apparaten hebben toch meer computerkracht. Maar niet de centrale vorm zoals momenteel het geval is want dan heb je weer het single point of failure. In essentie is dus de vraag of je dat gaat distribueren. En het enige wat ze moeten doen is ook bepaalde status vergelijken van de apparaten in het netwerk, dan krijg je al een hogere vorm van betrouwbaarheid wellicht.
Ja zeker, dat lijkt me een valide concept. Voor sommige functies moet je het weer iets anders inrichten dat je bepaalde checks kleiner houdt en zo, maar goed.
Ja inderdaad.
Maar als je die machine learning algoritmes wil toepassen heb je wel echt krachtige nodes nodig.
Dat kan ik me voorstellen, dat wil je wellicht niet op elk apparaat. Maar je denkt wel dat ieder apparaat zijn status betrouwbaar kan doorgeven? Bijvoorbeeld een thermostaat die geeft aan dat het 20 graden is, maar niemand kan dat zien behalve dat apparaat zelf. Dat apparaat kan wellicht wel aangeven dat het 20 graden is, en dit is mijn status.
Ja, dat kan ik me voorstellen. Je kunt niet de data controleren maar wel misschien dat hij nog steeds hetzelfde werkt. In de blockchain kan je vervolgens alles opslaan en kan die node ook niet ontkennen dat hij dat heeft gezegd en zo. Ik vertrouw bijvoorbeeld de pomp omdat ik de hash heb gecontroleerd.
Dat is het idee inderdaad. Misschien kan je weer allerlei analyses op de data doen en zo, maar dat is voor verder onderzoek.
Ja, soms is de control data voldoende. Ik denk om veilig te communiceren heb je een soort key management nodig, je kunt de secret key en zo via de blockchain communiceren maar de inhoud van de data gewoon buiten

de blockchain. Als je alles via de blockchain doet wordt daar alles opgeslagen en groeit het alleen maar, dat wil je ook niet. Om veilig te communiceren is wellicht alleen die key infrastructuur nodig en de gewone communicatie gebeurt dan onderling.
Dat is misschien een mogelijkheid. U bedoelt dat de blockchain alleen maar checkt of ik de andere persoon kan vertrouwen. Als je blockchain dan zegt dat dat goed is, dat ze kunnen communiceren.
Juist, maar dat hangt weer van de applicatie af.
Zoals u al zei komen er nog een aantal dingen bij kijken die je weer op een bepaalde manier moet oplossen.
Maar eigenlijk wat je zegt, ieder apparaat kan zich identificeren, we kunnen die hash zien en vergelijken, dus wat overblijft is wat we kunnen vertrouwen. Je kan niet elke meting inderdaad zoals waterniveau op afstand meten.
Juist, stel we hebben straks allemaal onze thermostaat aan het netwerk dan wil je niet dat een aanvaller ineens kan vertellen tegen die thermostaat dat hij het 30 graden moet maken. Maar als we kunnen vaststellen dat dat apparaat nog steeds juist functioneert dan zal het wel goed zitten.
Vooral als je bevestigt dat de software niet veranderd is en je kunt bevestigen dat er niemand binnen is lijkt goed. Mijn gevoel zegt dat als je kan bevestigen dat niemand jouw unit heeft veranderd, dan wat die apparaten dan doorgeven dat je dat kunt vertrouwen.
Precies, nou dat is het idee wat uit mijn onderzoek kwam. Ik denk dat we er lang genoeg over hebben kunnen brainstormen en ermee kunnen afsluiten. Ik vond het een waardevol gesprek, hartelijk bedankt voor uw input.
Ja, ik dacht dat ik niks kon toevoegen.
Juist wel hoor, ik spreek met verschillende experts en iedereen heeft een andere achtergrond en een andere blik op dit scenario. Veel kijken weer naar de use case kant van blockchain en IoT, maar zoals u al aangaf, kijkt u toch meer naar de cybersecurity kant en dat is ook goed voor dit onderzoek.
Nou mooi. Ik zal nog even die artikelen opsturen waar we het eerder over hadden.
Heel graag, daar zal ik naar kijken. Nogmaals bedankt voor uw input. Ik zal de volledige tekst van dit gesprek opsturen wanneer het is uitgetypt.
Oké, en wanneer je klaar bent kan ik dat verslag dan inzien?
Jazeker, dat zal ik dan uiteraard ook sturen naar iedereen die het wil lezen, om te beginnen bij iedereen die input heeft geleverd middels een interview.
Oké, heel goed.
Nogmaals bedankt en een fijne dag nog.
Jij ook, tot ziens.

End of document