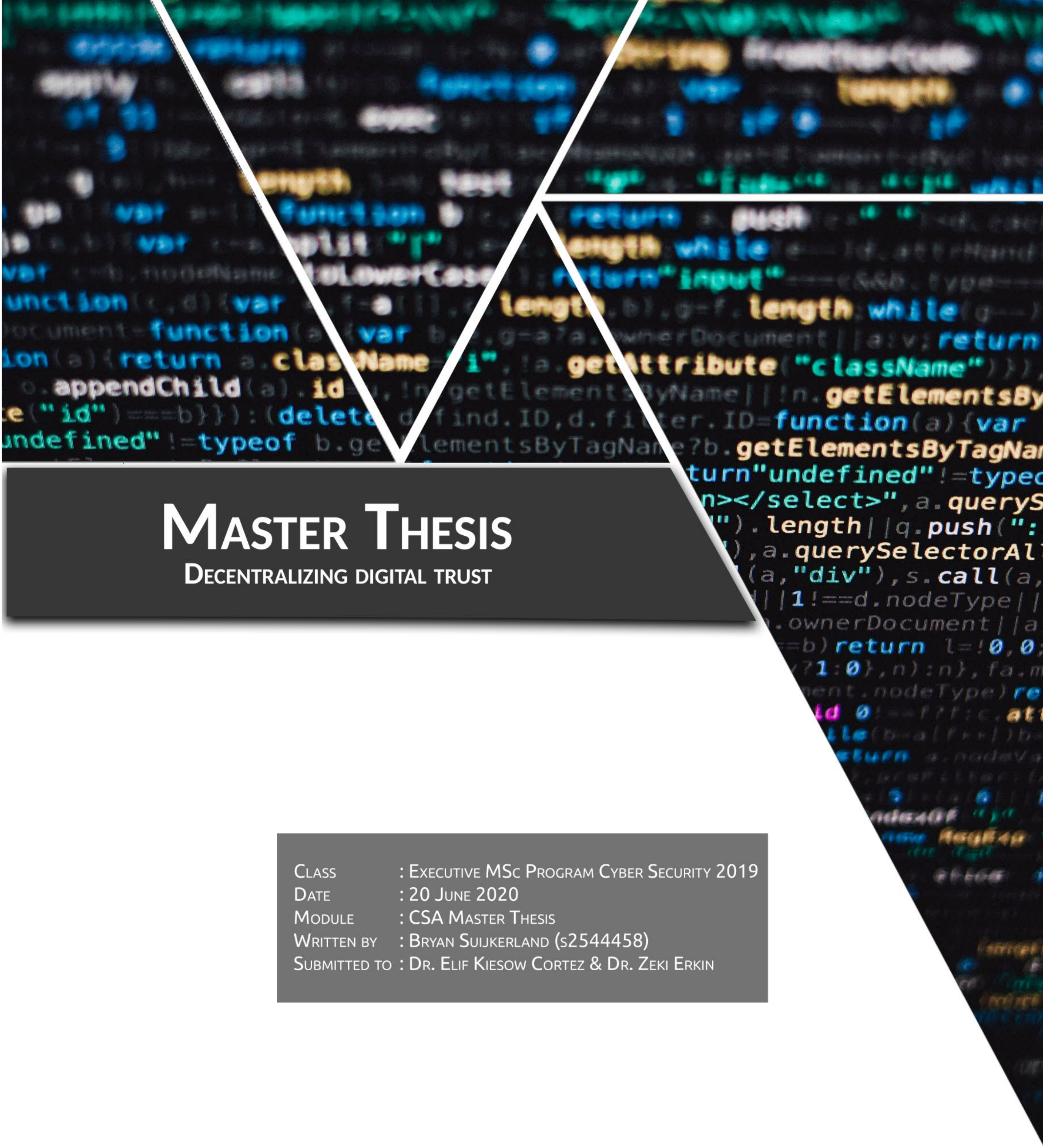


Master Thesis

Decentralizing digital trust

Class	: Executive MSc Program Cyber Security 2019
Date	: 20 June 2020
Module	: CSA Master Thesis
Written by	: Bryan Suijkerland (s2544458)
Submitted to	: Dr. Elif Kiesow Cortez & Dr. Zeki Erkin

Universiteit Leiden
Governance and Global Affairs

CYBER SECURITY ACADEMY

Abstract

In the current age, we use technology to communicate, share information, trade, and more. Within these forms of information sharing, we base our trust on the use of those digital connections that allow us to share. During this process, one bases his/her trust on trust coming from an authority. This authority is the certificate authority and allows us to trust an unknown party on the internet. By relying on the trust originating from the certificate authority, we put ourselves in a vulnerable position. This vulnerable position comes from the fact that it is difficult to check the party's information on the internet ourselves. We expect that the certificate authority does their work and conducts checks and balances on all details from the trusted actors. This process is very costly and inefficient to be conducted by every user. Therefore, we put our trust in the certificate authority to conduct these tests for us. In this case, the only vulnerable position that stays is the trust we put into the certificate authority. Once this authority corrupts this trust, it becomes challenging to trust all other trusted actors by this corrupting certificate authority. Furthermore, it becomes the single point of failure of trust that could trigger a market failure.

As the certificate authority conducts these tests, we cannot see all the information generated as the users of this trust [1]. Information we can check is connected to the used certificate. This information is basic and is related to the trusted actor. The disbalance that is created in possession of information is called information asymmetry. The information asymmetry created generates a few issues for the users of this trust: a large amount of information seeking, the uncertainty of information quality, and uncertainty of quality of information source. On top of this, we currently have the issue where the internet in its infancy and was not designed for the more prominent public. During the development of the protocols, the designers did not consider a large number of users, and security was less thought about [1]. Trust within these smaller networks was not a problem and led to the problem we have we current network protocols. Protocols like Domain Name System (DNS) and Border Gateway Protocol BGP are examples of protocols that can be manipulated. This effect and organic growth of different protocols led to the phenomena called a network externality [2].

As the internet grew, trust became an indispensable factor in connections/communications [1]. This is where the certificate authorities started offering their trust in the form of a certificate. These certificates are being used by the trusted actor to prove his trust against other users [3]. The burden on the certificate authorities grew and created a new form of threat over time. As this certificate authority possesses the power to trust or not trust actors, they became an attractive target for hackers and other malicious parties. The cases of Diginotar and Comodo showed this problem [4] [5]. Once the trust of a specific certificate authority is corrupted, users are unable to trust the other connected actors that fall under that specific certificate authority. This also showed that certificate authorities are centralized entities. This in itself, creates a problem for the users of this centralized certificate authority. Once the certificate authority is not delivering their services, in the case of a hack or downtime due to failures, users are not able to verify other actors. In order to improve the situation we take a look at the current implementations of PKI and how decentralization could improve the current situation.

Preface and acknowledgment

Before my current job, I studied at the University of Windesheim where I first got in contact with cybersecurity. I studied Infrastructure, Design & Security, which was a combination of the subjects around networking/ethical hacking/process management. After four very productive and exciting years, I was able to get my bachelor's degree. After this study, I joined the Royal Dutch Navy and started my daily job as a network architect. This job consists of creating and designing infrastructure for maintaining and testing innovations related to networks.

After working for a few years within the Royal Dutch Navy, I got the opportunity to start a new study focussed on cybersecurity. Without any hesitation, I wrote my submission letter and started the master. Since I was able to combine my current job with the study, time was no problem. Every Friday of the week was dedicated to this study and allowed me to invest this time. In the beginning, lessons within the classroom were something to get used to again, but these lessons were the most productive. COVID-19 dominated the last period of the two study years. This forced the study to take place from home. This new form of study allowed for a more flexible time schedule, but lost the personal contact and ease of asking simple questions in class. The past two years were advantageous in terms of knowledge and provided me with a new multidisciplinary vision towards cybersecurity.

This thesis is written in order to finish the Executive Master Cyber Security. This program is organized by Leiden University, The Hague University, and the Delft University of Technology. With this thesis, I took a different road than once thought before starting this thesis. The multidisciplinary approach of this thesis gave me a different view when thinking about technological solutions/improvements. As new developments are being made, I am very keen to always look towards the spectrum's technical side. This behavior is my nature due to my technical background and can steer you in thinking in solutions. However, by looking at the core of technologies, there is always a bigger picture with its connected problem it tries to solve/improve. This food for thought brought me to my current thesis and how I went about doing my research.

I want to thank Dr. Elif Kiesow Cortez (first supervisor) and Dr. Zeki Erkin (second supervisor) for their time and continued support throughout my research. They offered expertise, help, and support that was of great value and helped me conduct my multidisciplinary research. I want to thank them, especially during these COVID-19 times, as we all work isolated and have to work from home. It asks for flexibility from all of us.

I also want to thank my parents, Peter, and Esther, who supported/backed me throughout the research conducted from home. I also want to thank my girlfriend, Fleur, she helped me to stay motivated and push a little more. I also want to thank my employer, The Royal Dutch Navy, for allowing me to use this opportunity and use their valuable time to conduct this study.

Table of Contents

Introduction of research

Motivation

We use technology to communicate with one another and base our trust on context and individual factors. We want this trust relation present in every sensitive connection to share the information with the correct party. In this thesis, we refer to trust in digital services as digital trust

In this thesis, we refer to digital services, and we will use economics analysis. Using economic analysis, we try to understand how we can improve the digital trust originating from CA's (Certificate Authorities). When we share sensitive information by digital means, we want to know that the information is delivered to the right person. Defining trust within the current CA ecosystem, trust can be seen the same way as we experience social trust. We rely on a particular party to show specific behavior and put ourselves in a vulnerable position. Once the expected behavior is shown, we can trust the party. This can also be applied to the trust model of the CA's, as they are the trusted party [6]. The CA trusts the actor we are trying to trust and can prove this trust by validating that actor's information. Using this trust model currently delivered by the CA's, we can achieve a trust relationship between us as the user and the other user(s) receiving sensitive information. This trust relation is "proxied" through the CA, as there is no other direct and efficient way of validating all actors we need to trust daily [7].[1] As the user and the trusted actor, both of us trust the CA to trust each other. In figure 1, we can see how this trust flows.

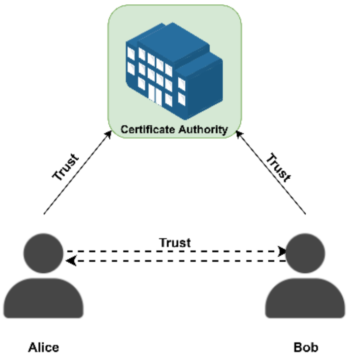


Figure 1 - Trust flow

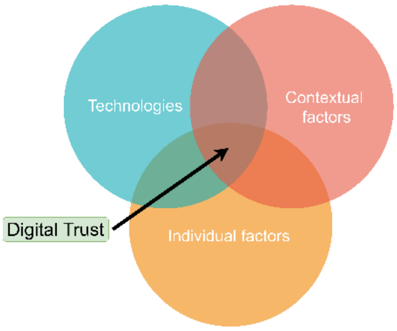


Figure 2 - Concept of digital trust

[8]
Digital trust is an indispensable element when it comes to communication/sharing over the internet. For these communications to transfer securely, we use the PKI (Public Key Infrastructure) system. With this system, we can set up secure connections between the sender and the receiver. For both parties to use this secure connection, trust is needed to use this secure connection. In figure 2, we can see how this digital trust is built. To better understand how one uses digital trust, we have to take into account these factors. New technologies can offer a higher standard of security, but people will likely not use them if they are hard to use. Contextual factors and individual factors may not be forgotten during introducing a new technology [8].

The burden on the certificate authorities grew and created a new form of threat over time. As this certificate authority possesses the power to trust or not trust actors, they became an attractive target for hackers and other malicious parties. The cases of Diginotar and Comodo showed this problem [4] [5]. Once the trust of a specific certificate authority is corrupted, users are unable to trust the other connected actors that fall under that specific certificate authority. This also showed that certificate authorities are centralized entities. Malicious parties are trying harder to get access to these CA's, as they are the key to the trust in many different connections. When an opposing party gains access to this trust, the integrity of this trust is completely gone. Users cannot rely on new and or existing certificates. There is a high likelihood that the malicious party creates them. These certificates pose a significant danger to the CA's trust and its current signed certificates [4].

[1] In the first introductory chapter we will go deeper into this topic and how trust is build.

CA's offer a hierarchical form of trust. This hierarchical trust, flows down to the lowest CA. Between the highest and lowest CA, there can be a multitude of different CA's. The primary source of trust originates from the root CA, which signs lower-level CA certificates. We refer to this flow of trust as the chain of trust [9].

The chain of trust is what is used within different CA's to offer trust. This trust is backed by different CA's that reside at a higher level in the trust chain. In the event of compromise, the trust chain breaks. All certificates that reside in this chain below the compromised CA cannot be trusted any longer. Secure connections are not secure anymore, as a malicious party can issue these certificates. The use of this trust chain is what strengthens different CA companies the ability to show their customer's trust. Certificate signing still happens at one centralized place in the lowest CA. Protocols used within the PKI originating from the CA require a high integrity/availability/confidentiality level. These levels are rendered with technical implementations that, in the end, render the trust within the CA. In this research, we dive deeper into using a new concept based on decentralization and what it offers from an economic perspective. These techniques and methods are discussed in the chapter "Why do we need digital trust?" and "What is the purpose of decentralization?". We apply these methods and look for better ways to improve trust. Within this thesis, we will focus on the trust from an economics point of view applied to the use case of a CA [10].

As decentralization itself can be very daunting and complicated, we will dissect the subject and look at the different aspects of decentralization—subjects like Consensus techniques, externalities, and concepts of trust are a few subjects we discuss. Building upon the research information within these subjects, we will discuss the advantages or disadvantages of a given technique.
The internet trust foundation is based upon the certificates from a handful of CA's [11]. This shows that users are connecting to a handful of trusted nodes. Each trusted node represents a trusted actor in the form of a CA. The vast majority of these actors are in for-profit as the main starting point. This incentive might not be in favor of the stewardship of the internet. [12] shows that economic incentives[2] have high importance on the assurance of the security of the internet. This same principle also applies to the CA. [13] shows that this problem is present today and in the earlier days of the development of the internet. The mentioned CA's will have a net effect of a 1 to many multisign. In the event of a failure in one of these CA's, all signed certificates behind that CA will be deemed insecure, as the malicious party might have issued these certificates.

In the current situation, the CA's have more information about certain trusted parties than the users of the trust from that CA. This creates an information asymmetry gap, which could lead to market failure in the end. CA's are currently the only authority that allows users to check other actors' trust. As this trust originates from the extra information present within the CA, it creates the mentioned information asymmetry gap.

[2] This form of economics refers to the financial and for-profit incentive.

Research Question

CA's offer us users trust on the internet, which originates from the highest level CA. As trust flows down from this CA, it has the trust of the highest level of CA. The trust at its highest level from the root CA is what we call the trust anchor. We use the definition of trust anchor to refer to the origin of trust in a particular system or network.
With the recent developments of new protocols and techniques regarding blockchain, we want to look at how these new developments could strengthen users' trust position on the internet. Trust originates from a trust anchor on the internet introduced by the IETF in the early days of the internet, the certificate authority. [14].

At its core, the internet was not developed for the masses and how we use it today. This led to the fact that many technical implementations and protocols were not ready for this usage. It is especially true on the security side of the spectrum. Sharing messages and sensitive information was done openly and in a transparent manner. This introduced a new problem; actors could listen and read these messages without receiving or sending parties' consent. To make this data transfer more secure, the IETF introduced SSL/TLS [15]–[18]. It allowed the users of this protocol to encrypt the traffic, which offered mitigation against eavesdropping. Message and sensitive information are now not readable by the actors who do not have the key to open the data. Data can now be sent secure and safe, but the problem of trust persists. Users of the SSL/TLS protocol cannot check the actors' digital trust he/she is communicating/sharing data with.

Still, we are unable to check identity and trust on the internet. We can share data in an encrypted way, but it is costly and inefficient to ensure the other party is the one he/she tells it is. This is where we need to improve the certificate authorities, as they are the ones with more information about these other parties. By improving the information asymmetry gap, the certificate authorities can help its users obtain a higher level of trust and prevent market failure in the end.

Certificate authorities offer the trust anchor we need in order for us to trust the other party. With this trust anchor, we can verify the certificate of the other actor. When we can successfully validate the other actor's certificate, we can trust the connection. It also shows that a trusted CA validates the other actor. As the certificate authorities offer different levels of trust related to different checks, we can check this as users of this system. When we go to our bank and connect, the certificate used within that connection Is based on a higher validation level [19] [20]. Different checks and balances are performed in order for the bank to receive such a high-level certificate.

We, as internet users, want to be sure that we are connected to a trusted party. We also want to be able to send our sensitive data in a secure manner. CA's offer the trust anchor we need in order to set up these validated/secure connections. Due to a centralized character and vulnerable offering of the current trust anchor, we have to build on a different method. We will look at improving information asymmetries by developing decentralization of digital trust via certificate authorities.

There are two main elements in play when we talk about information asymmetry between the CA and the CA users. There is a "**Signalling**" [21] element, and there is a "**Screening**" [22] [23] element. Signaling conveys information from one party (who has the information) to another party (with less information). Screening is the process where the party (that has less information) to induce the other party (who has the information) to reveal their private information. Both elements impact the balance of information asymmetry and allow the parties to get or show information to close the information asymmetry gap.

When we talk about the use case of trust on the internet, we have the users and the CA's. The CA is signaling information to its users in order for them to trust the third party. This third party is a party that is trusted by the CA. For the CA to trust this party, it has to screen the information on that given party. Once the CA has screened this party, it is trusted. Using this information signals its users to trust this party and therefore proxies this trust to its users(creating the trust anchor). The users of these systems are screening the information from the CA itself. Unfortunately, the information asymmetry gap persists. As the CA itself also needs to be trusted and therefore screened. This information asymmetry gap can lead to market failure in the event of CA failure(e.g., Hack, corruption, manipulation).

In order to improve the situation, it led us to the following research question:

How to improve information asymmetries by developing decentralization of digital trust via certificate authorities?

With these sub-questions, we try to get a better understanding of possible solutions to the main question.

- **Why do we need digital trust?**
- **What is the purpose of decentralization?**
- **What methods of decentralization are possible?**
- **Is it possible to improve the status quo?**

Research Methodology

This research uses desk research/literature study based on an economics analysis. Information gathered from academic sources is analyzed with an economics approach. This renders us a combined overview and enables us to formulate possible improvements to the current PKI digital trust ecosystem. This research aims to dissect the topics into smaller pieces and better understand how they work, formulate issues, and possible insight for improvements.

For this thesis, we have chosen between quantitative and qualitative approaches. Due to time constraints, we have chosen a qualitative research method. As the quantitative method offers a research method based on hard numbers and statistical analysis, we cannot answer the research question in the current formulated form. Qualitative research offered a research method that focuses on exploring theories and hypotheses that can be used and applied within the economics domain. It also enables us to answer research questions without the need for numerical data. It enables to answer the how and why question with the help of case studies. In this thesis, the methods of case study are based on the exploratory case studies. These case studies will be technical of nature and will add a different insight into the traditional way of economics research. The downside of these case studies is that they only apply to a small group of people, are not scientific, and can be biased from individual perspectives.

Within the first parts of the thesis, we lay down a baseline to build the thesis discussion. We tend to clarify every necessary part of the PKI we currently use with this baseline without going into in-depth technical knowledge. To keep this thesis readable and relevant to multiple different audiences, we have chosen not to go into deep technical details of protocols and technical implementations. Because this thesis has an economics starting point, deep technical details and implementations will not directly add to the discussion and proposals of the current PKI system's direct or indirect improvements.

This thesis describes distinct processes within the ISP, CA's, the PKI system, and the concept of trust in particular. These processes related to the delivery of trust or the PKI model add to the inner workings of economic processes we know and understand. These economic processes are the enabler for the actors delivering their services/products. These processes relate to actors, externalities, information asymmetry, and uncertainty. When we refer to these processes within this thesis, we call this the economics of trust.

The economics of trust is discussed regarding the certificate authorities and how they fit within the PKI current ecosystem. By clarifying different economic concepts, we try to better understand how and why we currently use a CA's (certificate authority) services. It also shows us how this is currently the "best-worst" trust solution regarding the externalities that took place during the development of the internet. We highlight the working of social aspects that play a significant role in the adoption of new technologies. It will help give more insight into how currently certificate authorities can transfer their current trust anchor into an origin of trust.

After clarification of the current trust model, we describe different consensus techniques. With these techniques, we try to understand the concept of trust originating from the given consensus techniques and apply them to our current trust model. The last chapter will discuss our current PKI solution's distinct outcomes and the trust outcomes from the consensus techniques. We will discuss how we can improve the status quo with these outcomes from an economic perspective.

Relevance

The COVID-19 pandemic forced us to transform our society in a digital way dramatically. Businesses, schools, universities, and other organizations are forced to move their current operations into a digital solution. The pandemic created a significant burden on the use of the internet and the infrastructure providing these services. Due to these developments, the digital infrastructure will change in different ways to support significant usage. With our current digital infrastructure, we as users can use the internet safely and securely.

Due to the research's multidisciplinary approach, we try to add a new angle of approach regarding the research of digital trust and propose an improvement. Technical insight/background gives the research a different approach compared to other economic papers regarding this subject.

The relevance of this research topic is determined by the requirement for trust in digital systems. As the burden on the CA's keeps growing, the systems need to scale with it. Earlier failures of CA's have shown the vulnerabilities of the trust present in our current PKI. Due to these failures, we can state that this trust's certainty is affected negatively. In order to strengthen this trust, This research's outcomes might be relevant for scholars, professionals, or economics who benefit. As they are the actors who develop and help strengthen/steer the PKI ecosystem's current developments.

Furthermore, this thesis shows prospects that help to research this topic further. The technology discussed is in its infancy stage and is currently only used in specific domains. With the help of this research, we want to show the relevance of the discussed technology. We also want to show the level of illumination of the discussed topic. Currently, the topic is widely known but not frequently applied in different domains [24].

This thesis is relevant for all those who use the PKI x.509 system and those who use certificate authorities' services. As this user group is extensive, the relevance is substantial. Outcomes of this research may perhaps influence scholars, professionals, or economics working on applied projects. Therefore, changes in these projects might impact the users of the current PKI x.509 system.

Furthermore, the insights from this research are very relevant for those who offer PKI x.509 services. Certificate authorities and parties alike can benefit from these findings and apply or steer their current operations.

The developing community might also benefit from these findings, as these add indirect food for thought value and future-proofing of their products.

Limitation of research & Future research

Limitation of a multidisciplinary approach:
This research will not focus on technical details and deep inner working of discussed protocols and technical implementations. This discussion will not directly add to the answering of the research question. The writer's technical background is a benefit on the technical side but a limitation on this thesis's economic side. Therefore the writer has to read up on this topic to add a different angle of approach from the economic sight.

Limitation access to data:
Limitation of research method, no interviews or questionnaires have been conducted. This limits the research to case studies that have already have taken place. It limits this thesis to historical-based events.

Limitation time constraints:
The Leiden cybersecurity program gave time constraints. These time constraints limited the overall research done. Reading up on different disciplines limited the thesis's actual work, limiting the overall research on different topics. Due to a lower level of experience in these disciplines, some elements might be underexposed. Due to time constraints, we were not able to compare different adoption models or other theories that apply. Due to time constraints, it was costly to compare many different consensus algorithms and apply them to a CA use case. Ultimately, this led to a limited representation of the whole subject regarding the decentralization of digital trust. Further research is recommended to reflect a direct representation of reality.

Limitation of personal bias:
Due to personal trust bias and belief in philosophy related to blockchain technology, personal bias might influence counter argumentation. This limitation influences the discussed topics within this thesis. It also renders a select outcome and use of specific sources that strengthen the position and use of blockchain technology regarding trust from certificate authorities.

Limitation of early-stage development:
As the developments of blockchain technology are in their infancy, new developments could offer better improvements. These new developments could offer a new insight during research with different outcomes.

Structure of the thesis

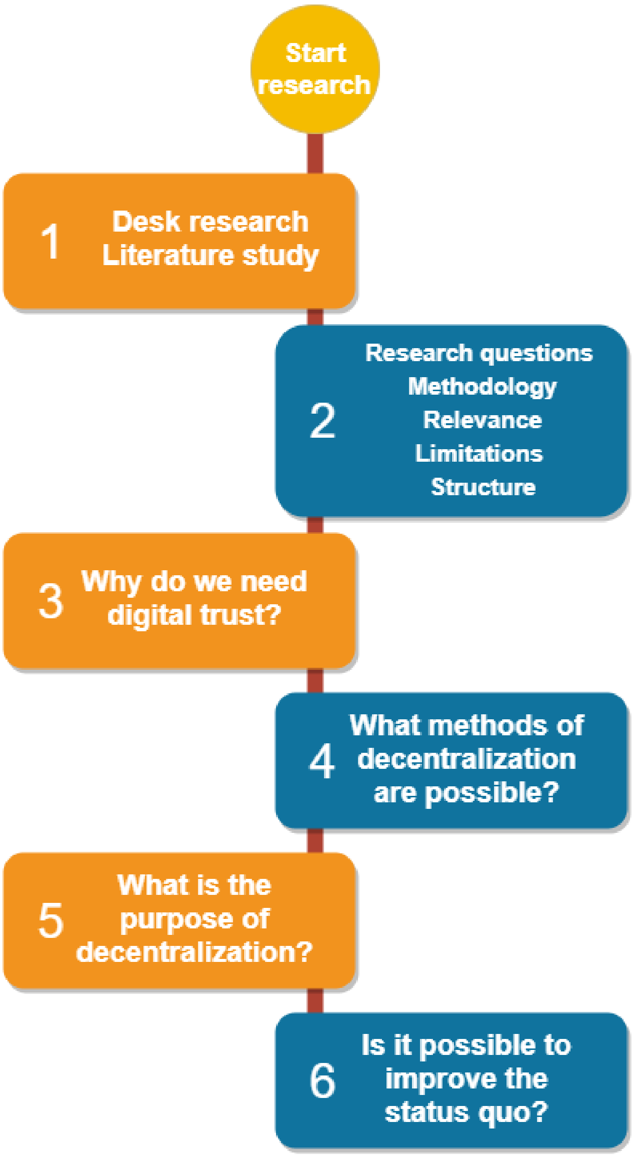

Start research
1 Desk research Literature study
2 Research questions Methodology Relevance Limitations Structure
3 Why do we need digital trust?
4 What methods of decentralization are possible?
5 What is the purpose of decentralization?
6 Is it possible to improve the status quo?

Figure 3 - Thesis structure

The structure of this thesis is based on the research sub-questions. As these sub-questions try to answer a part of the main research question, it perfectly fits the formatting. Each chapter tries to give a better picture in regards to the main research question.

For some of the sub-questions, some elements are highlighted with **bold** text. These elements discuss parts of that given sub-question or try to get more attention from the reader.

For references, we use the IEEE standard. This standard allows us to keep the text clean and clutter-free. To find the corresponding source, they can be found in the last chapter (references).

Within the thesis, we use many different abbreviations. The first time an abbreviation is mentioned, we will fully spell the word in question behind the abbreviation.

If more explanation is needed about a specific topic or wording, we use inline references on the page itself. These references look like these[3] and can be found at the bottom of that current page.

For each figure, we use number referencing. When we refer to a specific figure, we will refer to the corresponding figure number.

In figure 1, we can see the structure of this thesis.

[3] Example inline reference

Why do we need digital trust?

We just covered the structure of the thesis, the relevance, and the main question to try to answer with the sub-questions. With this in mind, we will start laying a baseline for the research question. In the following chapter, we will lay down the fundamentals of economics applied to the research question. We will cover relevant actors that apply to the use case of the certificate authorities and their services. By clarifying these actors, we can better understand who digital trust is relevant to and how economic aspects play a role. We take a look at an economics example applied to the ISP stakeholder. With that example, we try to give a better view of how stakeholders are connected and dependent on each other.

Furthermore, we will discuss information asymmetry and how it can be applied with decentralization in mind. Terms like signaling and screening show that stakeholders can check or show information to close the information asymmetry gap. Applied externalities show the development of various hardware/software implementations. We will briefly show examples of current blockchain-based projects that try to improve the current PKI solution fully or partially.

With these different subjects within the introductory chapter, we give a better overview of the current situation and why there is a need for digital trust.

Introduction

To get a good grasp of digital trust economics, we have to understand where we need digital trust. Nowadays, we are using the internet more heavily for our daily jobs. It enables us to make foreign trade, share information, read the news, improve products, collect insight, and much more. Especially with the current pandemic COVID-19, there is an increased burden on the use of the internet. As the internet enables us on different levels, it also economically enables us. With the help of the internet, foreign companies and services are right at our fingertips. It gives us a broad new offering in products and services and allows malicious parties to exploit us through digital means.

To make the internet a safer place, we need to implement safety measures that keep the users safe. Our internet service provider (ISP) gives us a router with an integrated firewall and stops most online attacks. Unfortunately, our digital systems get attacked [25], but we also get attacked on a social level.[4] It shows that new sorts and forms of vulnerabilities allow malicious parties to abuse their victims. New forms of attacks, but also new forms of services/products, are offered. It shows new economic forms regarding this danger and a new form of economics for the attacking party. Without the internet, this malicious party is not able to conduct these kinds of attacks. Without the internet, the internet service provider would not have existed or offered useful products.

[4] This refers to social engineering which allows an attacker to exploit and execute different malicious activities. This is accomplished with human interaction, and involves psychological influence.

In short, this shows that there are multiple different stakeholders connected to the internet. These stakeholders come from worldwide, offering new services/products and a new form of threat. Local or foreign companies develop new products and have foreign sales markets. These merchants can or might not even have local sales markets and could only live from their income with the internet's help. New digital-only markets can only exist with the help of the internet. When we look at the primary income for most prominent digital companies like Facebook, Google, YouTube, and others, it exists for the most significant part out of advertisement revenue. These stakeholders have different incentives with the internet and use it within their business model [26].

Internet users are vast. It can be an individual user, a company, a government, or any other organization. All these users fall within the scope of three different actor groups:

Engineers/developer perspective: These actors help develop the internet and its security. These actors propose new protocols in order to secure the internet and make it a better place. They help create better and secure software, write new standards, improve encryption, and more.

A government perspective: These actors look at the internet based on the activities conducted by users. They check and want to know more about the legality of these activities. If activities endanger the nation's security, endanger national interests, jeopardize local companies' security or private persons, they want to intervene where possible.

Market perspective: These actors look at the internet purely as a trading ground and want to create efficient economic mechanisms. The incentive is to generate digital markets with economic starting points.

Consumer perspective: These actors look at the internet based on their form of usage. This can be the subscription to a streaming service, buying a product online, using social media, and more.

When we look at market incentives regarding the use of the internet, internet service providers (ISP's) (Or other businesses) put different domains to deliver their services to their customers. These domains originate from cybersecurity-related issues and can directly be connected to their respective end-goal/utility perspective:

Availability: "*Can we use the service without interruptions*?". "*Can we offer the service without hiccups, and how are we going to implement measures to stop hiccups?"*. High availability is one economic example of how ISP's tend to cover this area. Without high available systems, it is tough to offer a high uptime for certain services. Furthermore, the economic aspects that come into play during the setup and purchase of the hardware/software show that this domain can have a significant economic impact.
High available systems are redundantly put in place. The way this is done is dependent on the application and service level agreements (SLA). Systems that need a high uptime implementation are implemented with multiple layers of hardware. This implementation has a higher cost for the ISP and, in the end, a higher cost for the customer [27].

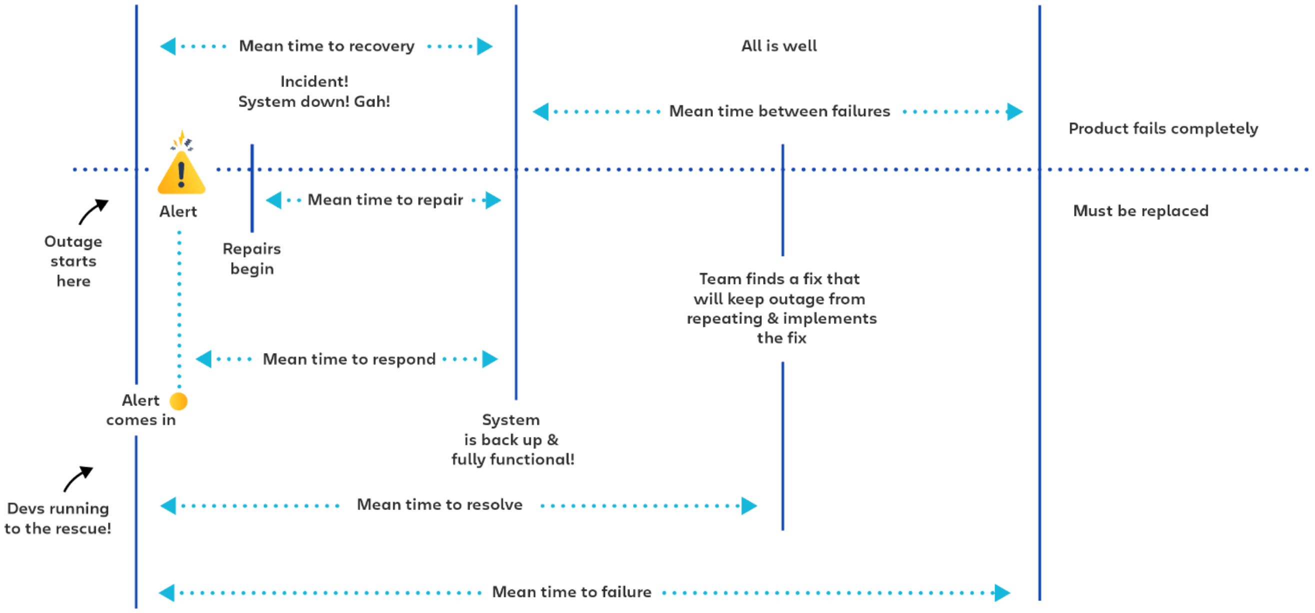


Figure 4 - MTBF, MTTR, MTTF, MTTA incident metrics
[28]

Figure 4 shows how the different incident metrics work. These metrics are essential for the customer, but also from an economic point of view. These metrics can be used to plan for specific hardware/software implementations/solutions. With these hardware/software solutions, the ISP can check and validate the improved situation with the incident metrics. With the help of these metrics, the ISP can communicate these numbers with their customers. Using different SLAs and their corresponding incident numbers, the ISP can offer different SLA support levels.

Integrity: "*Can we trust the data we are storing, and is de data untampered?*" As the ISP will store different forms of business/consumer data, this data is sensitive. In order to provide the customer with the correct information, mechanisms need to be in place that proves the integrity of that data. If a malicious party can alter the data, the value of the data is lost. This also renders a lower quality of service as the data integrity cannot be offered. The ISP can offer higher SLA levels that guarantee data integrity. In return, the customer has to pay more for the given service. This economic aspect is linked between the customer and ISP and between "the customer's customers" [25]. Businesses that use the services of an ISP also have customers. The customers rely on the same domains within that business. We will go deeper into this "chain of economics" later in the document.

Confidentiality: *"Can we protect the data from unauthorized parties?" "Can we protect the data from actors that do not have the rights to see this data?"* As an ISP, it is mandatory to protect sensitive data from actors who do not have the right to see this data. Without this protection, it is costly to protect the data, customer data would leak, and customers will not take the ISP seriously. Furthermore, the implementation of the new GDPR could pose prosecutions for the ISP in such events [29]. Access Control Lists, File permissions, and other access control implementations offer the confidentiality the ISP need. Third party software developers offer protocols and implementation that are used to offer this domain. The development incentive can be economical from a financial standpoint or to add to the community. Opensource projects and developments add to the development and maturity of these different domains. The open-source community is a unique subject within the economics world, especially when we look at it from a financial standpoint. As there is no direct monetary return for the work done, the open-source community focuses on other standpoints. Other standpoints like freedom of sharing and ethics shed more light on why these developers add to the community and the whole concept around open-source economics [30].

Identity: *"Do we know the other party we are talking to, and do we trust him/her?"* With the help of an identity, we know who where are dealing with. The ISP is an organization that exists out of different staff members. The customers from the ISP can be very diverse, as they consist of companies and consumers. These stakeholders are diverse individuals that have different or similar interests. Using identities within the economics point of view, we understand whom we are talking/trading/sharing. Without this identity, it is tough for us to build trust[5].

Chain of incentives

When we look at the different domains described above, we can see those different stakeholders rely on each other. Without the service of the ISP, the business that uses that service cannot offer his service. Multiple stakeholders use internet services from the ISP. With this service's help, it enables them to conduct business in a different and new way.

This example of a chain of incentives is also present for the ISP. The ISP uses hardware and software to make services possible for its customers. As the ISP tries to be compliant with all the domains mentioned above, its investments can be very high. These investments come down to hardware and software that enables the ISP to offer its services. Different levels of investment are based on the needs of the customers coming from SLAs. In the case of the ISP, the hardware/software enables the enabler.

The shift of this chain of incentives is happening very quickly, as businesses try to find a new and modern form of revenue by shifting to a digital presence due to the COVID 19 pandemic. This pandemic, traditional trade (partially) shifted to the digital version and enabled some businesses to get higher revenue. This forced economic shifts for some businesses enabled and enabled new revenue for others. Once we change one thing in the chain, it affects the other side of the chain [31] [32].

Due to the increased burden and usage of the ISP's internet service, this service is now mission-

[5] We will go deeper into this subject in the second chapter

critical to some businesses. Without this service, these businesses are not making any revenue, and business will be stopped. Investments made by the ISP can be costly and will not be done for every customer. Therefore, the ISP is offering different SLA's(Service level agreements). These so-called service level agreements are a perfect example of economics, as they offer a higher level of service if the customer is willing to pay more. The ISP is offering certainty in the different domains and quantifies them with numbers. Each domain service level is agreed upon and used to create a contract between the ISP and its customer. In the event of a systems failure or service failure from the ISP, steps will be taken to compensate the customer.

The level of certainty that is sold to the customer in the form of an SLA is also present in other ecosystems. When we take a look at the online advertisement networks, certainty is something that is very interesting. With the help of this certainty, advertisement networks are able to generate more revenue. To get this certainty, we have to find the right place to ensure the advertisement is seen. Social networks or other heavily visited websites are an excellent example of such a place. As social networks have a big network of people and many data about these people, they are the place to get this certainty. The social network knows which interests certain persons have and where and how to place advertisements [33]. For business, it is the perfect place to place ads and have guaranteed revenue. This example shows a perfect representation of how certainty can be used as a business model. The fact remains that the ethics behind this kind of certainty is debatable and if this should be done or not. To not go into a whole different subject, we only touch the surface of this specific economic development.

Besides the different domains discussed earlier, we can see that more elements come into play when talking about economic chains. Each business has its core business and its unique way of creating revenue. These forms of "creating revenue" mix with the domains mentioned above will give us a new insight into how new/current businesses create new economic chains. Once a business finds a new economic chain, other actors can join/sell/connect to this economic chain. For example, a small start-up company creates a new digital payment form, and another company makes payment cards. Both companies can connect in order to make each other more relevant. The small start-up can start offering physical cards for the new digital payment system.

Information asymmetry in a nutshell:

Information asymmetry induces a form of imbalance of information possession between two parties. In the case of a trade, a seller might have more information about a product. This can also be the case in a reversed way; the buyer might have more information about the product. In such cases, decisions that are made during transaction might go wrong or create a market failure. Information asymmetry is significant for our current digital trust system [21] [23].

These parties have a different amount of information available about the product. One party is **Signalling** information, and the other party is **Screening** information. Without the screening and signaling process, it would be hard to close the information asymmetry gap. Users do not have the resources (time, knowledge, experience) to check the risks and benefits connected to specific technologies. The information asymmetry is considerable for users of a service/product. They did not develop/create it themselves, making it very hard to invest all resources to understand all concepts. To evaluate certain technologies' risks and benefits, we look at experts (users, experts, developers, stakeholders, and others) to give us an assessment. We can evaluate ourselves if we want to use/buy a particular product/service with this assessment. This assessment needs to be trusted to be useful for us as users. Without this trust in the experts, it is tough to bridge the information asymmetry gap [34].

Decentralization and information asymmetry:
To understand how decentralizing technologies can help fight information asymmetry, we begin by looking at George Akerlof's theory. This theory described the information asymmetry that is present within the car market. In this market, the car seller knows all about the car: how it rides, which parts are good or bad, the actual mileage, and more. The car buyer does not know this and can only see the seller's data available and shared. This disbalance of information knowledge between the seller and the car buyer is called information asymmetry [35]. Akerlof called this market the lemons market, as some of these cars might be a lemon and have a bad history or perform poorly. The lemon buyer does not know this until he bought the car and starts driving it. It shows that the buyer cannot assess a product's quality before he/she buys it.

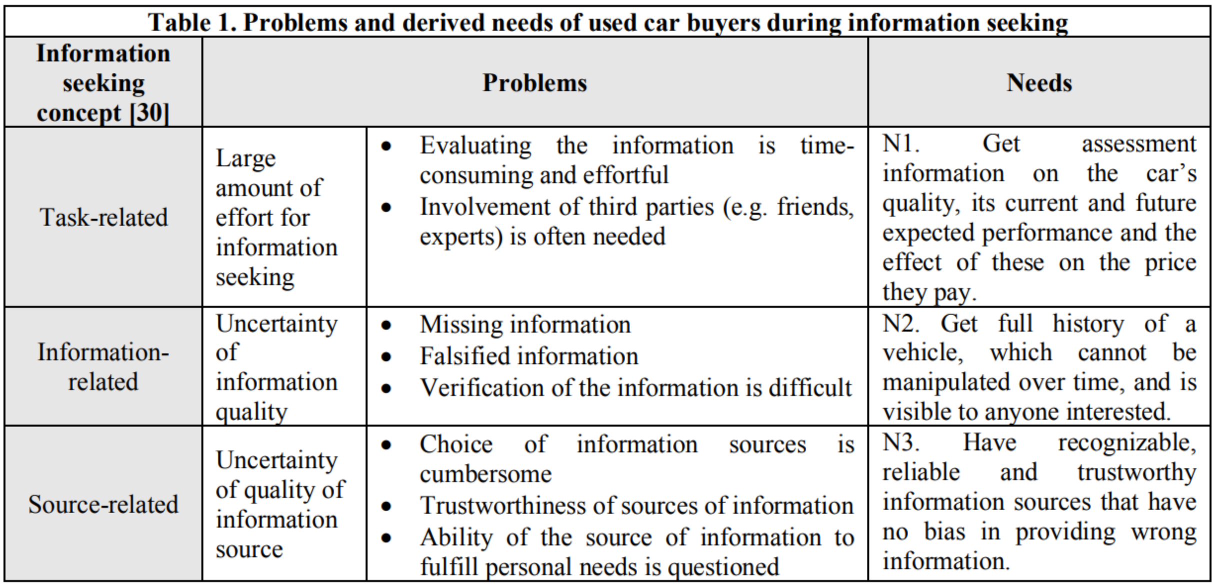


Table 1. Problems and derived needs of used car buyers during information seeking

Information seeking concept [30]	**Problems**		**Needs**
Task-related	Large amount of effort for information seeking	• Evaluating the information is time-consuming and effortful • Involvement of third parties (e.g. friends, experts) is often needed	N1. Get assessment information on the car's quality, its current and future expected performance and the effect of these on the price they pay.
Information-related	Uncertainty of information quality	• Missing information • Falsified information • Verification of the information is difficult	N2. Get full history of a vehicle, which cannot be manipulated over time, and is visible to anyone interested.
Source-related	Uncertainty of quality of information source	• Choice of information sources is cumbersome • Trustworthiness of sources of information • Ability of the source of information to fulfill personal needs is questioned	N3. Have recognizable, reliable and trustworthy information sources that have no bias in providing wrong information.

Figure 5 - Lemons market buyers assessment
[36]

We can apply the same theory to many different technical implementations nowadays, as the users of these technical implementations do not know how the software/hardware works and if it is any good. We as users do not have to know the ins and outs of protocols, hardware, and software, but it shows that users are not always aware of the lemon or the good protocol/hardware/software implementation[6] to use. The same information asymmetry theories apply with the use of these technologies [21] [23]. Tech companies signal their technical implementation as safe, and customers need to screen this to trust and use these products. This also applies to gadgets; people do not know what technical implementations are present within that device and if it is safe at all. For most users, "*it just needs to work*" is the main starting point of using a technical implementation. "*It just needs to work*" incentive can be linked to the Technology Acceptance Model (TAM) model.[7] The fact that users have this starting point is not something out of the blue. It is normal behavior because they rely on the expertise of professionals selling or recommending technical implementations. Because the user relies on this professional, the "*knowledge gap*"[8] grows [37].

[6] We refer to this as technical implementation
[7] In the next chapter we will discuss this TAM model in more detail
[8] Other method of defining information asymmetry

In order to apply the theory of Akerlof to decentralization, we have to look at the aforementioned information asymmetry and how decentralization can improve the current situation. Due to the technical nature of blockchain technology, information asymmetry and product uncertainty can be drastically reduced. By reducing both information asymmetry and product uncertainty, the buyer and seller are able to build a stronger trust relationship. Some studies explore these benefits, applying the benefits of blockchain to improve real-world problems within the car market [38]. As this example shows the benefits of cars' history, we can also apply these benefits to other domains where the same information asymmetry is present. One of these domains is the main starting point of this thesis, digital trust. Currently, this trust is provided by CA's. The information asymmetry part here is that the CA's recognizes to trust or not to trust a specific party. This trust originates from checks and balances a CA conducts.[9] Users did not perform these checks and balances and did not own this specific information. In this case, the CA is **signaling** trust, and the users of the system are **screening** trust [21] [22] [23]. These users trust the competence of the CA, so they can safely communicate with the trusted actor. This centralized trust is only present from a CA and is hard to verify. Therefore, improvements were proposed to allow users to get a higher level of trust. Example of current/possible improvements are shown below:

Examples of protocols:
Users currently rely on PKI x.509 to solve this trust issue. Due to the current PKI x.509 system's centralized nature, problems like the inconsistency of identities arise. This means that malicious parties could issue certificates in the case of a successful CA hack. Without the knowledge of the user, these malicious certificates are trusted and can be used on different websites. In order to detect these compromised or inappropriate behaving CA's, there are technical implementations that offer transparency for the users of the CA:

Certificate Transparency (CT) is a transparency solution offered by Google to allow users to check compromised or inappropriate behaving CA's. With the help of this list, the browser can check the validity of the issued certificate. By using the Markle tree algorithm, logs of certificate issuance are added to an append-only log. Using the Markle tree algorithm can prove its consistency the same way specific consensus algorithms work within the blockchain [39]. This method is a perfect example of signaling information from the CA's towards their users. This method allows the users to screen the information that is coming from a specific CA. With the help of this information, the information asymmetry gap is smaller.

Accountable key infrastructure (AKI) is an alternative example that uses a public log to increase transparency. AKI uses public log maintainers and validators to monitors CA's. With this method, AKI tries to reduce the level of trust that resides at the CA's. Unfortunately, the AKI implementation shifts the trust from the one third party to the multiple. This spreads the overall risk but does not improve the current situation. With the help of this alternative, users can screen the CA with a third party's help. One big downside is that the same information asymmetry gap is present between the user and this third party.

As there are more technical examples to show the current improvements, the main point is that there is a consensus about the necessity of transparency. Different technical solutions offer a hybrid solution between the centralized trust and the authority of the CA's. As this offers a better form of trust, this is not the solution to the main problem. CA's still happens to be the central weak point of this system [3].

[9] These checks and balances are discussed on page 30

Examples with use of blockchain:
CeCoin is an example project on how the blockchain can improve trust for online users. CeCoin is doing this by implementing the lifecycle of a certificate into a blockchain [40]. In the case of CeCoin, they try to improve online users' trust levels by proposing a different implementation of authority within the PKI[10].

CertCoin is another example to improve the current x.509 PKI system. With CertCoin, an alternative decentralized authentication scheme is proposed. This is done by creating a public ledger in which all domains and their respective public key are stored. This helps to authenticate these domains during a connection between it and a client [41].

Handshake is an example of how decentralization could offer a trust anchor between the names (domain names) and certificates. This is done with a network of consensus based on proof of work. How these consensus proofs work will be discussed in the last chapter. According to the website of handshake [42] they are an experimental, decentralized naming and certificate authority. They are still in development, and the protocol is in its infancy.

As we only described a select few technical implementations that offer a current or propose a future improvement, it shows that our implementation current and future implementations of trust have not matured yet. It also shows how different protocols grew and became more mature when they got used in different contexts[11] [43]. The new decentralized implementations offer the trust anchor from a different/innovative/new context. The figure below shows blockchain technology's characteristics and how it tries to fit in with the trust anchor. With these characteristics, we can bridge the information asymmetry gap and share information in a trustworthy fashion.

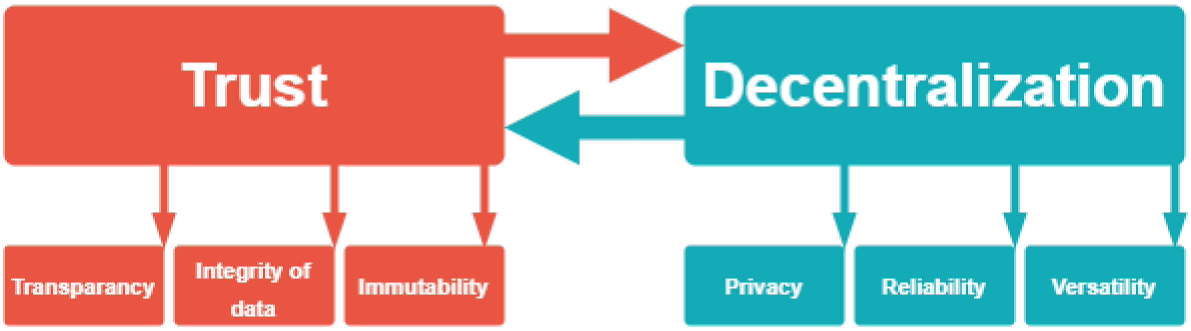


Figure 6 - The characteristics of blockchain technology
[36]

[10] How this authority is a centralized entity will be discusses in a later chapter
[11] With different context we refer to the use of the internet by a bigger audience (the internet as we know today)

Traditionally with the help of tools like user reviews, expert reviews, and other business solutions, we as users can bridge the information asymmetry gap. Businesses saw opportunities to create a business model out of this concept. Businesses like: Trustpilot, TripAdvisor, Google reviews, and more allow users to fill the asymmetry gap. Nowadays, we see that companies implement user reviews/ratings on their website themselves. In eBay's case, we can see another user's rating and see if he/she is trustworthy [44]. Both systems are trying to induce trust, one system is inducing trust between customers and the company, and the other system induces trust between customer and customer.

Externalities

Within the digital industry, there are multiple forms of externalities. In simple terms, an externality is an effect a service/implementation/protocol/hardware has on others due to organic growth that service/implementation/protocol/hardware implementation. It remains unclear, but we will clarify the meaning regarding two different externalities in the next paragraph. We have two different externalities: **network externalities** and **externalities of interdependent security**.

Network externalities:

When we look at the ISP company from a previous example, we understand that it has many different software and hardware implementations. All these implementations need to talk to each other on the same level. Using protocols that are standardized and known helps a lot within that ecosystem. Different hardware/software vendors will implement these protocols in order for their product to function. As the ISP has many hardware/software, it can be smart to choose the correct hardware that talks the same protocols. Without this implementation, the investment would be worthless.

Furthermore, choosing this hardware/software can be interesting in regards to other companies. When another ISP business needs to talk to the hardware/software of our ISP, these systems must understand the protocols and implementations. This also shows why the IT industry tends to lean towards big and dominant IT firms for their hardware/software implementations. The main reason for this trend is the fact of network externalities. If you choose different protocols to implement, the chances are that you, as an ISP company, might not be able to deliver the services.

The same principle applies when we, as users, are selecting an operating system. We know Windows and Apple as they are widely known within the IT world. As a user, if you choose a whole different operating system that is unknown, chances are software is not written for your operating system. As the userbase of this chosen operating system is tiny, companies are less likely to develop software for that operating system. A perfect real-world example might be the mobile operating system from Windows. This operating system worked perfectly and had its charms, but the userbase was not as big as those from apple and google. Therefore, apps and software were not developed at the same level of volume as those apps and software for apple and google operating systems. This also clearly shows that the chain of economics from dominant IT businesses is more attractive, as these companies will deliver a more significant userbase. A bigger userbase will, in the end, result in a higher volume of revenue.

Besides the fact that the higher volume generates more revenue, it introduces the vendor locking phenomenon [45]. As dominant companies want to stay dominant and create an even more significant userbase, new protocols and implementations are added. These protocols and implementations will offer an improved experience but will only be available once the customer chooses the company's products. In essence, the company delivering the service will be dependent on the hardware/software from this vendor. A simple example of vendor locking: A company buys new printers for all its departments, but the printers only use cartridges from the original vendor [46].

A great example of network externalities are visible within the adoption of newer network protocols like DNSSEC and S-BGP. These protocols add an additional layer of security on top of the current solution. As the security benefits only show when other actors also switch to using this protocol, the urge to adopt the protocol is not high. After the user group's most significant part is switched and a direct impact for the switching actor is there, more and more actors will adopt the protocol. It has to directly impact the actor; without this return, there is no immediate need to adopt, as there is no direct return for this actor.

Externalities of interdependent security:
The ISP company is dependent on other companies for infrastructure and software implementation. This creates a new form of externalities regarding interdependent security. Within the info security (infosec) world, it is commonly known that the strength of your security comes down to the strength of the weakest link. The weakest link could be a software or hardware implementation that is coming from a third party company. The ISP is willing to invest in its security; this depends heavily on the market's security incentive. As some of the security investments are dependent on the SLA's (what the customer wants to pay) and its market competitors (Market norm), there is a possibility that the ISP will not invest in the security measure [47]. Furthermore, the externalities that come with different security implementations of hardware and software create a significant ISP dependence on the software/hardware vendors.

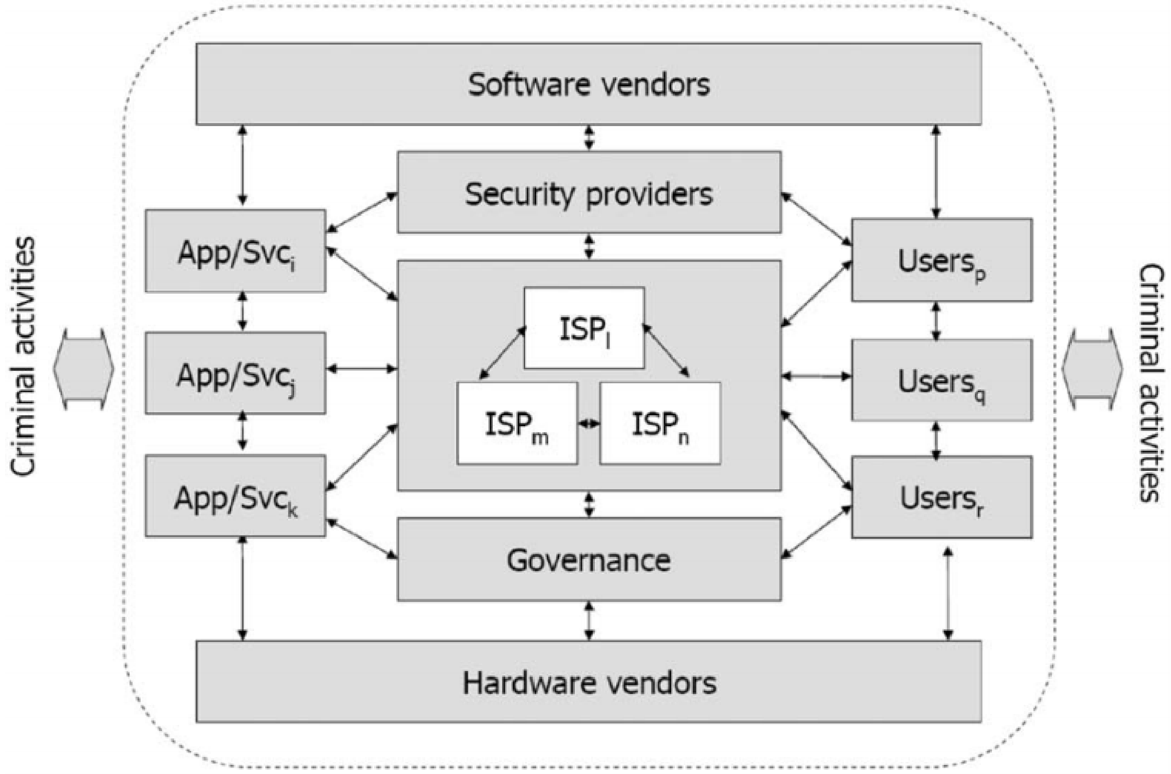


Figure 7 - ISP interdependencies
[48]

In the figure above, we can see the interdependencies for the ISP and its different stakeholders. We can state that the infosec world's interdependencies are present at the service/product level and the security level. Therefore, it is of high importance that every hardware/software vendor is implementing the latest security measure, as these measures will directly flow down on the customer's customers. This interdependent security model is described in [48] and is still very relevant today.

Actors:
Within cyberspace, there are a lot of different actors that have a direct or indirect impact on the development of externalities. Furthermore, all these different actors benefit from these network developments directly or indirectly. The ISP, customers/users, hardware/software vendors, developers, opensource community, and governments, to name a few of these actors. These different actors have different roles and different authorities within the space. One of the most important actors in the IETF (Internet Engineering Task Force). The IETF is a constitute that develops the protocols and standard for the internet's inner workings. With the help of the IETF, the internet is something we know as is of today. As the IETF is an engaged constitution with protocols and technical standards, they are well known within the internet community. For the users of the internet, it "just needs to work." Users do not want to get into the technical details[12] and will not know actors like IETF.

Other actors have to use these and implement them into their products for the protocols and technical standards to work. Hardware and software vendors need to comply with these protocols in order for their products to work with other products. Without the implementation of these technical standards and protocols, products from different hardware/software vendors would not be able to communicate with each other.

The IETF writes an RFC (Request for Comments) document to discuss and publicize new internet protocols and standards. With the help, a working group, the RFC builds and publicized [49]. Every working group has a specific domain and expertise in which they conduct research. Each RFC has its reference number, which can be found in a public list on the IETF website. The PKI standard's RFC number is 5280 and describes the inner workings of the PKI we currently know today. Within the RFC 5280, it is described that a CA is responsible for issuing the certificates [14]. This shows that the core concept of a CA came from the IETF itself. This also shows that everyone who is willing and able to participate and create technical standards and protocols can add to the internet's core workings. It is also stated in [50]. The IETF sees everyone as an individual and not as a company. In order to add to the internet ecosystem, we have to keep in mind the rules defined in RFC 8179, as these are mandatory regarding intellectual property. In [51], we can see that the mindset behind the IETF is open and willing to add to the core of the internet. You as an individual need to add to internet community as the main starting point.

[12] Rely on expertise of experts. Same for driving a car, you don’t want to know all technical details of the car if your incentive is to go from point A to B. The car just needs to drive.

Authority:
When we look at the digital trust authority on the internet, it is described to come from the certificate authorities, as they offer the trust we need to trust other actors on the internet. This authority has the power to issue or not issue specific certificates.

In regards to the information asymmetry concept, the CA, in this case, has a lot more information about a trusted party. The CA conducts different checks and balances to conclude if a party is trustworthy or not. The details of these checks and balances are not/partially shared with the user of this trust[13]. For the end-user, it is hard to check the service quality of a CA [26]. In chapter two, we will dive deeper into digital authorities.

Furthermore, the concept of authority has a different meaning when we are looking at it from a decentralized character. The authority that comes from a decentralized implementation originates from a consensus protocol. This protocol describes all characteristics of that blockchain: rules, regulations, governing roles, and more. Adopters of different blockchain projects are attracted to the function of this authority, as this function is put into a consensus protocol and is not originating from a single entity. The core authority that originates from and consensus protocol is based on an algorithm. This algorithm is accepted by all parties that use that specific blockchain. We can state that the role of authority has changed from its traditional connotation to algorithmic authority. This algorithmic authority is not controlled by a single person/business but is collectively developed by a group of developers with the same starting point as to how the algorithmic authority should work [14] [52].

Another development of authority is linked to aggregation theory. [53] shows that by delivering the best user experience, you can attract a big group of users. Once this user group has grown to a certain level, companies start to adjust their distributors/aggregators/market-makers to win more users. When we look at Facebook, for example, this company offers advertisement space to its customers. Previously targeting of customers was done by the company itself; nowadays, Facebook sells a form of certainty to its customers. This is done by using its users' profile data, allowing them to pinpoint the customer's target audience directly. This method of business made businesses like Facebook, google, amazon and Netflix big. Because these companies grew so big, they in essence, became an authority within the economics of advertisement markets. As a small company, when you cannot adapt to this method or use old methods, chances are that it will be less successful. This form of certainty Is very successful in the advertisement marketplace and allows big companies to get even bigger. If we apply this certainty model to a CA, the chances are that this business model is more successful than the current CA's business model. This model will deliver a form of certainty and, therefore, close the information asymmetry gap between the user and the CA customer, lowering the chances of market failures due to lower levels of information asymmetry.

[13] More on these checks and balances in a later chapter.
[14] In a later chapter we will elaborate the working of different consensus protocols, that clarifies its connection to authority

We use online and digital systems more and more for our daily processes. These processes can differ a lot as a lot of new processes are getting digitalized. A well-known process is trade/commerce. This process used to be a physical process where the buyer and seller came together and traded different products. Within this process, there is a trust relationship between the two parties. Without this trust, the buyer cannot be sure about the product's quality or the trade itself. It also includes statements/claims about products. If a buyer cannot trust the seller on these statements/claims, the trade will become very hard. Trust has to come from both sides and leave both parties in a vulnerable state. As each party has to trust the other party, a possible exploit of this vulnerability is easy. Once this vulnerability gets exploited, and the other party knows about it, the trust between these parties breaks [54]. The trust problem is a core issue of information theory. This research focuses on the trust issue regarding digital trust, but the trust issue resides not only in digital trust. This shows that the trust issue is a deeper issue overlapping other topics [55].

Trust – "*Psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behaviour of another*" – Rousseau et al. [56].

Within a local community or region, buyers are aware if traders are trustworthy. When a seller tries to scam or damage a potential buyer's trust, this party will likely talk about this. Other potential buyers will be colored and are not likely to buy products from this trader. This organic word of mouth spreads around a community and will inhibit trades for this trader. This "local community or region" is not present within the digital world. The online trade/commerce world offers worldwide trade and is not bound to space and time constraints that had the be dealt with in previous physical markets. This also shows that trust factors have become a lot more critical, as the market is worldwide. Once a trader gets a bad reputation and is not trustworthy, his/her worldwide sales market will diminish very quickly [57]. IT solutions are the enablers of digital reputation systems. This lowers product uncertainty and allows the buyer to lower the information asymmetry gap. It shows that IT can play an essential role in regards to the lemon market model.

To get a better understanding of the concept of trust, we dissect trust into four different characteristics:

- **Trust and trustee:**
  Within each trust relationship, there is a minimum of two parties. This is the trusted party (trustee) and the trusting party (trustor). Both parties can exist out of a single person to a group of people that represent an organization. To build trust between these two parties, the trustee must act in a way the trustor has his/her interests.
- **Vulnerability:**
  The trust itself is based on the vulnerability the trustor poses him-/herself. Trust can develop the quickest in an uncertain and risky environment. When a trusted party poses him/herself in an uncertain/risky environment, he/she needs to rely on the operation of the other party's trust. When done successfully, both trustees did not exploit the trust and build a trust relationship.
- **Produced actions:**
  Building this trust leads to action that can be tangible or intangible. Lending a car to a friend is a tangible trust relation, as the car can or cannot be brought back in one piece. Trusting a friend that he/she handles the car with care. A married couple is an intangible trust relationship; both parties trust each other to be loyal. In the case that one of the persons in that relationship abuses this trust, it is broken.
- **Subjective matter:**
  As trust is a subjective matter, each actor sees the trust differently. It can lead to different reactions and different situations. Different magnitudes of trust can be invoked in the same situation by different parties.

Trust is also a concept based on the userbase of a specific product or service. It has a significant impact on the use of a specific product or service [58]. As users get more trusted with a product or service, they tend to use this product/service more. With the introduction of the internet, the sales market got significantly more prominent. New payment systems offered customers a new way of digital payment. Research done by *Oskar Szumski* shows a link between the level of trust and the level of usage. Figure 4 shows the resemblance between the level of trust and the popularity of use.

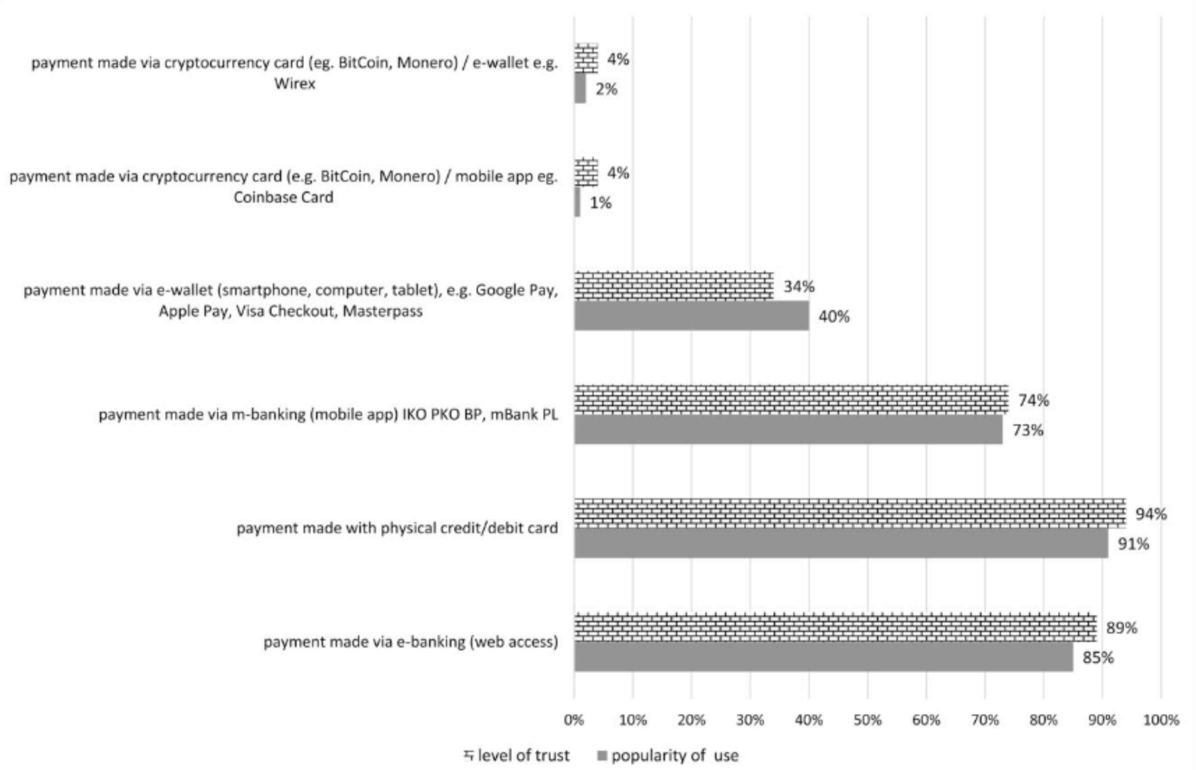


Figure 8 - Popularity payment method and level of trust
[58]

As well-known payments services have high popularity, they also have a high trust rate. The new and upcoming digital blockchain payments have a lower level of popularity and a lower level of trust. This level of trust is linked to the popularity of use. In this case, the digital blockchain payments are the service that is offered to the customers. Further research is needed regarding the drivers and accelerators. These drivers and accelerators can be vital to introducing higher popularity levels, thus increasing trust regarding these new services.

One of these drivers and accelerators is digital trust. Digital trust is a concept that will be part of a new paradigm shift. As industry 4.0 is driven by human-centric trust in digital trust, the way new companies implement this concept in their processes and innovations is leading. Companies that can successfully implement this concept will offer the customers/stakeholders more confidence/trust [59]. With the stakeholders' trust, it is possible to increase productivity and keep pace with innovations.

Trust within social aspects

We just covered the need for digital trust. As digital trust is mandatory for communications between stakeholders, we can state that information asymmetry grows without this digital trust. The likelihood of market failure also grows with an increased information asymmetry gap. We have seen that the level of trust is connected to the usage level and discussed the externalities that apply within the example.

In the following chapter, we will discuss the TAM. This model allows us the better understand why users use certain technologies or not. As the trust level is connected to the level of usage, this model can give us a better picture of how to improve the current situation regarding digital trust.

Suppose we took trust in a different context and apply it in social aspects. Every person has her/his aspects and social identity. This social identity is interesting, as this plays a huge role in individual decisions. These decisions reflect his/her preference or the way they look at new technology. This last aspect plays a significant role in the acceptance of innovations and technology. Applying the technology adaption model (TAM) shows how people accept new technologies and developments [60].

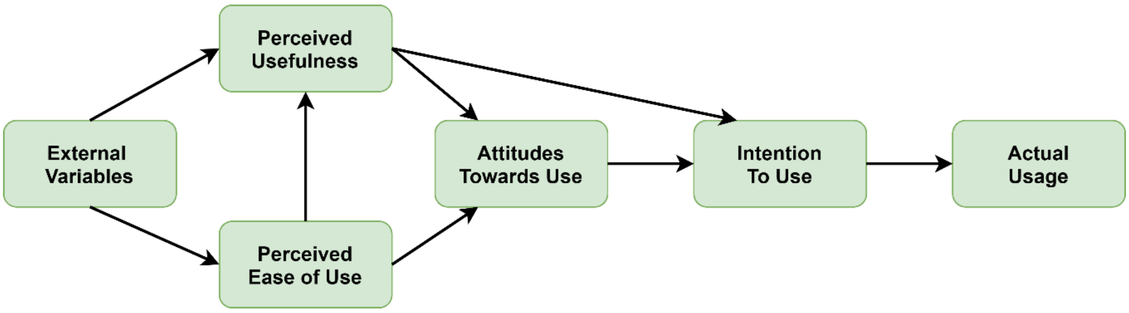


Figure 9 - Technology acceptance model (TAM)

[61]

The model above shows the significance of the perceived usefulness and the perceived ease of use. Both factors help a person to move to the next stage of the model. First, we see the perceived usefulness. It comes down to how much the use of technology adds to a person's life. If this is very low, the likelihood of a person using this new technology is very low. Once this is very high, the likelihood starts to rise. In order for the person's attitude to change, we also have to consider how easy it is to use the new technology. If this is very hard and the person has to invest much time, they will likely not use this new technology. It shows that a balance of both ease of use and usefulness is essential.

External factors play a significant role in the perception of people regarding the new technology. These factors can be virtually any information that regards this new technology. If a person hears a friend speak about a specific new product/service, he/she might get right or false information about this technology. He/she might see another person using a product/service and be very productive. As this outcome may be beneficial to the person him/herself, it could prove useful to use the product/service.

Furthermore, information that he/she might get on the internet may be biased or coming from advertisement networks. This perception of information could alter the person's decision regarding the use of the product/service. As the TAM model does not address intrinsic motivations, it is limited regarding emotional needs [61]. This limitation does not give us clear insight if the motivation and the use of a particular product or service are based on intrinsic needs. The shortcomings of the TAM model are described in the TAM2 model. This model is further developed, but with the current model's help, we can show relevance within TAM by implementing new and improved protocols.

In the end, the TAM model describes the adoption of a specific new technology. As adoption rates for a new technology start to rise, so does the trust with this new technology. Trust is connected to a new technology's use/adoption rate; adoption is essential for growing trust. It can be stated that the TAM model can stimulate the growth of digital trust by boosting the adoption rate [62]. As we stated in the previous chapter, the TAM model does not apply all intrinsic motivations to cover the whole spectrum of acceptance fully. We add the social identity theory to the model and get a better insight into applying the TAM model. This theory implies that human behavior can be biased based on the sociocultural groups they are a part of. In short, this comes down to the fact that humans behave differently when they are part of a group. This theory can also be applied to co-workers from company X. When company X produces a new product or service, the person working at this company likely feels the need to use/share it. The co-worker may not be in immediate need of this product/service, but it may reflect more significant adoption by other users. If the product/service is successful, this co-worker can refer to his/her group. He/she might refer to "people like me" or "my" when he/she talks about the product or service. This group of "me" is also a direct corollary of the trust within that group. A group of like-minded people gives a more profound sense of trust. Therefore, it can be stated that digital identities can give this feeling of a person/human with like-minded thoughts. A person is more committed to using a service/product once this trust is there [60].

Once a company can produce the level of trust where people can refer to it as "people like me" or "like-minded," it can help engage new users in using their products as this engages people on the level of trust. This can ensure growth in the adoption of new services or products. This also shows that trust from the userbase of services and products is essential in the role of adoption.

This adoption can be stimulated with the mentioned aggregation theory, as this theory uses a form of certainty to its users and its customers. [53] shows that by applying this theory, companies can offer an aggregated form of services to their users. This allows users to use a certain product or service quickly and attracts more users. The ease of use is very high, and more users will be attracted to use this service. Smaller companies might become a customer of the given service and get more certainty on selling products/services. Applied to a CA model, there is currently[15] no aggregator company that aggregates all services coming from CA's.

If an aggregator company should come into existence, one can discuss if it should be based on blockchain technology. This is to mitigate the centralization of the aggregator and the emphasis of philosophy on the end products of the aggregated CA's: "Digital Trust."

[15] As of writing this thesis.

Trusting identities

We just covered the TAM, which showed that people are willing to use a specific development and or technology based on the perceived ease of use and perceived usefulness. These two factors are essential during the introduction of new technology. It shows that solutions to improve the information asymmetry gap between the users and the CA should be based on two main starting points: “perceived usefulness” and “ perceived ease of use.” Once both of these metrics can be met with the introduction of new technology or service, users are more willing to adopt it. We covered the TAM model to understand better why people adopt certain technologies and why not. More models give a good view of how this adoption rate is developing, but that is out of scope for this research. The corollary of trust in using the product of services comes from the adoption. In order to trust a specific product or service, we want to use an identity linked to this product/service. The following chapter will cover why this identity is an essential element in this trust relationship between people or groups of people representing a company.

Adding to the level of trust, people or groups of people representing a company need to prove their digital identity. This identity is mandatory to build trust between two different parties. If a customer shops at a webshop, he/she wants to check this shop's identity. If this is not possible, it might be possible that a different actor is mimicking the shop and trying to steal information. As discussed in the previous chapter, trust is a mandatory element in the relationship between different actors. Checking the digital identity of a person/company is a bit different than the real-life version. One way to trust online identities is to use PKI.

As we do online shopping at our trusted webshop, we rarely verify the person or group behind this webshop. We trust that this webshop is valid and that we receive the goods we ordered in the end. As we have shown, a more significant userbase inherits a bigger adoption and use of a service or product. This significance is also the case for the use of a webshop. Based on a webshop's userbase, we read reviews and base our trust in these reviews [63]. Doubtful reviews and more numbers in these make us tend to believe that the webshop is trustworthy. However, we are already trying to trust a webshop reviewer; we are trying to check if they are trustworthy. What tells us this reviewer is even trustworthy, and does this reviewer have any incentive behind his/her review. These questions are hardly the answer as they all come down to these persons/groups of people's identity.

More and more transactions will happen online; therefore, a digital identity is necessary for these transactions. Not only webshop transactions or private transactions, but also official transactions between customer and company. These transactions have legal weight and therefore need a natural person to be bound. Online, we can be anyone that goes under the name of a different person. We can see the other party face-to-face during traditional transactions and see which whom we are dealing with. We cannot see this face-to-face during these online transactions, and therefore, the requirement of this digital identity requirement increased exponentially over the past 12 years [64]. Without this digital identity, it is hard to bound the transaction to a natural person.

Traditional identities of a natural person are bound to the identity documents. These documents consist of a birth certificate, passport, driver's license, and additional documents. During traditional official transactions between a company and a customer, the customer needs to prove the identity of him/herself with one of these documents. As this information is static and factual, it is hard for the person to alter this information without his/her government's consent. The information is verified and validated at the time of registration by his/her local government. By validating this natural person's information, the government acts as a trusted party by providing trust. This trust is originating from the proof of the validity of these legal documents.

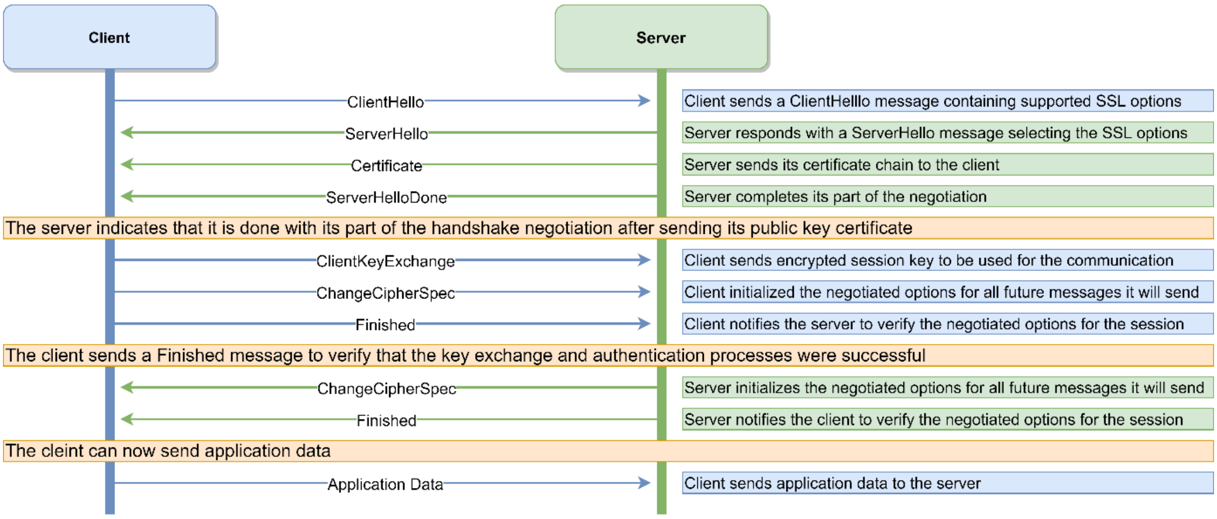
Not all information is needed for every business transaction between customer and company. Some transactions are more informal and smaller, and some are more significant and more formal. The information that is needed depends on the nature of the transaction between the two parties. During the transaction, there is a trade of personal bound information between two parties in order for this transaction to happen. The customer or the company can make up this trade of personal bound information in a digital sense. Therefore, the need for this static and factual personal bound information is mandatory for a transaction to happen in a legal sense. Furthermore, this information needs to be verified by a governing party that can provide trust as a traditional government can [64].

Companies offering different services have different levels of trade in personal information. Some companies offer financial services or other services that require the company to know the customer's personal information. When a customer from this company has committed a crime, fraud, or any other crimes, the company might be asked to deliver details regarding this customer. In [65], Microsoft offers customer data when there is a warrant for that data. It shows that customer details are crucial for criminal cases. These details are personal details that can be obtained from the Know Your Customer (KYC) implementation. This implementation askes the company's customers to trade their personal details to prevent money laundering, terrorism funding, or funding any other crimes. Therefore, some companies must offer a well-implemented KYC program. Without this program, the identity of these customers are not known. In such a case, customers can abuse the services the company offers [66]. The KYC implementation builds trust between the company and the customer and prevents the company from ending up in the wrong business. It serves as the company's first defense strategy, making it part of the risk strategy.

Furthermore, the KYC concept could work in multiple ways as we are talking about a person/customer's digital identity or a company/group of people. By reversing the KYC concept to "Know your company" (KYC)[16] , we can apply the same concept to knowing a particular company's details. As a customer, we can check the details of a company on the website itself. This company's identity is there, and they show us the location and sometimes that staff that works at this given company. However, in the end, the information has been put there by the company itself. For us, as a customer, it is tough to fact check this information. Fortunately, the PKI X.509 standard is there to offer public-key certificates. With these certificates, it is possible to set up a trusted connection between the customer and the company. Although this does not prove its identity, it does show domain validation at its lowest level. It shows that the company domain is connected to the correct domain holder. As this still does not prove its identity, we have to go to a higher certification level [9][67].

[16] Not an official abbreviation, used for illustration of statement

Before we start dissecting the different levels of validation within a CA, we take a quick look at the inner workings of how the certificate is used for communications.
We base our online communications on the certificate which are trusted by another third party company. Applications, mobile apps, websites, and more services use these certificates in order to secure the data that is transferred or received. To understand how this works and how software secures its data transfer, we added a schematic underneath. The figure below shows the steps that are needed to ensure a safe way of communication between a client and a server.



Client sends a ClientHelllo message containing supported SSL options

Server responds with a ServerHello message selecting the SSL options

Server sends its certificate chain to the client

Server completes its part of the negotiation

The server indicates that it is done with its part of the handshake negotiation after sending its public key certificate

Client sends encrypted session key to be used for the communication

Client initialized the negotiated options for all future messages it will send

Client notifies the server to verify the negotiated options for the session

The client sends a Finished message to verify that the key exchange and authentication processes were successful

Server initializes the negotiated options for all future messages it will send

Server notifies the client to verify the negotiated options for the session

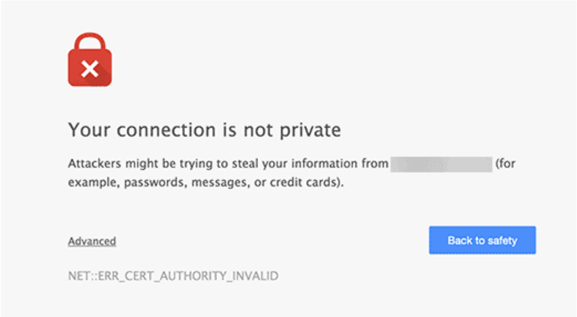
The cleint can now send application data

Client sends application data to the server

Figure 10 - SSL/TLS handshake
[68]

Once the server and client are done with this handshake, both know the chippers[17] and keys. These are used to encrypt the application data that is transferred. The only thing we miss in the schematic is the part where the client checks for the validity of the certificate connected to the public key of the server. This is done with the help of the process described in an earlier paragraph. During this check, the web browser/application will check if the server's certificate is trusted. If a certificate is untrusted, the browser shows a warning that a possible MITM (Man in the middle) could occur. The user can accept that risk if he/she knows the public key. If he/she does not know the trusted public key, it is not safe to connect to that server.

This error the browser shows does not imply that the connection is unsafe by default. It only shows that the public key is not trusted to any specific domain and that no CA has conducted the aforementioned checks and balances to see if this public key is trustworthy. In the figure below, we can see an example of such an error.



Your connection is not private

Attackers might be trying to steal your information from [redacted] (for example, passwords, messages, or credit cards).

NET::ERR_CERT_AUTHORITY_INVALID

Figure 11 - Certificate not validated by trusted CA
[69]

[17] Cryptographic algorithms allowing for encryption and decryption of data

There are four levels of validation within the X.509 PKI certificate protocol. The PKI uses this protocol in order to deliver its trust services to the users. These different levels of validation represent a different level of trust. In this case, the customer can use this level of trust in his/her own way of trusting the company. The four different levels are as follows: [18]

- **Domain Validation (DV)**: This validation level is the lowest and proves the validation at the domain level. It verifies the fact that the person that requests the certificate owns the domain and has full control. This trust level is deficient, as it only shows that a person owns a domain [70]. The information that is used within this level comes from the domain registrar. Unfortunately, it is possible to register yourself with fake information or with an anonymous whois[19] service. This last option is to register a domain without connecting any personal detail to the domain. Without this information, it is hard to identify a natural person behind a domain. Furthermore, it is hard to check the details when the domain is verified. The actual check conducted during the domain validation process depends on a text file and DNS records connected to the domain. During the process, the domain holder changes these parameters to the given parameters from the certificate authority. After changing these parameters successfully, it renders the domain validated.

  Trust level:[20] DNS based change/text record change, not connected to any personal details regarding a natural person. Low trust level.

- **Organization Validation (OV)**: This level of validation offers the validation of the organization. The company that offers the certificate validates the applicant against the business itself. It shows that the applicant for the certificate is connected to the company. This process takes a few more steps in order to verify the validity. The steps shown are an example of [71], where they describe the steps. The steps are as follows:

  - **Organizational authentication**: Here, the certificate authority checks if you are the legitimate owner of the company. Personal details are checked and looked up if connected to the company.
  - **Locality presence**: In this step, the certificate authority checks if you are registered at the given location. It checks your legal documents and see if it is connected to the location.
  - **Telephone verification**: During this step, the certificate authority is calling the registered company telephone number. It also checks if the number is listed.
  - **Domain verification**: This step is the same verification process described in the lower trust level. The certificate authority checks if the domain is in your possession. During the validation process, you have to take the same steps described above.
  - **Final verification**: During the final verification, the certificate authority calls the customer and checks all the certificate order details. He/she verifies every technical detail regarding the certificate order.

  This process is more complex and harder to comply with. All these steps make sure that the trust level is at a higher standard. By checking all these details, the certificate authority enabled a higher level of trust. This trust is linked to a natural person and a registered company.

[18] Going deep into the technical details does not add to this research, we only touch the technical surface and the impact for the trust levels regarding the identity

[19] Whois, is a service where other internet users are able to lookup information from the person holding that specific domain. This information is collected by the registar.

[20] Trust levels are based on the information behind the issued certificate and validation level.

Trust level: Based on a thorough validation process. Connected to a natural personal and business documents checked. Medium trust level.

- **Individual Validation (IV)**: This validation level offers the validation of the individual requesting the certificate. This level of validation verifies the person behind a domain/website. This validation level adds a higher standard of trust, as, during this validation, personal documents and information are checked. According to [20] [70], the certificate authority should check the following:

    - The certificate requires the applicant's name in combination with a legal photocopy of the applicant's face. This photo should match the photo present in a government-issued legal document (Driver's license, passport, military ID, or any equivalent document).
    - The certificate authority validates the applicant's address by using any given legal document. It can be done by any utility bill, government ID, credit card, or a legal document stating the applicant's address.
    - During this validation process, the applicant's domain is also checked according to the previously stated domain validation process.

    Individual validation for a certificate is a more thorough process when we look at the domain validation process. Individual validation looks at the natural person and his/her details. By verifying these details, the level of trust is higher than the domain validation trust level. Using these certificates, users of a domain can check the person behind the domain and have a higher trust level.

    Trust level: Based on an individual validation process linked to a natural person. Medium trust level.

- **Extended Validation (EV)**: This level of validation offers the highest level of trust and complies with the CA/Browsers forum's strict rules. To pass the validation for the level of certification, the applicant has to go through rigorous validation checks**.** Different checks are in place and described by the CA/Browsers forum. The checks are as follows:
    - The certificate applicant needs to verify its existence and identity
        - Legal existence
        - Physical existence
        - Operational existence
    - The certificate applicant needs to be in control/holder of the domain that needs to be included in the certificate.
    - The certificate applicant needs to communicate an entity that is named as the subject in the certificate.
    - The certificate applicant needs to be verified and authorized for the EV certificate.

    As all these validation processes are very rigorous and thorough, we will not detail them as they can be found at [19]. These documents show the validation steps and requirements before the EV certificate is issued to an applicant. It also shows that there are a lot of different details known about the applicant. By validating all these details, the certificate authority offers a high level of trust to their customers [19].

    Trust level: Based on an extended and rigorous process, validating all personal, legal, and business details. High level of trust.

Personal identification

As we discussed different levels of certification, we also have to look at the different rules and regulations that are present for the identification of natural persons. As local citizens' identification happens within different local systems, it is tough to identify a foreign citizen with their local identification method. In the Netherlands, we have DigiD and iDIN. With the help of these services, we can identify ourselves for different purposes. As we identify ourselves with local methods/documents, local businesses know the validity of those documents and verify them. Foreign businesses/governments or other interested parties cannot check the validity of the documents quickly. Therefore, the European commission comes with an implementation that helped all the stakeholders interested in using this service [72]. By using this system, the member states can build interoperability between the different systems and build a higher level of trust and security. All the electronic identification systems that are added are peer-reviewed. These peer reviews tend to stimulate a mutual learning process that improves the trust between member states. This shows that the implementation of the eIDAS is very new to members, and a lot can be learned. This also shows that mistakes can be made, and potential data leakage might occur during a faulty implementation of one of these systems.

As these implementations allow us to identify ourselves with others on the internet, we can build a trust relationship. As we discuss before, we have to know someone or a business's reputation within a trust relationship. As this reputation is connected to identity, it is of high importance that the other party cannot change/alter this identity. With the help of these systems, we are improving the identification of other users, thus strengthening the trust relation. Furthermore, we can check the trustworthiness based on the identification of that user/business. This allows us to bridge to information asymmetry gap between both parties.

Besides these systems, there is a protocol called Zero-knowledge proofs (ZKP), which allows the proofer to prove his/her identity without revealing his/her full identity. This is done by showing a statement/part of the secret, which enables the receiving party to check if that statement is true or not. This can all be done without revealing the proofer's sensitive information but allows the receiving party to check the information/identity is indeed correct. An implementation that is currently used within the blockchain of Zcash is called ZK-snarks (Zero-knowledge – Succinct Non-interactive ARguments of Knowledge). This ZKP solution is applied within the context of a blockchain and allows users to verify the other party's identity without knowing the secret[21] of that identity [73][74]. As the ZK-Snarks protocol still relies on the trusted setup provided by a trusted third party, ZK-Starks was developed. This protocol allowed for the same zero-knowledge proofing but without the need for the trusted third party setup. It allows for more scalable systems and is resistant to the quantum computer's high computational speeds [22] [75].

With the help of the ZKP and ZK-Starks, respectively, we can verify one another's identity without revealing the true identity. This allows the best of both world implementation, as we now have privacy and a decentralized trust system to bridge the information asymmetry gap present in the currently used PKI. Furthermore, information asymmetry functions of **signaling** and **screening** are conducted and are disconnected from the trusted third party. These functions can[23] be executed completely independently without the intervention of a third party or relying on one. This does not require closing the information asymmetry gap between both parties, as this technique allows for identification without the information that reveals the true identity of the other party.

[21] All the personal details that relate to that identity.

[22] A stronger cipher suite is implemented in the ZK-Starks protocol, which is quantum resistant.

[23] With the help of the ZK-Starks protocol

Trusting third party's

We just covered the different methods to verify the identity from a CA perspective. This information gives the CA information in order to check the validity of the given identity. As this information is mandatory to trust an actor, the CA's customers do not pose all of this information and create an information asymmetry between them. Furthermore, it is costly and inefficient for a user to check on all this information before trusting a party. This should be done by a trusted third party dedicated to conducting these checks (in this case, the CA). In order to establish a trust relationship between the customer and de CA, identities need to be connected to both entities. With the help of KYC, a CA can check the details of customers. Systems like DigiD and iDIN show local solutions to identify a user. As these systems only operate locally, it is hard for foreign companies to check foreign users' identities. The European Commission proposed a system called eIDAS that allows member states to check these foreign identities. These systems offer an identification service that allows companies to identify their customers. This again increases the information asymmetry gap between the users and the companies. We discussed a zero-knowledge protocol called ZK-Starks. In the following chapter, we will discuss the PKI system and different CA attributes. We will discuss how these PKI structures are built and how trust-flows down. We will discuss why there is a chicken and egg paradox present in our current digital trust system.

As we have discussed the different trust levels from PKI X.509 standard, we use this technology not based on the users' choice. During the implementation of these protocols, the growth and user base was a lot smaller than nowadays. It is a protocol that is developed in the early stages of the internet. It offered secure communications and offered a solution to protect people and businesses against digital espionage, e-commerce fraud, and intellectual property theft. Nowadays, we have newer and improved technical implementations that allow us to bridge this information asymmetry gap. In order for the development of the internet, looking at how we can use these protocols and technical implementation is mandatory. Currently, we are working with a patch method. Once something is unsafe and not working correctly, we patch it. Once patched, it will work for a given time until it not safe anymore. This cycle of patches can be found in DNS -> DNSSEC, SSL -> TLS 1.2 -> TLS 1.3, BGP -> S-BGP. These protocols keep getting updated once a vulnerability is found.

Without the PKI x509 protocol, data is transferred over the internet in an unsafe and open way, and everybody in between could impersonate the source of this data. The PKI x.509 standard uses SSL/TLS with its respective cipher[24] suites to encrypt this data. Without this encryption, Internet service providers or other infrastructure companies could look into the data being transferred over the physical lines. Users in the same network were able to look into the data being transferred. With the PKI x509 standard help, users can encrypt the data that rendered the data unreadable for the eavesdropping parties. Furthermore, the PKI implementation led the users to verify the identity of the sending and receiving party [76]. PKI has different security services with its characteristics summed up bellow:

- **Data integrity:** The transmitted data is not altered in any way. It may not be possible to alter the data between the sending and receiving parties. Data alterations need to be detected; the receiver needs to be able to verify the received data.
- **Confidentiality:** The data is restricted to access by parties that are not allowed to the data. Therefore, unauthorized access must be mitigated, and data disclosure can be ruled out in any event.
- **Identification and authentication:** Both the receiving and sending party can be uniquely identified in the transaction of data. Determining the origin and destination of the data needs to be possible.

[24] Cryptographic formulas to encipher the data into unreadable text

- **Non-repudiation:** The implementation needs to offer a way to validate the action of a sender of the data inextricably. The sender cannot deny the sent data [77].

These characteristics offer the backbone of the PKI services we know today. In order to make the PKI possible, we have to place components that facilitate this PKI. In order to make a PKI work, we need to following components [77]:

- **Certificate Authority (CA):** The primary building block to offer trust levels. Within the CA, checks and validations take place to sign certificates and offer trust. The CA is known for two different attributes: Name, and it's public key. These two identifiers give the PKI users the ability to check trust on issued/signed certificates. The certificate authority can issue different levels of certificates, which, in their way, are connected to a level of trust. As this trust comes from the CA, we use this authority for our direct line of trust on the internet. Later in this research, we will question why this is questionable.
- **Registration Authority (RA):** The registration authority is the entity that aggregates information regarding certificates. During this process, the RA verifies the information that resides within the certificates. The RA can request legal documents that are necessary for a certificate. Before issuing a certificate, a CA could delegate different validation tasks to an RA network. This network consists of different trusted third-party companies that fill in the different validation tasks.
- **Repository:** A repository is there to store active digital certificates for the CA system. With the repository, users are able to look up data that allow users to confirm the validity of the certificates. Certificates and CRLs are the main components of the repository. The repository can also be called Validation Authority (VA), as this is a service for the PKI users to validate issued certificates.
- **Archive:** The archive stores the data from a CA in long term storage. This way, the CA can check the certificates from old documents or files that were valid at a previous date/time. In the case of a dispute, it is possible to get back vital information that can be used to verify the key associated with a given certificate.
- **Public key certificate:** This is a public key that is issued by the CA and is connected to an identity. By using this public key, one can confirm the identity. As the CA is the party that holds the private key, an online user can verify a signed certificate with that public key issued.
- **Certificate revocation lists (CRLs):** Certificate revocation lists are a list of certificates that have been revoked and are deemed not to be seen as valid. By using the CRL as a user, he/she can check if a given/used certificate is valid seen from the CA that issued the certificate. The CRL also contains historical data about revocation states and certificates.
- **Online Certificate Status Protocol (OCSP):** The OCSP protocol is an alternative to the CRL and checks the revocation status with the CA's help. With this check, the user's browser can directly check the revocation status and not have to download the whole list of revoked certificates that reside within the CRL.
- **PKI User:** In order for the PKI systems to be working, we have to have users. These users use the certificates to check trust on a given website/service. Users can consist of a single person or an organization. Users do not issue certificates, although they can generate self-signed certificates. [25] This party is the relying party within the PKI system. The person/organization can hold certificates for signed documents or other applications.

[25] Self-signed certificates are only valid to the user itself or other users who accept the person/organization who signed that specific certificate.

Due to the nature of our current PKI implementation, the information asymmetry grows for all platform users. Users cannot check the source files and processes of the checks and balances that are conducted against a party interested in the certificate signature. Therefore, information asymmetry grows and renders a higher burden on the trust of the CA. It leaves the users in a vulnerable state, as the only option is to trust the disclosed documents from the given CA regarding these processes.

We can see the different actors/services that are present within the PKI. Without these actors/services, it was not possible to provide a PKI. One thing that is not clear about the different elements is how the whole infrastructure is setup. To understand the way trust flows down in a PKI, we have to understand the different frameworks that offer this trust.
First, the most basic hierarchical form of trust within a CA framework, trust flows from top to bottom. Trust/signed certificates are flowing down from the root CA to the subordinate CA's. The subordinate CA's will issue certificates/trust to its subordinate CA's or entities. This framework is scalable enough to implement in a small business or public service, but it has a central weak point. The root CA is, in this case, the single point of failure of delivering trust. This implementation of PKI is also present in our contemporary trust solution. As different companies offer trust in the PKI system, hierarchical parallel trust systems originate [53].

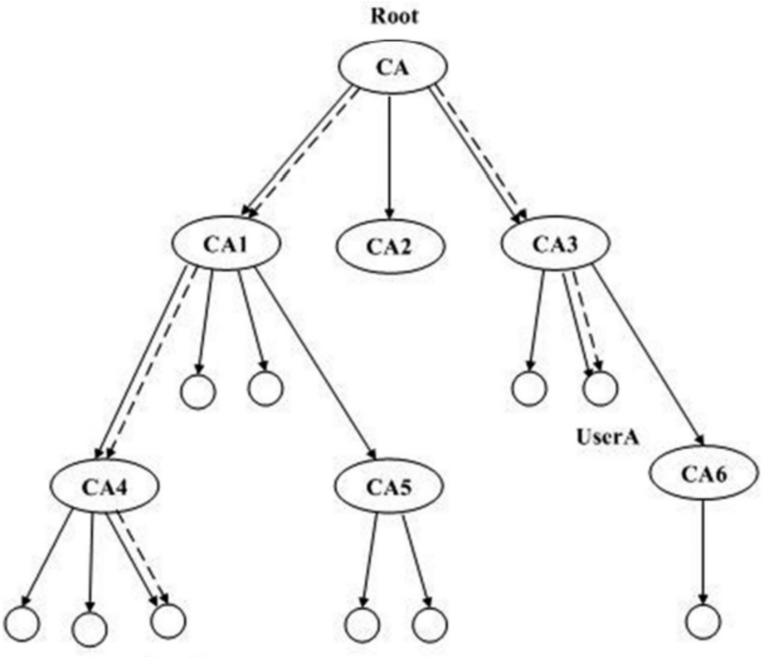


Figure 12 - Hierarchical PKI framework
[78]

In order to improve the scalability solution of the PKI systems, there is a range of different solutions present that offer different hierarchical, parallel hierarchical, mesh, and trust list architectures. These different solutions offer a more scalable PKI system, but they do not solve the main problem. This problem originates from the way the trust is flowing top-down in the system. In the figures below, we can see the different PKI solutions to address the scalability issues. Although some of these solutions might work correctly for the organization/person, new problems arise on the spectrum's manageability side. Once the tree of different CA's and subordinate CA's start to grow, It will start to be unmanageable. Especially when we start using these PKI concepts in the public space, the trust between the CA's is something that needs special attention [53].

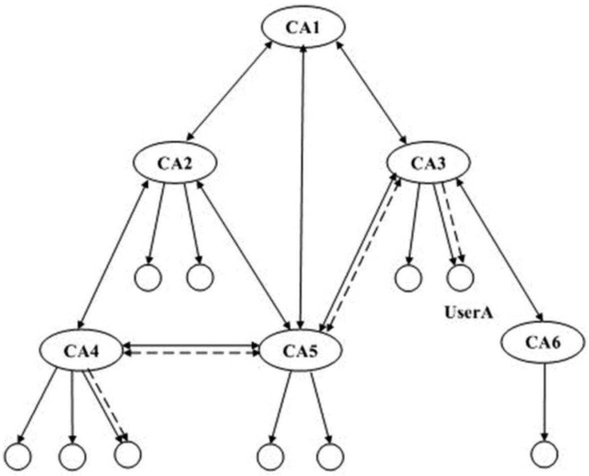


Figure 14 - Mesh PKI framework

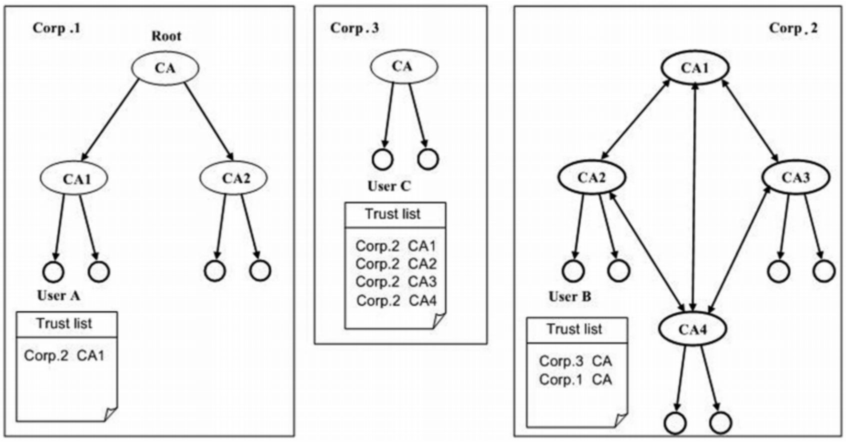


Figure 13 - Extended Trust list framework

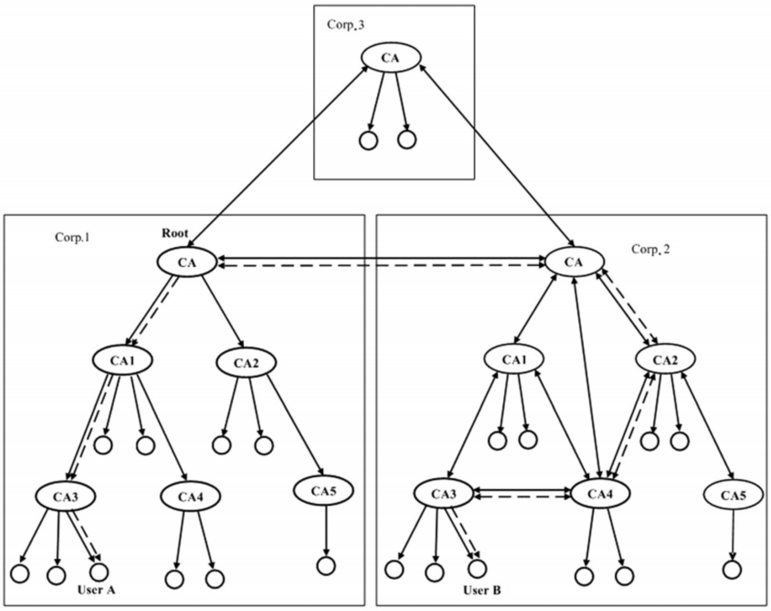


Figure 16 - Cross-Certified Enterprise PKI framework

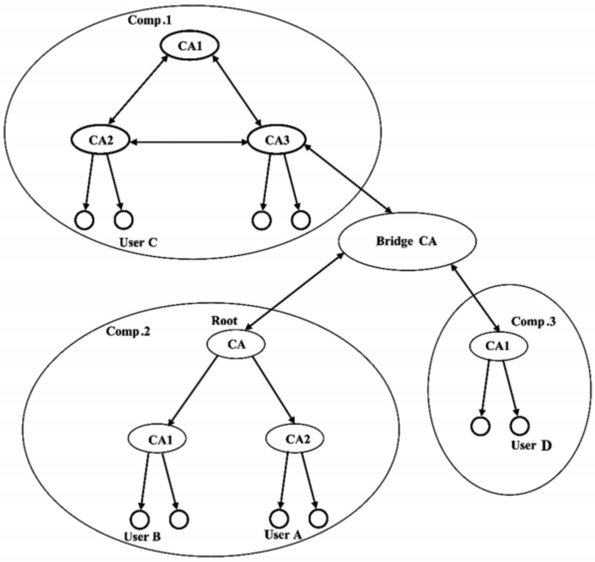


Figure 15 - The Bridge PKI framework

[78]

These different frameworks are used within organizations, businesses, educational institutions, or any other company. Selecting the correct PKI framework can be very hard, as they all have their advantages and disadvantages. [78] describes these advantages and disadvantages, which shows that it depends on the implementation and the requirements for the framework. Scalability, flexibility, trust point, and trust relationships, to name a few of these requirements.

The most crucial requirement that needs to be covered by all the PKI systems is trust. Trust has to come from a CA and show that an entity is trustworthy. The client/computer needs to know how to trust these certificates. To make the client/computer understand how to trust this certificate, software needs to know and be able to validate the certificate. There is a trusted root certificate store within every operating system we use today (Windows, Linux, macOS). These root certificates are essential for trust. A subordinate CA could have issued certificates that are used on the website. This subordinate CA inherits its trust from the root CA. Therefore the client/computer understands that the issued certificate originating from this subordinate CA is trustworthy [10].

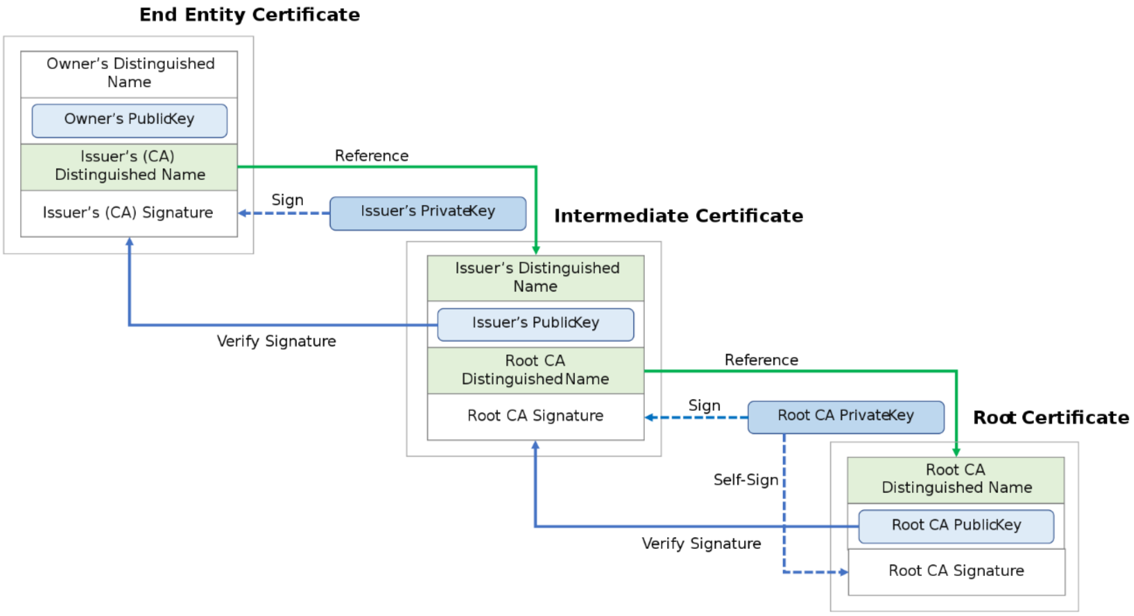


Figure 17 - Chain of trust
[79]

In the figure above, we can see how this process is working. The root CA has a public key used to verify the intermediate certificate (certificate subordinate CA). The public key is used to verify if the digital signature of the identity is valid. This digital identity can be any website/service that uses a certificate. This example clearly shows how the central trust is coming from the root CA.

Web browsers are pieces of software that allow the user/person/organization to browse the internet. They use the root certificate store on the operating system to check the certificate's chain of trust. Without this certificate root store, the browsers or any other service/application cannot check for trust. Because all these software uses the certificate root store, they assume that the root certificate authority is trustworthy. This can be seen as a severe flaw in the system. The root certificate authorities are the main trust backbone of the internet. As there is a hand full of these root certificate authorities, it is, in a sense, a centralized manner of trust. We, as users of these trust systems, have to rely on trust from a third party. Once a CA or a root CA goes rogue or get hacked, we cannot check when this is the case. The aforementioned implementation from the google team helped the PKI system check if certificates are valid. The implementation is called Certificate Transparency and uses a Merkle Three root to validate certificates and logs. With the help of this system, users can check if a certificate has been issued mistakenly or maliciously [80][81]. This can also be an indication of good or bad practice from a certificate authority. This indicates that the current implementation is not in its optimal state and is “patched”[26] with extra protocols.

[26] Temporarily fixed with a technical implementation.

According to [11], the root certificate list is made up of one hundred fifty-six individual records. All these records represent a root certificate authority who can validate and sign certificates for subordinate certificate authorities. Fortunately, the trust coming from the root CA's, which are backed by a rigorous validation process and policies they have to comply with [82]. Different software vendors have policies in place before a root CA is placed in the inclusion list. Microsoft[83], Mozilla[84], and Apple[85], to name a few software/hardware companies that have their strict policies regarding root store implementation. The fact that software/hardware vendors demand these policies' validation shows multiple checks before a root CA is allowed on the inclusion list. It also shows that these software/hardware vendors have the power to allow or disallow certain trust to their users.

It is especially true when we look at the implementation of android. Google is the company that owns and creates the software behind android. This gives them the power to decide if they add the specific root CA to the inclusion list of android. Furthermore, Google is also a root CA with his/her own subordinate CA's and customers. It could be debated that this might be conflicting in the choice of which root CA is or is not added to the inclusion list. We as users have the trust google about why some root CA's are added and why some are not. Vendors of different android phones can add or remove root CA's from this list. Samsung android users could have a different trusted list than Huawei android users. The implementation of this list depends on the company/brand we buy the phones from. The users can enable/disable or add/remove items from the list. This gives us the power to trust or not trust a specific third party root CA. This example is also applicable to the Windows operating system[86], the macOS operating system[87], and the Linux operating system[88]. This example also shows us we as users have to trust the implementation of different vendors. Different vendors choose different root ca lists. Because of this fact, it is good practice to check this list before using any service/application/website.

In order for us to trust the party that offers the root of trust, it comes down to the chicken and the egg problem. We are trying to validate a certificate; this certificate is coming from a root that we have never seen before. As we are trying to decide to trust this certificate, we look at the issuer itself. Unfortunately, this certificate is issued by the root CA itself, and we fall back to the previous step.

Egg:	Validating a certificate, checks ensue.
Chicken:	Validating the party that issued the certificate, the root CA itself.

Trust originates from this root CA, and it is tough to check the trustworthiness of a root by the average user. In order to make to process easier, certificate authorities are using requirement standards to conform themselves. These standards show that a certificate authority applies good practice in different processes within the company. The CA/Browser forum offers baselines requirement and guidelines for different levels of certification [89] [70] [90]. Furthermore, an organization like webtrust.org and European Telecommunications Standards Institute (ETSI.org) offers standards and guidelines for certificate authorities and other trust service providers. These standards offer guidance and scoping for public CA's. Government-owned CA's need to submit performance audits to the organization of ETSI in order to stay certified. This is also the case for CA that fall in the certification of WebTrust. Looking at a local CA KPN, they show clear insight into the business practices within their repository [91] [92]. CA KPN shows security controls, key life cycle controls, certificate life cycle control, and certifications. By showing these different documents and complying with a different standard, CA KPN shows transparency and implies trustworthiness.

But, the question still remains do we trust CA KPN after all this certification? Do we trust the organizations behind the audits and baselines? These questions are hard to answer, as they also come back to the chicken and the egg principle. As we discussed earlier, trust originates from two parties that are in a vulnerable state. The user of CA KPN's certificates is in a vulnerable state. Once CA KPN exploits this trust and loses its users' trust, the likelihood of other users not trusting CA KPN is high. CA KPN has a significant userbase that uses the certificates daily. Without this big userbase, the trust level may also shrink, as a more significant user base/popularity equals more trust in a system.[27]

A previous Dutch certificate authority who used to be in place of the where CA KPN is now was Diginotar. Diginotar played a big role for the Dutch government because they used many certificates that were issued by Diginotar. Unfortunately, the Diginotar CA was hacked by an Iranian hacker. Because of this hack, he/she could issue the *.google.com certificate, which is a wildcard certificate. Wildcard certificates can be used on any subdomain of the google.com domain. When the attack had been discovered, Chrome and Firefox's developers removed diginotar from the root store. This caused many problems with the legitimate Dutch websites that used diginotar certificates. Users were not able to connect to the websites and verify if the website was legitimate. In order to fix this problem, Google came up with a solution called certificate pinning. Within the web browser chrome, there is a mechanism that checks for a specific certificate on google.com. If there is a different signed certificate and not originating from the google CA, the chrome web browser deems that certificate unsafe. With the help of certificate pinning, Google can make sure that a specific certificate is used on a specific domain. The fact that any other registrar like Diginotar could issue a certificate is a big vulnerability. The current Dutch CA (KPN CA) can issue any given certificate and create a possibility to eavesdrop on users behind that specific domain. Thus, it is important to understand that the whole concept of trust on the internet is originating from CA's [93]. The combination with the older DNS protocols makes for a possibility where eavesdropping could occur.

In the Diginotar case, the company was used to eavesdrop on users in Iran. Using the trust from diginotar, an actor within Iran or any other actor with interests in the traffic from these users was able to eavesdrop on this connection. To render an overview of the situation, we added a bowtie model, which clearly shows the process and its different vulnerabilities, risk mitigation, risk treatments, and consequences.

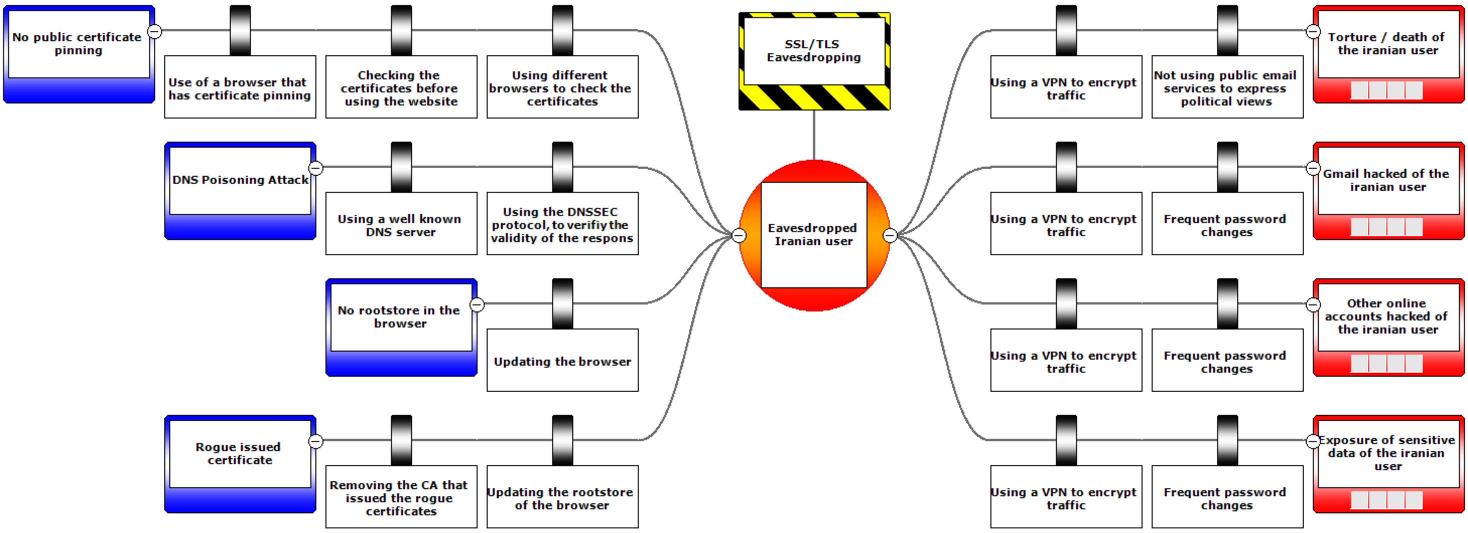

No public certificate pinning
Use of a browser that has certificate pinning
Checking the certificates before using the website
Using different browsers to check the certificates
DNS Poisoning Attack
Using a well known DNS server
Using the DNSSEC protocol, to verifiy the validity of the respons
No rootstore in the browser
Updating the browser
Rogue issued certificate
Removing the CA that issued the rogue certificates
Updating the rootstore of the browser
SSL/TLS Eavesdropping
Eavesdropped Iranian user
Using a VPN to encrypt traffic
Not using public email services to express political views
Torture / death of the iranian user
Using a VPN to encrypt traffic
Frequent password changes
Gmail hacked of the iranian user
Using a VPN to encrypt traffic
Frequent password changes
Other online accounts hacked of the iranian user
Using a VPN to encrypt traffic
Frequent password changes
Exposure of sensitive data of the iranian user

Figure 18 - Bowtie model of Diginotar attack

[27] Referring to figure 1 in the first chapter

In the eavesdropped Iranian user's case, we can say that the trust is mainly coming from The Diginotar CA. However, mitigations in the bowtie model can help the Iranian user build more trust in its communication. In order for the hacker to get access to the traffic from the Iranian users, he has to redirect the traffic to his own server. As there is no direct proof of how this happened, The best theory is that the hacker used a DNS spoofing attack to redirect the traffic to his own server. By using this attack in combination with a valid *.google.com certificate from diginotar, the hacker was able to show a legitimate-looking google website. If the Iranian user had used the DNSSEC protocol, this DNS spoofing attack would become very hard. As all DNS responses within the DNSSEC protocol use a digital signature that can be verified. By using the hash received from the authoritative DNS server, the client can check if this hash is the same as the connected trust anchor. The diginotar case would have been the top-level domain (TLD) .com[28] [94].

As DNSSEC uses a digital signature, it has to get its signature from the trust anchor. This trust anchor has to issue the certificate that is linked to that DNS response. In the case of an overlapping trust anchor for both the website and for the DNS response, the hacker could have spoofed both. In the case of a different trust anchor, the Iranian user spread its trust over two different trust parties. In this case, the DNS spoofing attack would have failed in all likelihood. By using this method, users can spread trust between different trust parties and have a more robust defense against these kinds of attacks. This also shows that a spread of trust (in this case, two trust parties) offers a more robust defense. It can be stated that trusting only one party with all the trust is a vulnerability in itself. Currently, it is possible to use a distributed way of trust. This trust form uses two different trust parties applied to the different protocols. By using one trusted party to trust a website, and the other trusted party to trust the DNS response, one can distribute the trust. In return, we can have a higher form of trust certainty.

Trusting a third party can be done collectively. By trusting multiple parties, you are less vulnerable when one party goes rogue or gets hacked. This being said, trust in itself is the chicken and the egg concept. As blockchain is a technology that has been in the media quite allot[29], the fact that it has been overhyped is undeniable. Although, the technology itself has some fascinating characteristics as it allows us to create a peer-to-peer trust-based system. With the help of this system, we can defy the rules that apply to that blockchain's specific usage. If we want to use blockchain technology in our trust systems, we need to defy strict rules that allow us to use this technical implementation as a trust anchor. Once this consensus has been met, we can all have one trust anchor and bridge the information asymmetry gap regarding digital trust. As there are multiple starting points on how this could be done[30], the hard part is to create a consensus that everybody will apply as a stakeholder of the current PKI digital trust system.

[28] Technical details about this protocol are excluded as we are only referring to the different trust path for this response.
[29] Bitcoin as digital payment method in particular
[30] The same way there are multiple digital payment systems

What is the purpose of decentralization?

We just covered the chicken and egg paradox that is present in our current digital trust system. The current digital trust system tries to deliver trust, but it has information asymmetry as a side effect. Due to the nature of the hierarchical PKI system, the centralization of this trust implacable. With these discussions, we demonstrated that the current digital trust system is inefficient in the form of information asymmetry and the form of centralization. We have also demonstrated the effects of legacy protocols like BGP and DNS. We demonstrated different externalities that allowed the use of these legacy protocols. It is debatable if these protocols are legacy as they are still used heavily today. Although, it is clear that the use of these protocols can have an impact on the digital trust of a user
To understand why we can use this decentralization to our advantage, we must understand its purpose relative to information asymmetry. There is an information asymmetry gap present within our current digital trust system between the users and the CA. To improve this situation, we will discuss decentralization applied to the use case of a CA.

Introduction

For users to use the internet securely, we have to use the PKI system. As this is critical infrastructure, it provides us the trust we need to communicate safely and securely. CA's offer us trust in a centralized way. This creates a single point of failure that can have adverse effects when things go wrong. The diginotar case [93] and the comodo case [5] are perfect examples of this centralized issue's importance and impact. We try to give a better insight into how to solve the centralized problem by discussing the purpose of decentralization.

Using decentralization

In the first chapter, we defined the main trust problem as a chicken and an egg concept. As this concept asks for what comes first: The chicken or the egg? Within the CA's world, this concept is clearly defined as coming from the CA that comes first.[31] Although, for the users, it is tough to have a clear answer to this question. From the CA perspective is pure business; for the users, it depends on the given application it is used for. There are methods/policies/checks to ratify the trust that comes from the root CA. However, these methods/policies/checks can be very complicated for the user to check him/herself. Therefore, we keep coming back to trusting a party that gives us this answer. This creates a new chicken and egg issue and renders an issue that is hard to solve. As we defined the concept of trust in the first chapter, the end-user has to put him/herself in a vulnerable position. The vulnerability lies in the fact that he/she has to trust the centralized company for delivering trust. Many users render themselves vulnerable nowadays as there is no other way to trust services online, as this centralized form of authority signs these services.

The current way root and intermediate CA’s sign their trust to a certificate, there is a 1 to many relation within that model. This model's effect can lead to an internet-wide failure of security, which happened in multiple cases [93] [5]. As this problem has occurred multiple times, the likelihood of this happening again is very high. With the internet's growth in mind, we want to prevent another catastrophic failure of this trust model. We also want to prevent market failure as a result of this.

[31] This statement can be ratified when we look at figure 10. We see the root CA using an self-singed certificate. This indicates itself as the point of origin of trust.

Decentralization concept

In order to improve the chicken and egg issue regarding the trust model, we take a look at decentralization techniques that offer possible solutions. In the next chapter, we will further discuss the different solutions. As these solutions might have different aims of issues, they give us more insight into the technique at hand. There are more decentralization techniques present; as these techniques do not apply to the cyber domain, we will discuss these techniques.

Let's first begin with the currently most known and maybe the most giant applied form of decentralization, bitcoin. In 2008 Satoshi Nakamoto introduced the world to a peer-to-peer electronic cash system. With this system, he tried to improve the so-called "inherent weaknesses of the trust-based model." Within his paper, it is not directly clear what he means by these inherent weaknesses. He tried to offer a solution to the current monetary system without relying on trust. As this statement is coming from his conclusion, it is very hard to understand how he meant these inherent weaknesses. For now, let's assume that we are on the same page and the trust weaknesses are similar to the same trust issues described in chapter one. In this case, he not only decentralized the concepts of monetary systems; he also removed the classic trust from the model. To re-introduce this trust, he uses a consensus technique that offers an algorithmic form of trust [95].

Besides the fact that bitcoin introduced a new form of algorithmic trust, it introduces a new way of looking at authority. [32] By looking at a non-centralized way of authority, the blockchain tries to solve a problem currently solved by different companies. These companies are active within the financial world, but in this example, we want to apply the concept to the "authority" within certificate authorities

These third-party companies have all the power to issue or not to issue specific certificates. It also gives them the power to trust or not to trust a particular company. This is very important, as this decision flows down to the end-user experience and how the end-users trust other users/services on the internet. The trust origin delivered to the end-users is very centralized and comes from a select group of companies. This select group of companies is not something the end-users have chosen but a combination of network externalities and market forces. With the help of decentralization, we could divide this form of authority into another entity linked to a different trust anchor. This new entity is not one or multiple companies, but a network of computers that represent it. Within this network, the computer executes different operations in order to deliver the trust anchor. The way this is done and how this anchor is delivered is called the consensus within that network.

Each consensus technique offers an algorithm that plays a significant role. With the help of an algorithm, google can offer relevant search results to its users. With algorithms, Facebook can show relevant social media posts to its users. Currently, we depend on these algorithms to show us relevant information we want to see. Without these algorithms, the platforms would show us irrelevant information, rendering the services less useful. While the algorithms of Google and Facebook do not work for a consensus techniques, they show an algorithm's relevance. Algorithms are enablers that give meaningfulness in the management of information and how its users perceive it. According to [96], algorithms would not only have to be embedded in software, which opens the hybrid implementations. People and processes can also be included in the workings of an algorithm. During the operation of these algorithms, people need to conduct specific actions themselves. This gives back authority during certain operations/actions. This also opens opportunities for certificate authorities to embed themselves within such an algorithm.

[32] Picking up where we left in the first chapter regarding autority on the internet.

[52] shows tension within the debate around the centralized or decentralized nature of bitcoin. Different participants from bitcointalk.org and from /r/bitcoin (Reddit) were interviewed. This interview's outcome was very interesting, as the views of these different users were completely spread all over. Some users deemed it necessary that human oversight was needed to make bitcoin function properly. Others were on the side that the algorithm should do all the work, and no human intervention should be needed at all. The outcomes of this research show that there are a lot of different starting points regarding the nature of the algorithm. [97] shows that the different decentralized cryptocurrencies have a centralized way of governance. Therefore it is hard to ratify the decentralized trust anchor for some users. The trust is coming from the consensus within that blockchain, but the development and, therefore, the control of that implemented consensus is coming from the people who develop that blockchain. The control of that blockchain is coming from the developers of that blockchain. It is hard for the normal users to control/steer the direction of that blockchain, as they do not have the power/knowledge to program for the blockchain. As for other interested parties that do have the power/knowledge, they can program and, in essence, steer the direction of the given blockchain.

Removing the human error in trust

Decentralization applied to the certificate authorities has a significant impact on the current operations of a CA's. CA’s have many different processes to account for, maintain, and audit in order for them to offer the levels of trust. These processes do not always favor the CA and show that these processes are vulnerable to human error [5] [93]. By removing human error from the deliverance of digital trust, we can improve digital trust's current situation. By implementing an algorithmic form of trust, we remove the human factor from the equation. In such a case, we can use a decentralized certificate[33] platform where the users trust the system itself. Users would put less effort into validating the other party's trustworthiness and legitimacy because they both trust the decentralized system[34] [8]. Although, there are services within the CA that still need human intervention (eg. Audits, setup of infrastructure, technical maintenance) to be executed. Without this intervention, mandatory systems are not added and or maintained to deliver digital trust. Without this intervention, corrections are not being made, and audits are not being conducted.
Due to blockchain characteristics and its respective consensus algorithms, some services can be automated and or do not require human intervention. With the help of smart contracts [98] it is possible to automate these services.

[33] Certificate in broad identification sense, to identify and accept that as a trusted entity

[34] Using an agreed upon consensus

What methods of decentralization are possible?

We have just discussed the different forms of consensus and how they improve digital trust's integrity and availability. These consensus techniques have different ways of rendering a network of digital trust. Once a network grows, and the nodes in that network grow, the digital trust's strength also grows with it. This shows that decentralization in a blockchain network grows hand in hand with its delivered integrity and availability. We have just discussed the purpose of decentralization and how it can help to improve the information asymmetry gap between users and the CA. We also demonstrated that even though the concept of digital trust can be decentralized, it still needs human intervention to keep systems running. It also demonstrates that the core trust is now coming from the developer of that given blockchain consensus protocol. This can be a downside as not all stakeholders can develop and have hearsay in this development actively.

In the following chapter, we will discuss different methods of decentralization. Within this discussion, we will look at various consensus methods, as they are the core building blocks of a blockchain.

A decentralized approach can be compared to the high availability approach we see in computer networks. These networks are built in a way that there is not a single point of failure. This can be achieved on multiple different levels, hardware/software/processes. Within this network, a service must keep running in order to provide certainty of operation. Without redundant systems in place, the highly available service and its connected uptime can not be guaranteed. This “certainty” can be sold to the customer in an SLA when discussed in the first chapter. By selling this certainty, the customer of that given service/product is confident they can operate and build upon that platform without worrying about failure or downtime. When we look at the CA, it has systems that are mandatory to stay online. Customers of the CA need to be able to check the validity of certificates. Without these systems, the CA can not offer the validation of certificates and thus cannot offer digital trust. Therefore, we can state that the CA’s needs to put redundant systems in place in order to guarantee this digital trust. In the case of downtime of these systems, users are not able to verify a certificate. The ability to build a digital trust relation between two actors is hindered without these checks [99].

We can state that the availability of the services of a CA is mandatory for digital trust. We can also state that these services' integrity is essential, as we don’t want any actors to corrupt digital trust. However, can we state that the confidentiality of the information within the CA should be available and shared with anyone? This is debatable and could offer a lower form of information asymmetry between the user and the CA, but could show sensitive information about a certain actor. As this sensitive information is linked to a person or company[35], it can be made anonymous by proofing identity with *Zero-knowledge proofs.* By using this method of proofing, one can identify itself without revealing any private/sensitive information. In essence, this allows for the confidential side of the CIA triangle to be satisfied. Making this private information irrelevant for a trust relationship between actors significantly improves information asymmetry. This information is mandatory to generate the digital trust we know and use today.

We set up the following requirements for the decentralization of digital trust (CIA) :

- **High availability**
- **High integrity**
- **High Confidentiality**

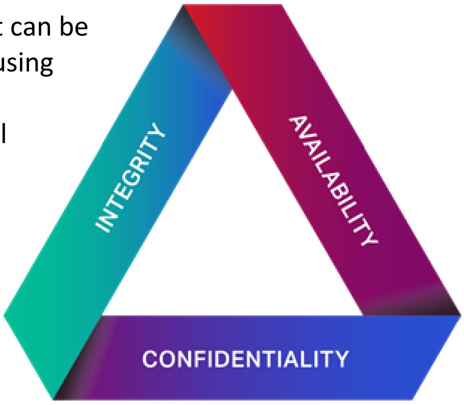


Figure 19 - CIA Triangle

[100]

Traditionally the CIA triad is used within networks/datacentre services, and concessions had to be made if one of the pillars was high. With the help of a decentralized network and smart protocols like ZKP, it is possible to satisfy all three pillars to a higher level.

[35] GDPR related

As the main starting point within this thesis is focused on digital trust, we will now focus on different decentralization methods and their respective consensus methods. Our primary focus is to strengthen the trust position of stakeholders of the current PKI solution. To understand the overlap of a proposed blockchain-based trust system and our current PKI solution, we have to dissect the different PKI components and overlap them with new blockchain-based improvements. In the figure below, we can see the different layers that are present within the blockchain implementation. This model shows a generic layer model of a blockchain and its different elements. Within the model, we can see that there are different implementations in different layers. This model has its similarities compared to the OSI (Open Systems Interconnection) model. The OSI model is used within networks to dissects the different network layers.

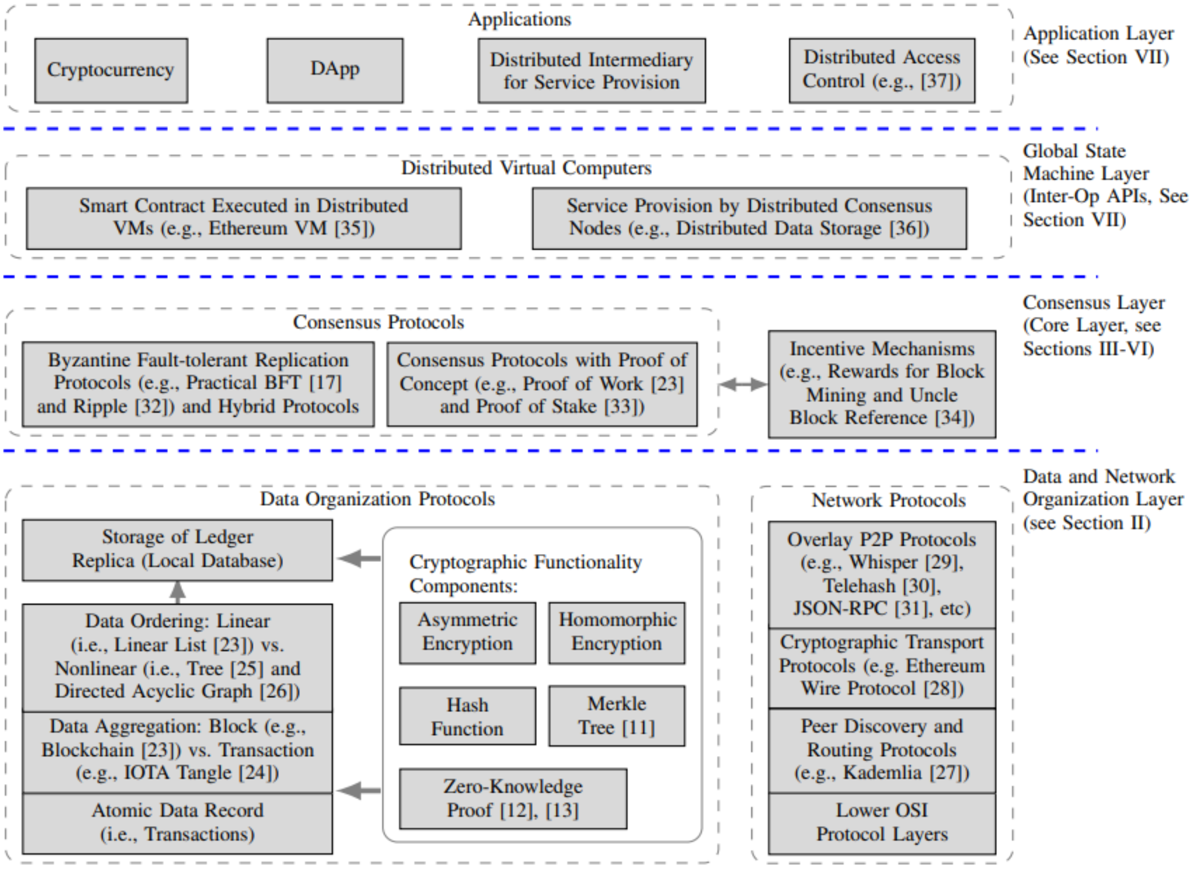

Applications
Cryptocurrency
DApp
Distributed Intermediary for Service Provision
Distributed Access Control (e.g., [37])
Application Layer (See Section VII)
Distributed Virtual Computers
Smart Contract Executed in Distributed VMs (e.g., Ethereum VM [35])
Service Provision by Distributed Consensus Nodes (e.g., Distributed Data Storage [36])
Global State Machine Layer (Inter-Op APIs, See Section VII)
Consensus Protocols
Byzantine Fault-tolerant Replication Protocols (e.g., Practical BFT [17] and Ripple [32]) and Hybrid Protocols
Consensus Protocols with Proof of Concept (e.g., Proof of Work [23] and Proof of Stake [33])
Incentive Mechanisms (e.g., Rewards for Block Mining and Uncle Block Reference [34])
Consensus Layer (Core Layer, see Sections III-VI)
Data Organization Protocols
Storage of Ledger Replica (Local Database)
Data Ordering: Linear (i.e., Linear List [23]) vs. Nonlinear (i.e., Tree [25] and Directed Acyclic Graph [26])
Data Aggregation: Block (e.g., Blockchain [23]) vs. Transaction (e.g., IOTA Tangle [24])
Atomic Data Record (i.e., Transactions)
Cryptographic Functionality Components:
Asymmetric Encryption
Homomorphic Encryption
Hash Function
Merkle Tree [11]
Zero-Knowledge Proof [12], [13]
Network Protocols
Overlay P2P Protocols (e.g., Whisper [29], Telehash [30], JSON-RPC [31], etc)
Cryptographic Transport Protocols (e.g. Ethereum Wire Protocol [28])
Peer Discovery and Routing Protocols (e.g., Kademlia [27])
Lower OSI Protocol Layers
Data and Network Organization Layer (see Section II)

Figure 20 - Blockchain network implementation[36]
[101]

To understand the different "network" layers of a blockchain and how decentralization is accomplished, we will have a look at the consensus protocols present in the model. These protocols are the core of the decentralized network and let it function in a certain way. With the help of these consensus protocols, a consensus is created within that given network. Each blockchain has it's own philosophy and application on how it should be implemented and how it can be used. In order to realize a decentralized digital trust system, one should look into these consensus protocols and how they relate to trust in itself. As every consensus technique has its own starting point of creating consensus, users using this network trust this network as this shares their view of how consensus should be working and implemented.

[36] There are some references in the figure that do not apply to this document.

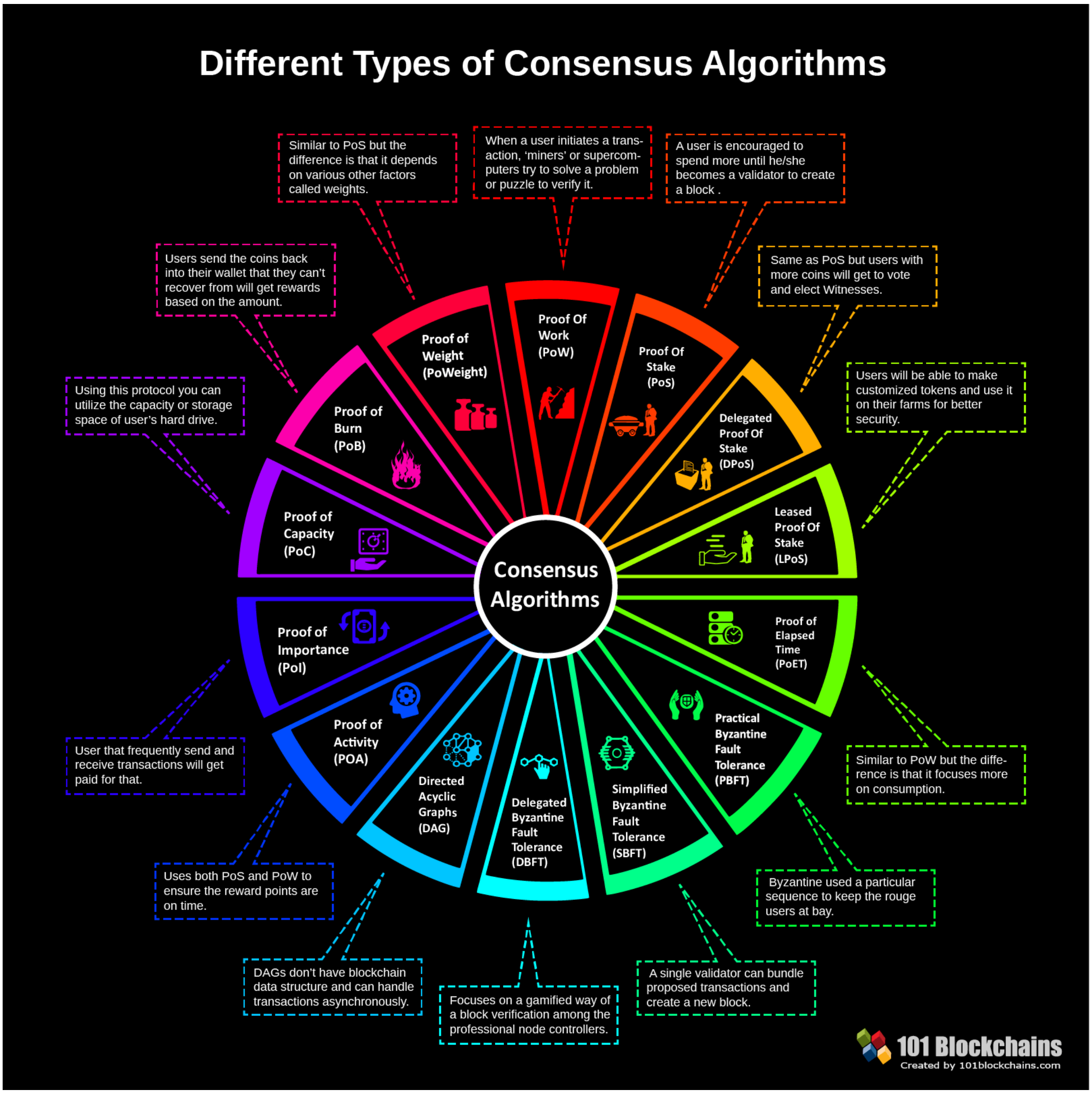
Consensus of algorithmic trust

We just discussed the basics of decentralization techniques applied to digital trust. These methods improve the current centralized character of our digital trust system. By introducing a decentralized character on digital trust, the system can excel in the CIA triad on all sides of the spectrum. We covered this to give a better insight into why it is essential to improve digital trust's current centralized character. It also demonstrates that this technique goes hand in hand with an improved form of integrity/availability. This integrity and availability are strengthened by the consensus coming from the network. Based on which consensus technique is applied, the size of the network allows for more robust overall integrity. ZKP allows verifying identity without revealing sensitive/private information and improving the currently known/used digital trust where the identity is needed in order for it to operate. In the following chapter, we will discuss a few different consensus techniques and why they allow for these improvements.

For each blockchain, there is an algorithm that is the core of that given blockchain. This algorithm described the rules that apply within that blockchain and how it operates. It described how transactions are conducted and how the network operates in order to approve these transactions[37]. All these rules are put into the consensus algorithm and allow a specific blockchain to behave in a certain way. The following few examples will discuss a few of these consensus protocols and how they are implemented in order to generate a network-wide consensus. As each consensus has a different starting point on how to reach consensus, not everybody is using the same consensus algorithms due to its underlying philosophy.
Reaching a consensus with a group of people is the same as the previous user reviews that require trust to work. With the help of a consensus algorithm, trust can be generated from the network that is produced from that specific consensus [102].

[37] Transaction are referred here in an non economical way. Network transactions

In the figure below, we see a collection of different consensus algorithms with their respective underlying philosophy.



Different Types of Consensus Algorithms

When a user initiates a transaction, 'miners' or supercomputers try to solve a problem or puzzle to verify it.

A user is encouraged to spend more until he/she becomes a validator to create a block .

Same as PoS but users with more coins will get to vote and elect Witnesses.

Users will be able to make customized tokens and use it on their farms for better security.

Similar to PoW but the difference is that it focuses more on consumption.

Byzantine used a particular sequence to keep the rouge users at bay.

A single validator can bundle proposed transactions and create a new block.

Focuses on a gamified way of a block verification among the professional node controllers.

DAGs don't have blockchain data structure and can handle transactions asynchronously.

Uses both PoS and PoW to ensure the reward points are on time.

User that frequently send and receive transactions will get paid for that.

Using this protocol you can utilize the capacity or storage space of user's hard drive.

Users send the coins back into their wallet that they can't recover from will get rewards based on the amount.

Similar to PoS but the difference is that it depends on various other factors called weights.

101 Blockchains
Created by 101blockchains.com

Consensus Algorithms
Proof Of Work (PoW)
Proof Of Stake (PoS)
Delegated Proof Of Stake (DPoS)
Leased Proof Of Stake (LPoS)
Proof of Elapsed Time (PoET)
Practical Byzantine Fault Tolerance (PBFT)
Simplified Byzantine Fault Tolerance (SBFT)
Delegated Byzantine Fault Tolerance (DBFT)
Directed Acyclic Graphs (DAG)
Proof of Activity (POA)
Proof of Importance (PoI)
Proof of Capacity (PoC)
Proof of Burn (PoB)
Proof of Weight (PoWeight)

Figure 21 - Most used consensus algorithms

[103]

Proof of Work (PoW):

With the proof of work consensus algorithm, computers have to conduct a certain amount of work in order to prove that a computational effort has been conducted. This proof is verified by the verifiers and is computationally more manageable than the work the prover has to conduct. This simple consensus concept is based upon the market's function, where the production of a certain product is more expensive than its consumption [104]. Although this concept works with simple market offering and consumption, the fact that it requires a lot of computational power is also its downside. The power consumption of this consensus algorithm is very high and requires to allot of resources from the party offering the production side within the consensus technique. The process of production is called mining and requires to allot of energy. When you want to participate in a proof of work blockchain and your energy price is high, you benefit much less from the reward compared to someone with a lower energy price. This downside concentrated the production of PoW blockchain transactions to places where the energy price is lower. Furthermore, the fact that it requires a allot of power does not positively add to the earth’s climate's desired development.

Proof of work is the consensus algorithm that is used within the blockchains of Bitcoin, Ethereum, Bitcoin Cash, Litecoin, Monero, and more.

Proof of Stake (PoS):

With the proof of stake protocol, the consensus is made within a staking network of nodes. This means that in order to participate in this network, one has to stake a certain amount. The higher this amount, the higher the chances are that this node is selected for forging the next block. The forging process is a process where that selected node handles blocks of transactions. The proof of stake protocol is entirely different when compared to the proof of work protocol. New tokens/coins are not “mined” during this process; instead, they are forged by the nodes that are selected in the staking process. Due to the non-necessity of releasing new coins as rewards[38], the given token/coin price is likely to stay more stable as no new coins are being created. This consensus method puts the actors in a vulnerable position as they have to stake their own money in order to get something in return. Therefore, the staked amount of money can be seen as some sort of collateral that strengthens the trust within that consensus [74]. In short, this consensus technique allows everybody that is staking (putting their own money at line) to participate in a random selection, to verify the transactions within that network of nodes. This method can be applied to the concept of CA’s, as blockchain that use this concept offers smart contracts. When we are talking about the processes within the CA, these processes can be written in these smart contracts and used as a service that resides on the blockchain. In this case, it is backed with algorithmic trust from the PoS consensus algorithm.

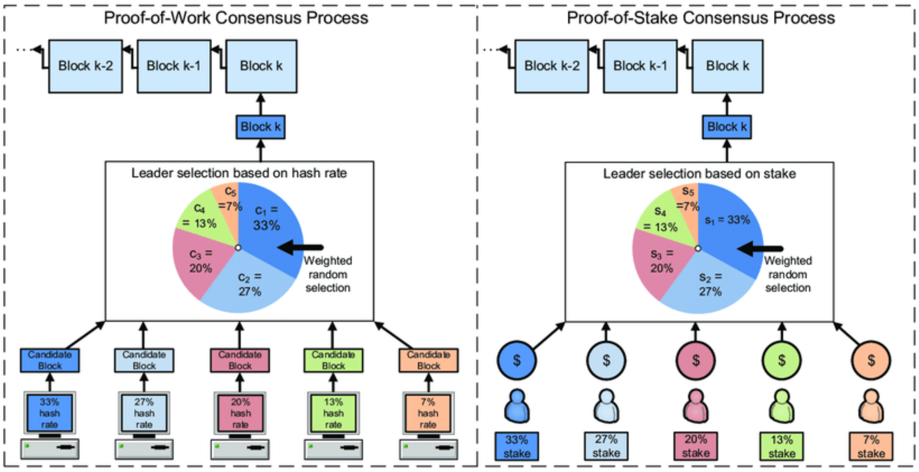


Figure 22 - PoW & PoS consensus algorithms

Proof of stake is the consensus algorithm that is used within the blockchains of Ethereum2, Cardano, Neo, Stellar, Dash, and more [74].

There are many different consensus

[38] Mandatory as reward in a PoW consensus.

protocols out there that try to solve the same issue differently, offering trust with the consensus's help. To understand the part where the algorithm gains authority, we have to understand the working of that algorithm and how it generates trust. As we have mentioned before, trust is built upon the fact that one party has to put him/herself in a vulnerable position and trust the other party to act according to expectation.

Trust – "*Psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behaviour of another*" – Rousseau et al. [56].

This also applies to the concept of trust when we are talking about trusting a consensus algorithm. As this consensus algorithm offers us the trust we want, we have to trust the consensus algorithm to act accordingly. During the beginning of this trust relationship, we have to put ourselves in this vulnerable position in order to build this trust. The trust relationship that we have to build has to come from the expected outcome, but in most software cases, this outcome is not visible in the real world. The input we give has expected outcomes that are not directly visible and render us blind to the invisible outputs. "Technological unconscious," Users trust in software because of the level of predictability, but at the same time are vulnerable to these invisible effects [52]. The more we are able to predict certain outcomes, the more trust we have in that given algorithm.

In the figure below, we can see the cycle of confidence from [105], where they describe a blockchain as a confidence machine.

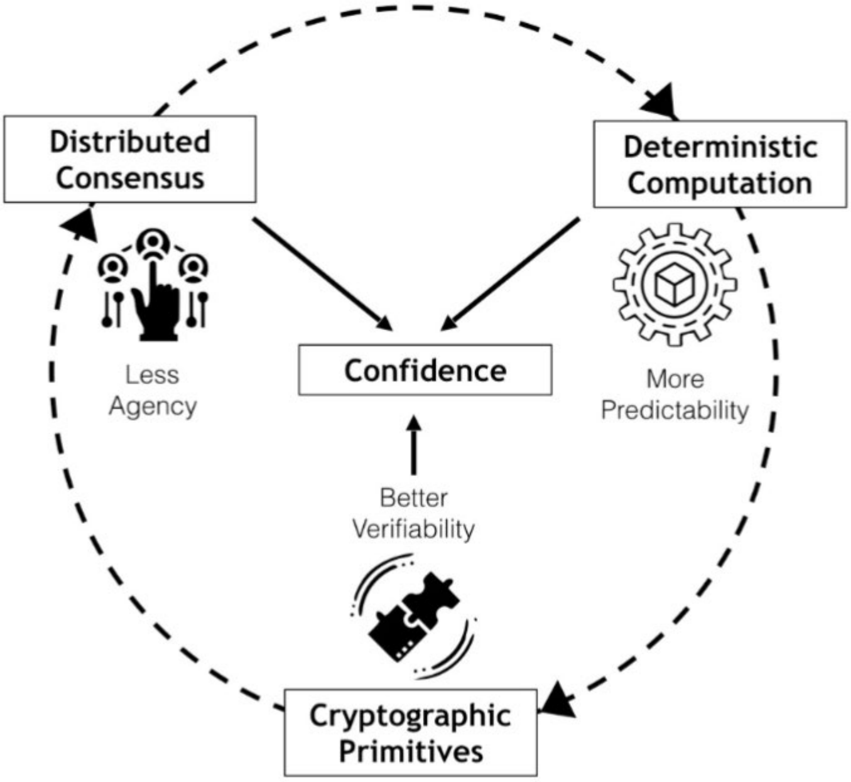


Figure 23 - Confidence blockchain cycle
[105]

Is it possible to improve the status quo?

Findings & Contributions

Information asymmetry is a crucial factor in relation to digital trust. We are using service/hardware/software, which contains technical implementations with much complexity. In order for the users to close this information asymmetry gap, he/she has to read up on everything he/she is using. This process is very costly and inefficient for users. They rely on the expertise of a professional/company to conduct this costly procures for them. The user puts him-/herself in a vulnerable position and trust this professional/company, with the expectation that the service/hardware/software works as expected. During this trust process, the user screens the professional/company and checks if it is trustworthy due to this process's lowered cost. The company/professional screens information to its users in order for them to sell a service/hardware/software product.
We demonstrated this same theory applies to the CA and it's services. As users of a CA need to screen it for digital trust, the information found is asymmetrical. The CA trusts a specific party due to its conducted checks and balances. We also demonstrated that the information originating from a CA could be corrupted information in the case of a hack. Diginotar and Comodo CA's are an example of a case where events went wrong. CA's put in place to create more transparency with protocols (e.g., CT, AKI) and allow users to check on misbehaving CA's. These protocols add to CA's behavior's overall transparency but do not improve the information asymmetry gap.

We demonstrated that the adoption of technologies goes hand in hand with the perceived ease of use and perceived usefulness. In the event of a change within the current PKI structure we know and use today, it is useful to focus on these elements. This helps in the adoption of new technology implementations. We demonstrated that there are externalities present in our current digital trust. These externalities show themselves in the form of software/hardware/protocol implementations. Without the changes in our current PKI system, these externalities can have an increased effect on the information asymmetry between the users and the CA. In the case where this information asymmetry gap is not improved, the likelihood of market failure increases.

Piloting projects offer additions and or complete new implementations of our current PKI trust system. Protocols that have been developed in the early days of the internet, the primary use case was different. This different use case had an externality that resulted in the usage of current protocols. These protocols are not optimized for bigger audiences (e.g., DNS, BGP). This same eternality is present in the use case of our current PKI. Multiple different companies offer the same form of trust with market-driven incentives.

This shows that the problem of information asymmetry linked to our digital trust is currently not in its optimal state. In order to further improve the digital trust system, we find that there are benefits connected to further research on this topic. This will require cooperation between different actors that benefit the use of the internet. Actors directly connected to the IETF can impact this by initiating an RFC that will improve the current situation of the PKI. At the same time, other actors that benefit can offer their technical expertise and offer improvement in the form of an open-source project like CeCoin, CertCoin, Handshake, and other similar projects.

The usage of blockchain to offer trust on the internet is not implemented from one day to another. This implementation will take time, as it is the same for building a traditional trust relation. With the help of this blockchain implementation, it can improve the information asymmetry currently present in our PKI x.509 system. If it is possible to close the information asymmetry gap within our PKI system, trade, communication, sharing, and other activities will have higher efficiency. This efficiency comes from a lowered level of uncertainty. A lower level of uncertainty renders a lower likelihood of market failure.

Adoption of new technological implementations are done once a higher level of adoption has been reached. Implementation of protocols that do not directly add to the implementing actor is likely to be postponed. Protocols like S-BGP and DNSSEC are a perfect example of improving security once multiple actors start implementing the protocol but do not directly add to the actor itself. This also applies to the users of technical implementations. Once the technology shows usefulness and the user perceives ease of use, adoption will likely start to climb. This theory is supported by the TAM model we discuss in the first chapter.

Conclusions

We started this thesis with the research question: “How to improve information asymmetries by developing decentralization of digital trust via certificate authorities?”. By dissecting the main research question into the sub-questions: “Why do we need digital trust?”, “What is the purpose of decentralization?”, “What methods of decentralization are possible?” and “Is it possible to improve the status quo?” we try to answer the main question. After analyzing different economic theories and applying them to digital trust, it became evident that we currently have a concern. This concern resides in the PKI ecosystem we currently use for all of our digital trust. We are confident that with the help of blockchain technology, the information security gap could be improved. It is demonstrated with historic failures on the market, it is demonstrated with externalities, it is demonstrated with the centralized character of the certificate authority. These concerns show that the current state of digital trust is not optimal. In order to improve the current situation, we propose that more research needs to be conducted with our future work in mind. With these points, new research can be started and give more insight into how we can improve the current situation.

When we talk about information asymmetry, we can conclude that this current digital trust state is the same as the lemons' car market. With the help of these recent technological developments, we can demonstrate that information asymmetry can be improved. By adopting decentralization and applying protocols like ZKP, we can disconnect the digital trust's actual private data. Without this private data and the immutability, it allows for a new form of algorithmic trust. With this algorithmic trust, we can mitigate historical issues linked to current technical implementations. By strengthening the PKI system's stakeholders to trust on an algorithmic trust, we give them back the following key needs: possibility to assess information quality, possibility to assess the history of information, possibility to assess the quality of information source. By giving back these key needs, market failure based on information asymmetry is lowered significantly.

Future work

- To get a better view of how blockchain and the different consensus techniques can be applied to our current trust system, comparative research needs to be conducted. This research will give us an overview of which consensus techniques work best for implementing a decentralized form of trust.

- Research on the adoption of an algorithmic-based trust model needs to be conducted. This research will indicate if it is possible to implement a new form of trust model based on algorithms.

- Research needs to be conducted on risks that are connected to a decentralized form of trust. As this thesis highlights the information asymmetry aspects, risks connected to a decentralized character of trust are not highlighted.

- Research needs to be conducted on how decentralization can be used in other disciplines where information asymmetry poses a risk. Other disciplines might also benefit the decentralized character trust.

- Quantitative research needs to be conducted to get a better view of how current CA’s allow for the implementation of decentralized algorithms.

References

[1] M. Lelarge and J. Bolot, *Network Externalities and the Deployment of Security Features and Protocols in the Internet*. .

[2] J. M. Bauer and M. J. G. Van Eeten, “Cybersecurity: Stakeholder incentives, externalities, and policy options,” doi: 10.1016/j.telpol.2009.09.001.

[3] J. Clark and P. C. Van Oorschot, “SoK: SSL and HTTPS: Revisiting past challenges and evaluating certificate trust model enhancements,” 2012, doi: 10.1109/SP.2013.41.

[4] C. Diginotar and O. Palmestraat, “Classification PUBLIC Interim Report Fox-IT BV,” 2011. Accessed: Oct. 06, 2020. [Online]. Available: www.fox-it.com.

[5] “Comodo Report of Incident - Comodo detected and thwarted an intrusion on 26-MAR-2011.” https://www.comodo.com/Comodo-Fraud-Incident-2011-03-23.html (accessed Nov. 03, 2020).

[6] D. W. Chadwick and A. Basden, “Evaluating trust in a public key certification authority,” *Computers and Security*, vol. 20, no. 7. Elsevier Ltd, pp. 592–611, Oct. 31, 2001, doi: 10.1016/S0167-4048(01)00710-6.

[7] A. Jøsang, *Theory and Practice of Cryptography Solutions for Secure Information Systems (CRYPSIS)*, vol. 13. IGI Global, 2013.

[8] D. D. H. Shin, “Blockchain: The emerging technology of digital trust,” *Telematics and Informatics*, vol. 45. Elsevier Ltd, p. 101278, Dec. 01, 2019, doi: 10.1016/j.tele.2019.101278.

[9] R. Housley, W. Ford, and W. Polk, “RFC 2459 Internet X.509 Public Key Infrastructure Certificate and CRL Profile,” pp. 1–129, 1999, Accessed: Oct. 26, 2020. [Online]. Available: https://tools.ietf.org/html/rfc2459.

[10] R. Hunt, “Technological infrastructure for PKI and digital certification,” *Comput. Commun.*, vol. 24, no. 14, pp. 1460–1471, Sep. 2001, doi: 10.1016/S0140-3664(01)00293-6.

[11] “Trusted Root Certificate Authority List.” https://www.checktls.com/showcas.html (accessed Oct. 29, 2020).

[12] M. Lelarge and J. Bolot, “Economic Incentives to Increase Security in the Internet: The Case for Insurance.”

[13] D. Alderson and K. S. Hoo, “The Role of Economic Incentives in Securing Cyberspace,” 2004.

[14] D. Cooper, “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.”

[15] “RFC 6101 - The Secure Sockets Layer (SSL) Protocol Version 3.0.” https://tools.ietf.org/html/rfc6101 (accessed Nov. 24, 2020).

[16] W. Diffie, W. Diffie, and M. E. Hellman, “New Directions in Cryptography,” *IEEE Trans. Inf. Theory*, vol. 22, no. 6, pp. 644–654, 1976, doi: 10.1109/TIT.1976.1055638.

[17] E. R. <ekr@networkresonance.com>, “The Transport Layer Security (TLS) Protocol Version 1.2.”

[18] T. Dierks and C. Allen, “The TLS Protocol Version 1.0.”

[19] “CA/Browser Forum Guidelines For The Issuance And Management Of Extended Validation Certificates,” 2007. Accessed: Oct. 26, 2020. [Online]. Available: https://cabforum.org/members/.

[20] “What Are The Requirements for SSL.com OV and IV Certificates? - SSL.com.” https://www.ssl.com/faqs/ssl-ov-validation-requirements/ (accessed Oct. 27, 2020).

[21] M. Spence, “Job Market Signaling,” 1973.

[22] “Uncertainty and the Welfare Economics of Medical Care on JSTOR.” https://www.jstor.org/stable/1812044?seq=1 (accessed Dec. 28, 2020).

[23] “The Theory of ‘Screening,’ Education, and the Distribution of Income on JSTOR.” https://www.jstor.org/stable/1804834?seq=1 (accessed Dec. 28, 2020).

[24] C. Chawla, “Trust in blockchains: Algorithmic and organizational,” *J. Bus. Ventur. Insights*, vol. 14, Nov. 2020, doi: 10.1016/j.jbvi.2020.e00203.

[25] “INTERPOL report shows alarming rate of cyberattacks during COVID-19.”

https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19 (accessed Jan. 08, 2021).

[26] H. Kox *et al.*, "Economic aspects of Internet security 1 CPB Background Document 1 We would like to thank."

[27] H. Rohani and A. Kamali Roosta, "Calculating Total System Availability."

[28] "MTBF, MTTR, MTTF, MTTA: Understanding incident metrics." https://www.atlassian.com/incident-management/kpis/common-metrics (accessed Nov. 12, 2020).

[29] N. Binh Truong, K. Sun, S. Member, G. Myoung Lee, and Y. Guo, "GDPR-Compliant Personal Data Management: A Blockchain-based Solution," 2019. Accessed: Jan. 08, 2021. [Online]. Available: https://gdpr-info.eu/.

[30] J. Lerner and J. Tirole, "The Economics of Technology Sharing: Open Source and Beyond." Accessed: Nov. 12, 2020. [Online]. Available: http://news.netcraft.com/archives/web_server_survey.html.

[31] N. Iivari, S. Sharma, and L. Ventä-Olkkonen, "Digital transformation of everyday life – How COVID-19 pandemic transformed the basic education of the young generation and why information management research should care?," *Int. J. Inf. Manage.*, vol. 55, Dec. 2020, doi: 10.1016/j.ijinfomgt.2020.102183.

[32] P. Soto-Acosta, "COVID-19 Pandemic: Shifting Digital Transformation to a High-Speed Gear," *Inf. Syst. Manag.*, vol. 37, no. 4, pp. 260–266, Oct. 2020, doi: 10.1080/10580530.2020.1814461.

[33] "Social Networks, Personalized Advertising, and Privacy Controls Terms of Use Creative Commons Attribution-Noncommercial-Share Alike," doi: 10.1509/jmr.10.0355.

[34] G. Cvetkovich, M. Siegrist, E. Zurich, R. Murray, and S. Tragesser, "New Information and Social Trust: Asymmetry and Perseverance of Attributions about Hazard Managers Chemophobia and intuitive toxicology View project New Information and Social Trust: Asymmetry and Perseverance of Attributions about Hazard Managers," doi: 10.1111/0272-4332.00030.

[35] G. A. Akerlof, "The Market for 'Lemons': Quality Uncertainty and the Market Mechanism," *Q. J. Econ.*, vol. 84, no. 3, p. 488, Aug. 1970, doi: 10.2307/1879431.

[36] L. Zavolokina, G. Miscione, and G. Schwabe, *Buyers of Lemons: Addressing Buyers' Needs in the Market for Lemons with Blockchain Technology*. .

[37] "Americans and Digital Knowledge | Pew Research Center." https://www.pewresearch.org/internet/2019/10/09/americans-and-digital-knowledge/ (accessed Nov. 26, 2020).

[38] Y. Jaradat, I. Jannoud, D. Zaidan, and M. Z. Masoud, "CarChain: A Novel Public Blockchain-based Used Motor Vehicle History Reporting System," doi: 10.1109/JEEIT.2019.8717495.

[39] "RFC 6962 - Certificate Transparency." https://tools.ietf.org/html/rfc6962#section-2.1.1 (accessed Nov. 26, 2020).

[40] B. Qin, J. Huang, Q. Wang, X. Luo, B. Liang, and W. Shi, "Cecoin: A decentralized PKI mitigating MitM attacks," *Futur. Gener. Comput. Syst.*, vol. 107, pp. 805–815, Jun. 2020, doi: 10.1016/j.future.2017.08.025.

[41] C. Fromknecht and S. Yakoubov, "CertCoin: A NameCoin Based Decentralized Authentication System 6.857 Class Project," 2014.

[42] "(No Title)." https://handshake.org/files/handshake.txt (accessed Nov. 30, 2020).

[43] B. M. Leiner *et al.*, "A Brief History of the Internet," Jan. 1999, Accessed: Nov. 30, 2020. [Online]. Available: http://arxiv.org/abs/cs/9901011.

[44] K. Kuwabara, "Do Reputation Systems Undermine Trust? Divergent Effects of Enforcement Type on Generalized Trust and Trustworthiness," *Artic. Am. J. Sociol.*, 2015, doi: 10.1086/681231.

[45] J. Opara-Martins, R. Sahandi, and F. Tian, "Critical analysis of vendor lock-in and its impact on cloud computing migration: a business perspective," *J. Cloud Comput.*, vol. 5, no. 1, pp. 1–18, Dec. 2016, doi: 10.1186/s13677-016-0054-z.

[46] J. Opara-Martins, R. Sahandi, and F. Tian, *Critical Review of Vendor Lock-in and Its Impact on Adoption of Cloud Computing*. .

[47] T. Moore, "The Economics of Cybersecurity: Principles and Policy Options 1," 2010, doi: 10.1016/j.ijcip.2010.10.002.

[48] G. Heal and H. Kunreuther, "Interdependent Security: A General Model," 2005.

[49] S. Bradner, "IETF Working Group Guidelines and Procedures."

[50] "IETF | Participate in the IETF." https://www.ietf.org/about/participate/ (accessed Nov. 17, 2020).

[51] "RFC 8179 - Intellectual Property Rights in IETF Technology." https://datatracker.ietf.org/doc/rfc8179/ (accessed Nov. 17, 2020).

[52] C. Lustig, "Algorithmic Authority: The Case of Bitcoin." Accessed: Nov. 19, 2020. [Online]. Available: https://coinbase.com/charts.

[53] D. R. Kuhn *et al.*, "Introduction to Public Key Technology and the Federal PKI Infrastructure," 2001.

[54] Y. D. Wang and H. H. Emurian, "An overview of online trust: Concepts, elements, and implications," *Comput. Human Behav.*, vol. 21, no. 1, pp. 105–125, Jan. 2005, doi: 10.1016/j.chb.2003.11.008.

[55] C. Sierra and J. Debenham, "An Information-Based model for Trust," 2005.

[56] D. M. Rousseau, S. B. Sitkin, R. S. Burt, and C. Camerer, "Introduction to Special Topic Forum: Not so Different after All: A Cross-Discipline View of Trust," 1998.

[57] S. Mariotti and F. Sgobbi, "Alternative paths for the growth of e-commerce," *Futures*, vol. 33, no. 2. Elsevier Ltd, pp. 109–125, Mar. 01, 2001, doi: 10.1016/S0016-3287(00)00058-6.

[58] O. Szumski, "Technological trust from the perspective of digital payment," *Procedia Comput. Sci.*, vol. 176, pp. 3545–3554, Jan. 2020, doi: 10.1016/j.procs.2020.09.032.

[59] M. F. Mubarak and M. Petraite, "Industry 4.0 technologies, digital trust and technological orientation: What matters in open innovation?," *Technol. Forecast. Soc. Change*, vol. 161, p. 120332, Dec. 2020, doi: 10.1016/j.techfore.2020.120332.

[60] M. Warkentin, S. Sharma, D. Gefen, G. M. Rose, and P. Pavlou, "Social identity and trust in internet-based voting adoption," *Gov. Inf. Q.*, vol. 35, no. 2, pp. 195–209, Apr. 2018, doi: 10.1016/j.giq.2018.03.007.

[61] H. Taherdoost, "A review of technology acceptance and adoption models and theories," in *Procedia Manufacturing*, Jan. 2018, vol. 22, pp. 960–967, doi: 10.1016/j.promfg.2018.03.137.

[62] P. Legris, J. Ingham, and P. Collerette, "Why do people use information technology? A critical review of the technology acceptance model," *Inf. Manag.*, vol. 40, no. 3, pp. 191–204, Jan. 2003, doi: 10.1016/S0378-7206(01)00143-4.

[63] A. M. Evans, O. Stavrova, and H. Rosenbusch, "Expressions of doubt and trust in online user reviews," *Comput. Human Behav.*, vol. 114, Jan. 2021, doi: 10.1016/j.chb.2020.106556.

[64] C. Sullivan, "Digital identity – From emergent legal concept to new reality," *Comput. Law Secur. Rev.*, vol. 34, no. 4, pp. 723–731, Aug. 2018, doi: 10.1016/j.clsr.2018.05.015.

[65] "About our practices and your data - Microsoft & Data Law." https://blogs.microsoft.com/datalaw/our-practices/ (accessed Oct. 26, 2020).

[66] T. H. Chen, "Do you know your customer? Bank risk assessment based on machine learning," *Appl. Soft Comput. J.*, vol. 86, p. 105779, Jan. 2020, doi: 10.1016/j.asoc.2019.105779.

[67] D. Solo, R. Housley, and W. Ford, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile."

[68] M. L. Das and N. Samdaria, "On the security of SSL/TLS-enabled applications," *Appl. Comput. Informatics*, vol. 10, no. 1–2, pp. 68–81, Jan. 2014, doi: 10.1016/j.aci.2014.02.001.

[69] "How to Fix Common SSL Issues in WordPress (Beginner's Guide)." https://www.wpbeginner.com/wp-tutorials/how-to-fix-common-ssl-issues-in-wordpress-beginners-guide/ (accessed Nov. 30, 2020).

[70] "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates," 2020.

[71] "Organization Validation Process for OV SSL Certificates." https://comodosslstore.com/ssl-validation-process/ov (accessed Oct. 27, 2020).

[72] "COMMISSION IMPLEMENTING DECISION (EU) 2015/ 296 - of 24 February 2015 - establishing procedural arrangements for cooperation between Member States on electronic identification pursuant to Article 12(7) of Regulation (EU) No 910/ 2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market."

[73] O. Goldreich and Y. Oren, "DEFINITIONS AND PROPERTIES OF ZERO-KNOWLEDGE PROOF SYSTEMS DEFINITIONS AND PROPERTIES OF ZERO·KNOWLEDGE PROOF SYSTEMS," 1990.

[74] "What are zk-SNARKs? | Zcash." https://z.cash/technology/zksnarks/ (accessed Nov. 30, 2020).

[75] E. Ben-Sasson, I. Bentov, Y. Horesh, and M. Riabzev, "Scalable, transparent, and post-quantum secure computational integrity," 2018.

[76] S. Lancaster, D. C. Yen, and S. M. Huang, "Public key infrastructure: A micro and macro analysis," *Comput. Stand. Interfaces*, vol. 25, no. 5, pp. 437–446, Sep. 2003, doi: 10.1016/S0920-5489(03)00043-6.

[77] Kuhn, Hu, Polk, Chang, and Shu-Jen H, "Introduction to public key technology and the federal PKI infrastructure." doi: 10.6028/NIST.SP.800-32.

[78] R. Prodanović, I. Vulić, and I. Tot, "A SURVEY OF PKI ARCHITECTURE," doi: 10.31410/ERAZ.S.P.2019.169.

[79] "Root certificate - Wikipedia." https://en.wikipedia.org/wiki/Root_certificate (accessed Oct. 29, 2020).

[80] "How Log Proofs Work - Certificate Transparency." https://www.certificate-transparency.org/log-proofs-work (accessed Oct. 29, 2020).

[81] "What is Certificate Transparency? - Certificate Transparency." https://www.certificate-transparency.org/what-is-ct (accessed Oct. 29, 2020).

[82] "Principles and criteria." https://www.cpacanada.ca/en/business-and-accounting-resources/audit-and-assurance/overview-of-webtrust-services/principles-and-criteria (accessed Oct. 29, 2020).

[83] "Microsoft Trusted Root Certificate: Program Requirements | Microsoft Docs." https://docs.microsoft.com/en-us/previous-versions//cc751157(v=technet.10)?redirectedfrom=MSDN (accessed Oct. 29, 2020).

[84] "Mozilla Root Store Policy — Mozilla." https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/ (accessed Oct. 29, 2020).

[85] "Root Certificate Program - Apple." https://www.apple.com/certificateauthority/ca_program.html (accessed Oct. 29, 2020).

[86] "Installing the trusted root certificate | Microsoft Docs." https://docs.microsoft.com/en-us/skype-sdk/sdn/articles/installing-the-trusted-root-certificate (accessed Oct. 29, 2020).

[87] "FAQ: How to add root certificate to Mac OS X | OCIO." https://www.eduhk.hk/ocio/content/faq-how-add-root-certificate-mac-os-x (accessed Oct. 29, 2020).

[88] "How do I install a root certificate? - Ask Ubuntu." https://askubuntu.com/questions/73287/how-do-i-install-a-root-certificate (accessed Oct. 29, 2020).

[89] "EV SSL Certificate Guidelines - CAB Forum." https://cabforum.org/extended-validation/ (accessed Nov. 02, 2020).

[90] "Network Security Requirements - CAB Forum." https://cabforum.org/network-security-requirements/ (accessed Nov. 02, 2020).

[91] KPN BV, "Certification Practice Statement PKIoverheid." Accessed: Nov. 02, 2020. [Online]. Available: www.kpn.com.

[92] T. M. I. (CA S. C. member) By Kirk Hall, "Standards and Industry Regulations Applicable to Certification Authorities." Accessed: Nov. 02, 2020. [Online]. Available:

https://casecurity.org/wp-content/uploads/2013/04/Standards-and-Industry-Regulations-Applicable-to-Certification-Authorities.pdf.

[93] C. Diginotar and O. Palmestraat, “Classification PUBLIC Interim Report Fox-IT BV,” 2011. Accessed: Nov. 03, 2020. [Online]. Available: www.fox-it.com.

[94] M. Southam, “DNSSEC: What it is and why it matters,” *Netw. Secur.*, vol. 2014, no. 5, pp. 12–15, 2014, doi: 10.1016/S1353-4858(14)70050-9.

[95] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System.” Accessed: Nov. 18, 2020. [Online]. Available: www.bitcoin.org.

[96] T. Gillespie, “The Relevance of Algorithms PROPERTY OF MIT PRESS: FOR PROOFREADING AND INDEXING PURPOSES ONLY.”

[97] Y. Chen, I. Pereira, and P. C. Patel, “Decentralized Governance of Digital Platforms,” *J. Manage.*, 2020, doi: 10.1177/0149206320916755.

[98] L. W. Cong and Z. He, “Blockchain Disruption and Smart Contracts,” 2018.

[99] P. Warichet, “Section 3: High Availability Catalyst 6500 Bootcamp Section 3: High Availability,” 2007.

[100] “Following the 3-pillar approach to effective security strategy - Ciena.” https://www.ciena.com/insights/articles/Following-the-3-pillar-approach-to-effective-security-strategy.html (accessed Jan. 04, 2021).

[101] W. Wang *et al.*, “A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks,” 2019.

[102] S. Bouraga, “A taxonomy of blockchain consensus protocols: A survey and classification framework,” *Expert Syst. Appl.*, vol. 168, p. 114384, Nov. 2020, doi: 10.1016/j.eswa.2020.114384.

[103] “Consensus Algorithms: The Root Of The Blockchain Technology.” https://101blockchains.com/consensus-algorithms-blockchain/ (accessed Nov. 19, 2020).

[104] D. Liu and J. Camp, “Proof of Work can Work,” 2006.

[105] P. De Filippi, M. Mannan, and W. Reijers, “Blockchain as a confidence machine: The problem of trust & challenges of governance,” *Technol. Soc.*, vol. 62, Aug. 2020, doi: 10.1016/j.techsoc.2020.101284.