OCTOBER 17, 2017

OPPORTUNITIES FOR BLOCKCHAIN-BASED IDENTITY IN HEALTHCARE

MASTER THESIS

JEROEN SCHOUTEN
RADBOUD UNIVERSITY NIJMEGEN & CZ ZORGVERZEKERINGEN
Science, Management & Innovation

Opportunities for blockchain-based identity in healthcare

Master thesis

Science, Management & Innovation master specialisation

Faculty of Science, Radboud University Nijmegen

Name		Jeroen Schouten
Student number		S4064070
Discipline		Mathematics
Host organization		CZ Zorgverzekeringen
Start	Date	03-04-2017
	Academic year	2016/2017
Presentation	Date	24-10-2017
	Academic year	2017/2018
University coach		Egbert-Jan Sol
Host organization coach		Fleur Hasaart
Reader		Tommy Koens
This thesis is confidential?		No

Contents

Acknowledgements

This thesis was realized with the help of several people. First of all, I would like to thank my university supervisor Egbert-Jan Sol for introducing me to the subject of blockchain technology, and for our meetings in which he shared his valuable expertise and gave feedback on my work. I am also grateful to the reader, Tommy Koens, for his feedback during the project.

Special thanks go to my company supervisor Fleur Hasaart who helped me with advice throughout the project and to Tjerk Heijmens Visser who was actively involved in guiding my project.
My gratitude also goes to the participants to the interviews. I'm thankful that they were willing to share their views with me.

1 Executive summary

Services and products are increasingly digital (or digitalized) to ensure a better cost-efficiency or ease of use for society. Individuals must be enabled to participate in these various digital transactions. To protect them in this digital society and make sure that abuse, fraud and criminality are minimized, a robust solution to give individuals a digital identity is needed.

Current systems are not optimal to provide such a digital identity. Digital identities are often scattered across online service providers, which do not interact. This leads to troublesome authentication and much information redundancy. Also, the individual does not have control over who can access and use his personal information. Digital identity data is becoming more valuable and thus much power lies with the companies that hold this data, while at the same time they face increasing threats of cybercrime.

Several of these risks can possibly be obviated with blockchain technology. This technology is characterized by a decentralized governing model providing irrefutable records and possibilities of making trusted third parties obsolete. The trusted third parties decrease efficiency and speed in current system configurations.
A specific application of this blockchain technology is the so-called self-sovereign identity model which advocates absolute control for the individual over his own digital identity, across multiple services and providers. The decentral character of the blockchain network enables individuals to set up a persistent identity, which cannot be controlled or shut off by other parties.
A literary study made clear that blockchain and self-sovereign identity have aspects that can add value in managing identities. However, reservations should be made on the scalability and volatility issues regarding the technology.

Although the blockchain technology has a disrupting potential, innovations in public utility systems like healthcare often have a more incremental nature. Therefore, possibilities of implementation in the dental care subfield were investigated by interviewing dental care providers. However, they did not show a great dissatisfaction with current systems, and there was no sense of urgency to change the identification processes of their clients. This can be partially explained by their lacking awareness of privacy legislation and security risks. Dental care providers want to focus on their main activities and not on security and privacy. Nevertheless, they were able to envision new services that can add value in the dental practice. For some of these self-sovereign identity can be a necessary facilitating technology.

Potentially, self-sovereign identity can become a standard way of digital identification. Governments are changing the current digital identity standards and are experimenting with new features to DigiD and other approved authentication methods. Blockchain might be easily integrated with these standards. Interviewed experts of self-sovereign identity and blockchain recognized the potential of the technology and pointed out that there is momentum to make it a success, as is illustrated by the consortia and actors in the system of innovation that are investigating the possibilities.

Nevertheless, blockchain and self-sovereign identity will not affect the core activities of healthcare providers, who are generally also not aware of many privacy issues. Therefore, they will probably be a passive actor in blockchain innovation. Since health insurance companies have more (financial) means, and an intermediary role which *can* be affected drastically by blockchain, they are most likely to be the ones to stimulate this innovation in the healthcare sector.

The blockchain experts expect self-sovereign identity to become implemented society-wide. To make it also suitable for healthcare, complex requirements and desires from this sector should be supported by the eventual self-sovereign identity framework. Thus, participation of the sector in these developments is beneficial. This holds provided that there is belief that patient-centered care with more data control by patients will take flight and that many additional services can be delivered to clients in the future. It is important to re-evaluate one's processes by actively thinking about them: a new data-model requires rearrangements on all levels of the organization.

This research shows that legislation and organizations' missions are supportive of blockchain-based identity in society. Further commitment to self-sovereign identity experimentation can add value in the future, also for

healthcare. This is, however, not so much regarding current identification processes, but with respect to future services and changing relationships with patients. Raising awareness of security and privacy risks is an important precondition for the adoption of these new robust identity systems.

This report is the result of a Master of Science thesis project, which is set up on the basis of a main research question, subdivided into subquestions. Research methods are described, as well as the results and a conclusion.

2 Introduction/problem definition

Bitcoin was introduced to the world in 2008.[1] It launched a new cryptocurrency technology, combining several existing technical components into one system that could give digital trust a completely new form. The cryptocurrency took some time to get into mainstream attention and acceptance, but eventually became a hype.[2] It was the first time that digital financial transactions were facilitated without the brokering of a trusted third party (TTP), and without a central point of power or vulnerability. A payments network consisting of peers had been constructed with the aid of asymmetric cryptography and a consensus mechanism. Thus, the peers could rely on privacy, security, and anonymity.[3]

The Bitcoin protocol was the first application to make use of what is called blockchain technology. A blockchain consists of a digital ledger, shared between entities in a peer-to-peer network, that essentially functions as a database that keeps track of who owns a financial, physical or electronic asset: a unit of currency, items inside a shipping container, or health data, for example.
Some blockchains can execute small programs which serve as contracts. Crucially, every participant in the network can keep an up-to-date copy of the blockchain. An update consists of appending a block of transactions which are validated by the users. The security and correctness of the information is maintained through cryptography to ensure that all copies of the ledger match each other and the information is safe and secure. The network is Byzantine Fault Tolerant (BFT), which means that even malicious entities in the network cannot abuse or corrupt the database.

As the bitcoins became more valuable and the network expanded, interest in blockchain also increased. It was discovered that blockchain had the potential to be of value in a much broader context than financial transactions alone. Since then, many new 'flavours' of blockchain have emerged. Variations exist in terms of permissions, consensus mechanisms, programming language and openness, for example. It is questionable if this jungle of different platforms merely signifies the pre-shake-out phase which will lead to one dominant blockchain design, or if more of these platforms will find their place in the future. The diverse range of solutions/platforms seems promising, but a real application on a significant scale has not yet emerged, except perhaps for Bitcoin, but even Bitcoin's user base is fairly small with around 17 million users. (These are only estimates, since the number of wallets and users do not correspond 1-on-1. [4][5]) Hence, there is no platform that can be regarded as a killer app or the top dog who will dominate the mature phase of the technology.

Blockchain technology's disruptive potential has been widely advocated, so companies and organizations feel the urge to latch onto the experiments and research that are being conducted at the moment. Blockchain can potentially overthrow their existing business models. Therefore, monitoring the current developments and also influencing their direction is of vital importance, especially for actors who have some intermediacy role in their value chains. Only thus can they structurally adapt their business models and reorient their role in such a way that they will survive a disruptive innovation unscathed. Governments, firms, institutions, startups, the media: they have all taken up the subject.[6]
Research on blockchain technology is still in its infancy. The number of (exploratory) studies on possible applications is still increasing explosively and the technology can be labelled a scientific hype: current state-of-the-art has just passed the highest peak of the technology hype cycle.[7] As such, many new ideas and use cases are invented. Also within a healthcare context. For example, the US Department of Health and Human Services has organized a challenge to come up with the best use case for applying blockchains in healthcare.[8] But these cases are mostly not thoroughly investigated or tested yet. So it is still a big question whether the technology can really live up to its hype. It is worth noting that the Dutch government is now also starting to explore the possibilities of this technology. This is exemplified by Zorginstituut Nederland's development of a blockchain-based log assisting patients' home care.[9]

That blockchain will become a disruptive innovation is not an open-and-shut case. Some present it as the most disruptive innovation since the Internet, as Internet 2.0 [10], but others are more skeptical about the reach of the technology. Developments are going fastest in the financial sector (where it also started, with Bitcoin), but in other fields too interest is increasing. Examples are logistics, the energy sector, but also healthcare. What can blockchain mean for a health insurance company? Can blockchain bring added value to the healthcare chain? Will the current system with its many actors and roles be drastically rearranged?

An important recurring factor in possible blockchain applications – which are being screened and ideated in consortia like the Techruption field lab in Heerlen[11] – is the authentication and authorization process for persons and organizations. In short: identification. For instance, the most fruitful project that has spawned from Techruption is a so-called Self-Sovereign Identity Framework. A self-sovereign identity is a digital identity which is fully controlled by the individual. Such a blockchain-based identity framework can serve as a platform for multiple applications in different fields. The question is if such blockchain-based identity can also be applied in a healthcare context, between different actors like patients, healthcare providers, and health insurance companies.

Digital identity has been a troublesome concept in the past (see also chapter 5). Categorizing the different considerations, we see that three perspectives are most important in assessing the true added value of self-sovereign identity technology: socio-economic, technical and legislative perspectives. Socio-economic issues are for example the costs of this new technology – think of the implementation costs and the costs of abandoning old methods – and the new functionality that it brings to clients in terms of empowerment and decentralization. But also perception and attitudes towards the technology are vital. These considerations are closely linked to technical feasibility constraints: scaling up the technology (to national-level implementation, for example) seems to be problematic and making the different applications interoperable is no trivial matter either. Lastly, legislation and policy regulations should be taken into account. The distributed storage nature of blockchain gives rise to questions on data ownership and access. Blockchain technology might be useful in financial environments, but strict (European) privacy and patient protection laws[12] might make implementation in a healthcare context more difficult. So for each application a data protection impact assessment is required.[13] These perspectives are depicted in the following framework:

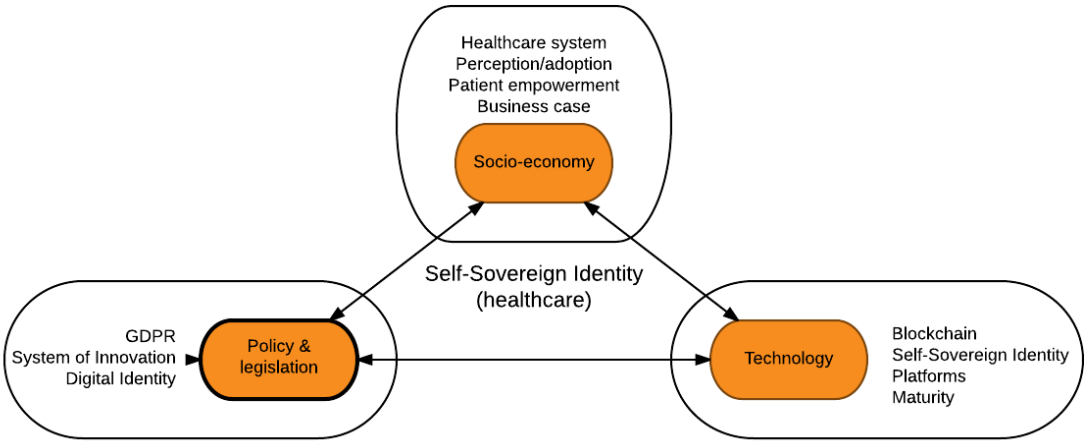

Figure 1: Framework for Self-Sovereign Identity in healthcare.

The inherent qualities of blockchain technology promise several socio-economic opportunities in healthcare: trusted intermediaries become redundant and transaction costs can be reduced. Also, blockchain technology offers a new framework to store digital identities of patients. This is with the additional characteristic that the shared data is updated nearly in real-time and that the patient potentially can get more control over his own data.[14] These strengths of the technology can answer several needs that arise from deficiencies in current health systems. Weaknesses of data management systems that are presently in use are amongst others: a central point of failure, varying data standards, high transaction costs, limited access to population health data, difficulties in establishing trust networks and inconsistent rules and permissions.[15]. However, many of the problems with current systems mentioned earlier have underlying causes which blockchain cannot affect.[16]

While blockchain may thus have its advantages and significant potential to be a game changer in healthcare, it is important to note the technical limitations of the technology. Blockchain might improve standards in interoperability, security and privacy, but it certainly is not a complete substitute for an organization's database. Applications based on blockchain are not optimized for vast amounts of data that need absolute privacy and instantaneous access within an individual organization. Nonetheless, there are efforts to overcome this, as is

exemplified by the BigchainDB protocol.[17] As for now, parties who are experimenting with the technology are very reticent about putting sensitive information about patients 'on-chain'.[16]

Important to consider in this respect is the type of blockchain to be used. Every use case has its own requirements. These can relate to the need for smart contracts linked to the blockchain issuing permissions to stakeholders in an automatic way. Or to the nature of the information stored on the blockchain and possible links to other databases. Also relevant are limitations as to type and size of data that can be stored on a blockchain. Standardized data, like gender and age can be easily stored on the blockchain, allowing immediate access and visibility. However, more abstract data types (like MRI-images) and expansive medical details might be less suitable, since they would require a blockchain with enormous computing power.

The legislative context should also be taken into account when assessing blockchain technology. The Wet bescherming persoonsgevens (Wbp) sets severe limitations on the use of personal data. Its successor, the General Data Protection Regulation (GDPR) poses additional demands on storing and processing data. Blockchain's encryption methods should support these requirements. Also new possibilities for granting ownership of the health data will arise. Regarding patient-centered care it could be desirable that patients get more control over who can access their data. Blockchain can enable such new configurations, but for each of them data protection impact assessments are required.[13]

2.1 Reading guide

This research has the goal of assessing the implementation opportunities of blockchain technology in the context of identity management in healthcare. The problem definition and the motivation for the research have been expounded in this chapter. Because of the explorative character of the research, this will be a story converging from a broad problem statement to a more focused domain.
The focus of the research will be further elaborated upon in the chapter 'Research'. Arguments will be provided for the several research questions. These research questions constitute a delineation and time frame for the research.
In the chapter 'Methodology' the general approach to the research is explicated and supported. The used methods are explained per subquestion.

First of all, a theoretical framework has been constructed: definitions and historical developments of digital identity and closely related notions are being explained. (This is in accordance with the evolutionary systems of innovation approach.) Furthermore, the state-of-the-art in this domain is described by shortly introducing important initiatives and platforms that provide digital identity. A comparative look at these platforms gives more insight in the current issues.
Likewise, important concepts and characteristics of blockchain technology are shortly treated. Once again a comparison of the most important platforms should give a better understanding of tradeoffs and opportunities that blockchain offers.

In the next section of this report the (healthcare) context is clarified. The Dutch healthcare system is being treated very briefly to sketch the roles of the different actors. To bring further focus, one healthcare subdomain is treated in particular: oral care. The processes of identification and personal information management within this subdomain are described.
The mission statement and values of the commissioning company, CZ health insurances, will be linked to the identity framework and a stakeholder analysis will clarify the project configuration.
A systems of innovation (SI) approach will be used to analyze the results of the interviews. But first a rationale is given on why this approach is suitable in a blockchain context.

The literature study that will have the theoretical framework as its result, is complemented with interviews held with different parties in the healthcare chain. Primary information of healthcare providers and CZ is used to fill in relevant process visualizations. Besides, interviews with healthcare providers give an insight in the technology acceptance level. The insights and opinions extracted from these interviews are included in the chapter 'Discussion with healthcare providers'.

The concepts of blockchain technology and self-sovereign identity are very technical and therefore less easily grasped by laymen, a category which nearly all healthcare providers belong to. Because of this, the results of

the interviews with the healthcare providers are 'validated' in a number of interviews with blockchain experts, who can spot misconceptions and assess technical feasibility. They will also have more to say on the necessity of using blockchain for the proposed identity system and on the innovation system in which blockchain experiments are pursued.

The section 'Discussion' comprises an analysis of the most important results. Relations between different outcomes are established in this chapter. The meaning and effects of the results are contemplated. Returning to the research questions, they will be answered in the chapter 'Conclusion'. Following this, a set of recommendations with respect to further research and next steps is added.

3 Research

This section comprises the research questions that were devised on the basis of the problem definition stated above. First of all, the goal of the research is made clear; a goal with which all the research questions will be in alignment. The main research question is concisely put. Addressing the multiple facets underlying this question different subquestions were composed that will enable a structural examination of the problem.

Goal
The goal of this research is to investigate whether blockchain technology can add value in managing digital identities in a healthcare-related environment.

Research questions
This goal can be achieved by answering the following research question.

Main research question:
Can self-sovereign identities using blockchain technology improve the management of identities and access in the interactions between a health insurance company and its external stakeholders in a cost-efficient manner within Dutch and European legal boundaries?

The research question is subdivided into 8 subquestions. This high number is explained by the orienting and thus broad character of the research. A holistic view on the problem is vital in the chosen approach.

Subquestions:
1. *What is blockchain technology and what are its main characteristics?*
   A first step is understanding the core strengths and weaknesses that blockchain technology has. These can give a first indication on possible use cases.
2. *What is self-sovereign identity?*
   Likewise, the concept of self-sovereign identity is not straight-forward. An overview of its principles and a comparison with other forms of digital identity is necessary. The historical development of the concept is important in the system of innovation.
3. *What is the current state-of-the-art of blockchain applications in health- and identity-related problems?*
   Incumbent applications are a good indicator of issues that still need to be resolved and tradeoffs that exist.
4. *What interactions and legal boundaries with external stakeholders concerning identity does a health insurance company maintain in the Dutch healthcare system?*
   A closer look at the context in which the applications should find their way. Relevant actors and institutions have a great impact on the innovation process.
5. *What requirements must a feasible blockchain application meet to provide a desirable identity system between a health insurance company and an external stakeholder?*
   Taking a closer look at selected actors in the system, their requirements and desires are important to assess the possible added value of the new technology.
6. *To what extent does self-sovereign identity technology fit these requirements?*
   The most characteristic aspects of blockchain and self-sovereign identity are analyzed by coupling them with the requirements of the actors in the healthcare field.
7. *What could self-sovereign identity technology add in terms of business value?*
   This is closely linked to the previous question. Next to requirements also business rules and constraints should be added to the model.
8. *What should be the role of the different actors in the system of innovation?*
   An application can satisfy all requirements and have significant added business value for all actors, but the process towards this application is not trivial and has some prerequisites and ideal roles for certain actors.

4 Methodology

The overall research has an orienting character: hence qualitative research methods are used, to extract in-depth opinions and a deeper understanding of underlying motivations, causes et cetera.
The individual subquestions each require suitable methods to be answered. The used methods are briefly accounted for in this section.

What is blockchain technology and what are its main characteristics?
What is self-sovereign identity?
To gain a good understanding of what Blockchain and Self-Sovereign Identity are, an extensive literature study is required. Academic literature and business reports can provide the necessary background information.

What is the current state-of-the-art of blockchain applications in health- and identity-related problems?
New solutions and use cases can be garnered from secondary sources as well. Whitepapers and business websites will yield valuable information, but also primary sources like presentations and pitches at the Techruption sessions or other seminars can prove useful. CZ's own efforts can be obtained from internal documentation. A comparative analysis between some of the most used blockchain platforms will be included.

What interactions and legal boundaries with external stakeholders concerning identity does a health insurance company maintain in the Dutch healthcare system?
An overall overview of the Dutch healthcare system can be obtained by external literary sources, but a more detailed analysis of a health insurance company's position with respect to identity will be procured from internal documentation of CZ. This overview is important, since a blockchain application will always involve multiple parties. Multiple stakeholders must support a use case before it can become successful. Talking with CZ's employees can provide the necessary information.

What requirements must a feasible blockchain application meet to provide a desirable identity system between a health insurance company and an external stakeholder?
The goal of this question is to determine the desirability of applying self-sovereign identity. In other words, to determine in what situations blockchain-based identity could add value according to professionals from different stakeholders. And more generally, what these professionals want to achieve in working with blockchain technology. In a series of interviews with professionals from healthcare providers and their colleagues who have affinity with innovation and/or IT, they will be asked to translate perceived opportunities and requirements and hold these against a proposed use case.

To what extent does self-sovereign identity technology fit these requirements?
What could self-sovereign identity technology add in terms of business value?
This question will be addressed by conducting at least 5 semi-structured interviews with participants who have in-depth knowledge on blockchain technology. Interview questions will focus on what kind of business problems self-sovereign identity could add value to on an inter-organizational level. Thus, desirability requirements can be coupled with technical constraints as well as the characteristics of the innovation system.

What should be the role of the different actors in the system of innovation?
The insights of the blockchain experts will be held against a selected innovation model. The garnered overview of the current context, the opinions of the interviewed healthcare providers and experts will be infused inside the model. Thus, a better understanding of future steps and opportunities can be gained. The most important actors in the system and their roles in the process will be devised.

Systems of Innovation approach
The overall structure of the research is devised to support an approach to innovation which can help understand the investigated technology. The chosen framework is the Systems of Innovation (SI) approach.

As blockchain is a technology which promises to be radical and to shift relations between many actors, a holistic view of the whole system seems the right way to tackle the subject. Therefore, the System of Innovations approach as explained by Edquist[18] is chosen. This conceptual framework can explain in what kind of system

we are embedded, what actors are of importance, how technology is shaped, and what this means for the innovation process (particularly in a high-tech context).

Strengths of the SI approach:

- The SI approach places innovation and learning processes at the center of focus.
- The SI approach adopts a holistic and interdisciplinary perspective.
- The SI approach employs historical and evolutionary perspectives, which makes the notion of optimality irrelevant.
- The SI approach emphasizes interdependence and non-linearity
- The SI approach can encompass both product and process innovations, as well as subcategories of these types of innovations.
- The SI approach emphasizes the role of institutions.

Weaknesses of the SI approach:

- The SI approach is still associated with conceptual diffuseness.
- Boundaries of innovation systems are not clearly defined.
- It is rather a conceptual framework than a formal theory, without providing causal relations among variables.[19]

The focus on learning processes, the interdisciplinary perspective and the role of institutions like laws are very relevant to this research. Historical and evolutionary perspectives are also import to include since they can illustrate troubles and opportunities with the current issues. The approach being rather a framework than a formal theory, the results of using it will be more descriptive than persuasive.

Components of the system

The systems in the SI approach consist of actors and relations between them. The actors are organizations and institutions. The meaning of institution has been the subject of debate and conceptual diffuseness, but for the sake of clarity we define it here as the rules and regulations, the cultural environment and similar factors. So there is no overlap between organizations and institutions.

Relations between organizations in an innovation system may be of a market and or a non-market kind. Markets deal exclusively with transactions, while for example an interactive learning process cannot be captured in a market transaction. Organizations are embedded in institutions, but institutions are also embedded in organizations. This is of influence to the innovation process.

Functions of the system

A system has a common goal, role, or such. This is achieved by the activities that are performed inside the system and the functions that the organizations and institutions have. Functionalities include research, implementation, end-use and education.

Boundaries of the system

Important with this approach is the setting of boundaries to your system of innovation. There are three types of boundaries: functional, sectoral, and geographical.

Spatial/geographical boundaries are slightly different depending on what kind of system of innovation you are looking at. National SI's have the national borders as their boundaries, while regional SI's geographical boundaries should be determined on the basis of knowledge spill-over and inward orientation of innovation. For sectoral SI's this dimension of boundary is less relevant.

Sectoral boundaries pose limits concerning specific technology fields and/or product areas. Where the boundaries are drawn in terms of geography can vary.

Not the whole socio-economic system can be included in the system of innovation. Which parts can, is a matter of functional boundaries. These have to be defined for all kinds of SI's. This remains an open problem in the literature and is now mostly solved by intuitive arguments.

The SI approach supports an evolutionary approach. This means that innovations are not collectively aimed at reaching an optimal direction of progress. Rather, innovations are placed in a local context with institutions having a great influence, thus not ultimately leading to an optimal improvement. This is in accordance with the situated approach by Janssen.[20]

5 Identity & Digital Trust

Notions pertaining to digital identity will be explained in this chapter. To better grasp the (historical) importance of digital trust, a theoretical framework is set up around these central concepts. Definitions are stated to delineate concepts to be able to discuss and work with them. In this way, an innovation system boundary can be set on the applications that belong to identification and self-sovereign identity. Current issues are coupled with historical developments to stress the bottlenecks and impediments when trying to improve digital trust and identity management.

5.1 Concepts

Main definitions

Digital identity

To discuss and work with digital identities one first needs to define what an identity is. The philosophical implications raised by this question will for now be ignored. For the sake of alignment with online identities, we say that an identity is a set of attributes appertaining to a certain entity.[21]

Taking this to a digital level, we say that a digital identity consists of information on an entity which is used by computers as a representative of an external agent. An alternative definition is: 'a digital identity is an online or networked identity adopted or claimed in cyberspace by an individual, organization or electronic device.' [22] This means that objects can also have an identity.

Attributes are pieces of information on an entity. Hence, identities are sets of attributes. Examples of attributes are: skin-colour, medical records, a purchase record, or a bank account balance. As of today, digital identities are commonplace, nearly every online service makes use of a way to identify the persons it deals with. As such, nowadays all of the information generated by someone's online activity can be regarded as pertaining to his identity. Thus, usernames and passwords have become part of a person's online identities, but also online search activities and transactions.

Some of these attributes uniquely determine a person (like a social security number, BSN). But other attributes on which access control can be based, are not unique for a single person. These preserve anonymity (e.g. the fact that you're registered as a student, or that you are over 18).

A digital identity is a social construct and highly contextual.[23] Especially on the Internet where you establish an identity with every application you interact with. Contextuality of identity means that individuals reveal or ascertain different aspects of their identity in different contexts. To illustrate this, for a car rental service my driver's license will be an important part of my identity while for Facebook it is not. In this sense, an identity is a singular perspective on an entity within a mutually acknowledged relationship.[23] Identities are however linked to each other (and a person) by companies to retrieve valuable knowledge. These linkages are, however, often unknown to the person whose identities it are. This concept is called profiling and is used for the benefit of marketing purposes.[24]

Digital trust

Trust is something that underpins every interaction, and particularly every transaction. In the volatile and sometimes unpredictable world of digital business, new business patterns spontaneously bring together many different people, businesses, things and algorithms, at massive scale. This creates the need to establish instant trust, such that value can be realized.[25] Regular trust models do not suffice to describe the emerging digital identities.

Gartner defines digital trust as a measurable confidence in the distinct expectations that:

- A person, business, thing or other entity is who or what it claims to be.
- It can represent itself or be faithfully represented by another entity.
- It is able to fully participate in digital business interactions and consents to do so.
- It does so in a truthful, predictable, reliable, secure, safe, ethical and privacy-respecting manner.[25]

Digital trust is achieved by two seminal mechanisms every (general purpose) identity system should incorporate: authentication and authorization.

Authentication

Authentication is the method of verifying an identity. One party affirms his identity to another party. Authentication is established using authentication factors: factors that provide some evidence that someone at the end of the communication channel is who he says he is. Three kinds of factors can be used to authenticate an identity:

- Knowledge factors: for example, a password.
- Possession factors: for example, smartcards, hardware tokens etc.
- Being/inherence factors: for example, biometrics.[26]

With authentication there is a clear tradeoff between security and ease of use. Nowadays, services which involve sensitive or valuable data tend to use a combination of multiple factors for authentication. This is called multi-factor authentication. Examples are DigiD (password and SMS) and online banking (hardware device/debit card and PIN-code).

Boundaries to identity

It is important to note that authentication factors are part of a person's identity, but that they are not their complete identity. Information which is not used to verify that someone is who he claims to be, but which also relates to him, is also part of his identity and used as such by organizations he interacts with. A date of birth can be an authentication factor. A medication history probably is not, although it is part of the digital identity.

Authorization

Authorization is the granting of access to resources to someone who has been authenticated. Authorization relies on authentication since access is determined on the basis of one or more attributes that have been verified.

Attribute based identity

With our first definition of digital identity in mind, it seems only natural to look at Attribute-Based Access Control (ABAC) Also called Claim-Based Access Control (CBAC), it is a logical access control model that controls access to objects by evaluating rules against certain attributes of the entities.[27] Since authentication and authorization are only based on certain attributes, the need to only reveal those attributes is recognized. A next step is to only reveal the selected attributes when identifying or authorizing. The I Reveal My Attributes project (IRMA) is an example of this.[28] Only relevant attributes are revealed and identities are not linked or coupled.

Authentication levels: STORK QAA

To identify possible problems with authentication methods, it is important to measure the quality of authentication methods. The quality of authentication methods and electronic identification can be assessed with the help of a framework. In Europe the framework STORK QAA is mostly used. STORK is an initiative supported by the European Union. It defines 4 levels of security.[29]

QAA Level	Impact of erroneous authentication
1	Very low or negligible
2	Low impact
3	Substantial impact
4	Heavy impact

With level 1 authentication identification factors are copied without further verification. With level 2 authentication verification of the identity takes place on the basis of some trusted central registration, but physical appearance is not required. With level 3 authentication 2-factor authentication is required and level 4 requires at least one physical appearance of the user.[30]

Know-Your-Customer (KYC)

Certain types of organizations have a legal obligation to assert the identities of their customers. An instance of the due diligence that these organizations face, is KYC. It requires that organizations are aware of their clients' identity to a certain extent, such that their services cannot be misused for criminal activities like money laundering. [31] Examples of these organizations are banks, real estate brokers and insurance companies.

In the healthcare field there is also specific legislation regarding identity. There is a law on identification obligation of patients in healthcare.[32] Linked to that there is de Wet gebruik burgerservicenummer in de zorg (Wbsn-z) which infuses the model where patients are identified by means of their social security number (BSN).[33]

Bitcoin is funded on whole other principles. It is based on anonymity, not on knowing who you are dealing with. Some argue, that this is one of the difficulties for a system like Bitcoin: it provides a safe hideout for criminals.

5.2 Issues

In modern societies communication is increasingly facilitated by information and communication technology (ICT). Guaranteeing privacy and security of this communication and the storage of the appertaining data is a serious precondition for a robust society.[36]

The Internet was not designed to identify persons. Rather, it serves to identify machines, and facilitate communication between these machines.[35] This fundamental mismatch leads to several difficulties in managing digital identities.

Fragmentation

Because of the fact that the Internet doesn't inherently support identification of persons, every Internet application or service needs to take care of this identification by itself. Thus a myriad of identification methods and services has arisen, with no real consistency or shared architecture. This fragmentation brings a couple of problems with it:

No ease of use

Because people are confronted with an increasing number of internet services, they are also faced with more and more authentication procedures. For all of these procedures they have to remember usernames and passwords. For every procedure they have to go over the same tedious filling-in of registration forms.

Honeypots

This redundancy is hopelessly inefficient. Besides, every organization gathering a complete set of personal details from its clients is a potential target for cybercriminals and identity thieves. Organizations are often obliged to have all this information, or they want to have access to it out of trust-considerations. Thus, they are attracting unwelcome intruders by complying with the law.

As a consequence, other laws (and reputation concerns) enforce these companies to protect all this data, which incurs them high costs. According to Gartner these amounted to $81.6 billion in 2016.[106] The number of victims of identity fraud are also rising. According to CBS data,[36] in the Netherlands 1% of people older than 15 have fallen victim to identity fraud in 2015. A research performed by the Javelin Institute showed that in 2016 6,1% of American citizens fell victim to identity fraud.[37]

Weakest link in security

The identification step is one of the most vulnerable steps in digital security systems. People use passwords with low-entropy. Furthermore, they store them at unsafe places.[38]

Individuals don't read the terms of use of their applications. These are not user-friendly: long pieces of text no one wants to read, with terms and conditions that only become relevant in a few cases.[39]

Users have on average 92 different accounts registered to the same email address [40]. Often the same passwords are used for many different services.

Lack of control

Closely related to this, is the powerlessness persons can experience while dealing with their digital identities. In most cases, it is not clear what happens with personal details after they have been handed over to organizations or services. Who can use them and how? Surveys conducted by the European Commission sketch a picture of a world where persons are not secure about their own data anymore.[41]

Lack of identity

At the same time, having an identity is not even obvious. There are 1.1 billion people in the world who live without an officially recognized identity.[42] ID2020 is a public-private partnership dedicated to solving the challenges with identity for these people through technology. This organization poses four requirements to identity:

Personal: unique to you and only you
Persistent: lives with you from life to death
Portable: accessible anywhere you happen to be

Private: only you can give permission to use or view data

It is one of the United Nations' Sustainable Development Goals to provide such a legal identity for all, including birth registration.[43]

The lack of legal identity is especially problematic in situations where poverty reigns. Today, legal identities are increasingly important in associating with institutions, to be able to operate in society.[44]
In light of the turmoil in the Middle East and Northern Africa and the ensuing refugee crises that have a devastating effect on solidarity and social coherence in Europe, statelessness of people is now especially relevant. The provision of a self-sovereign identity might help these people and the countries they get stranded in.

5.3 History

To understand the innovation process regarding identity, in this section an evolutionary perspective is given on digital identity.

Digital identity has evolved over the last decades, in the pursuit of dealing with the mentioned issues. The work of Christopher Allan[45] gives a good overview and is seminal to understanding the current blockchain-based efforts. Four phases can be distinguished in the evolution of online identity: centralized, federated, user-centric, and self-sovereign.[45] These are not phases in the strictest sense of the word, since they do not follow linearly on one another. The advent of a new phase does not mean the end of a prior form of identity.

Centralised identity

The centralized identity model is a description of identity where administrative control is with one authority or hierarchy. In the early days of the Internet several organizations took up these administrative tasks. Take for example ICANN, which regulated the domain names.
Problems do remain with such configurations: users are forced to use a certain authority, which can deny or erase their identity. Current-day examples of these centralized identity providers are tech-giants like Google or Facebook who now have control over a considerable portion of people's online identities.

Federated identity

This term describes administrative control by multiple, federated organizations. Federated identity made its entrance at the turn of the century. Microsoft Passport was an example of a service which allowed users to authenticate on different websites with the same identity. This still put Microsoft at the heart and control of the users' identities, but at least some ease of use was added. Later more truly federated systems were established, where control of the identities was in the hands of a small group of organizations. Thus, it improved on the problem of balkanization.

User-centric identity

User-centric identity consists of individual or administrative control across multiple authorities without requiring a federation. Its aim was to create a persistent online identity into the very architecture of the Internet.[45] Initially, this movement focused on creating a better user-experience. The definition soon expanded to include the desire for users to have more control over their identities and for trust to be decentralized. Powerful institutions co-opted their ambitions and kept them from fully realizing their goals. Ultimately ownership of user-centric identities lies with the entities that register them.

Self-sovereign identity

Self-sovereign identity is the first model which advocates true individual control across any number of authorities. There is however no consensus on what self-sovereign identity is precisely. Allan tries to demarcate it by giving ten principles specific to it. These principles are:

1	Existence	Users must have an independent existence
2	Control	Users must control their identities
3	Access	Users must have access to their own data
4	Transparency	Systems and algorithms must be transparent
5	Persistence	Identities must be long-lived
6	Portability	Information and services about identity must be transportable
7	Interoperability	Identities should be as widely usable as possible

8	Consent	Users must agree to the use of their identity
9	Minimization	Disclosure of claims must be minimized
10	Protection	The rights of users must be protected

As can be seen, several of these principles (i.e. 1, 5, 6 and 8) are also echoed in the ID2020 requirements for a legal identity.

The desired aspects are very much in line with what blockchain can offer (see chapter 6). Self-sovereign identity implementations are usually based around claims and attestations in which often actors can play different roles. We take the terminology of the Self Sovereign Identity Framework (see section 6.5) as an example to illustrate the mechanism.[46]

Usually the self-sovereign identity system is used to facilitate electronic (business) transactions. A general form of this is that an end-user wants to use a service by a service supplier. In order to use this service, he should prove attributes about himself. (Vice versa one can imagine that the service provider must prove his identity). The service supplier is a Relying Party (RP) who gives out an attestation request: he needs information about the end-user to fulfill business rules and to ensure the transaction will be beneficial to him. The user processes this request and gathers the desired attestations, whether they be stored on his phone, in a public blockchain, or should be generated first. The third kind of party is the Attestation Issuer, who issues missing attestations that are required.

The model is based around statements. An attestation is a collection of statements about the veracity of another collection of statements. The original set of statements can also be named a claim. The receiver of an attestation should be able to validate the commitment of the attester to the claims. The commitment should thus be in the form of a digital signature or a pointer to data in a blockchain.

Identification of nodes in the network takes place by means of decentralized identifiers. A Decentralized Identifier (DID) is essential for participating in the network and doing transactions. This is the number/name/string by which someone is identified. A Cryptographic Identifier (CID) is a DID which is cryptographically linked to a certain private key.

Use case
To illustrate the workings of Self-Sovereign Identity based on attestations, an example is shown of a patient (the end-user) who wants to identify himself when going to the dentist.

In order to be eligible to receive care by the dentist the patient must give some personal details for authentication and prove that he is insured. The dentist (Relying Party) has decided that an attestation from a recognized health insurance company is sufficient for him to trust the patient and offer him his services.

1. First, the patient needs his health insurance company to attest to his insurance. CZ will be the Attestation Issuer in this case and the patient sends CZ a digitally signed attestation request. The statement of this request might be: 'I have a basic insurance with CZ Health Insurances.'
2. The attester verifies the patient's insurance. He puts his signature in the public blockchain, so that it can be used by others, to verify that his attestations are genuine.
3. The issued attestation with his signature is sent back to the patient, such that he can use it.
4. The patient now requests the service of his dentist, namely: access to dental care.
5. The dentists can only grant this access when he is shown some verified claims, like the insurance package and the authenticating personal data. So he requests the attestations from the patient.
6. After the patient has given him the required attestations, the dentist checks their validity in the public ledger.
7. Dependent upon this validity, the healthcare provider grants or denies access to the patient.

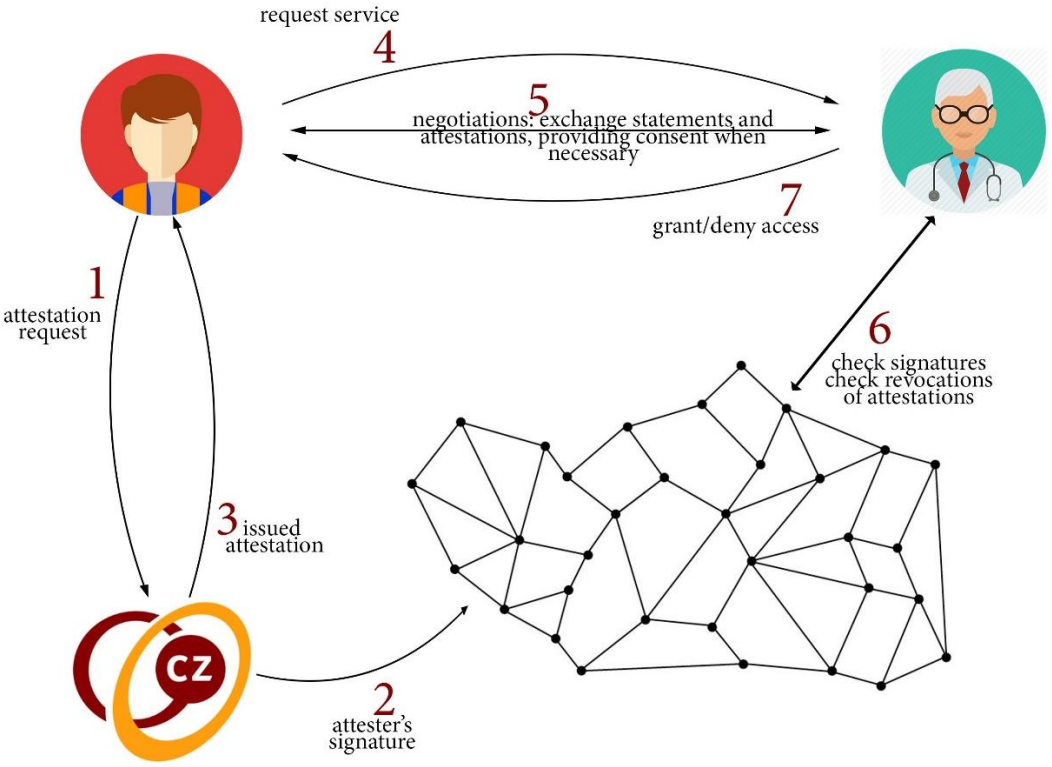

Figure 2: Workings of the SSIF framework with attestations.

Thus a secure identification is guaranteed. Several state-of-the-art applications will be briefly described in the following chapter, as well as the cryptographic principles on which the security is based.

5.4 Dutch and European digital identity

We have discussed current issues with digital identity and looked at related historical developments. Now it is time to connect this with the direction the Dutch national system of innovation is headed.

The Dutch digital identity system which is called eID (electronic identification), comprises a set of several trajectories, which consist of the development of new public eID methods, an agreement system and the experimentation with bank log-in methods in the public domain.[105]
However, the Algemene Rekenkamer concluded in 2016 that several preconditions for a good functioning of the system were not satisfied. The governance structure is complicated and responsibilities are ambiguous. On several essential parts decisions are not yet made or elaborated. They conclude that an actual integral business case and comparison with alternatives is missing. An integral vision on the supervision of the system is missing as well.[59]
Its principles and starting point are linked to the Generieke Digitale infrastructuur (GDI) and it also provides a framework for authentication methods which should also be applicable to authentication in other countries. (Cf. the European eID project).

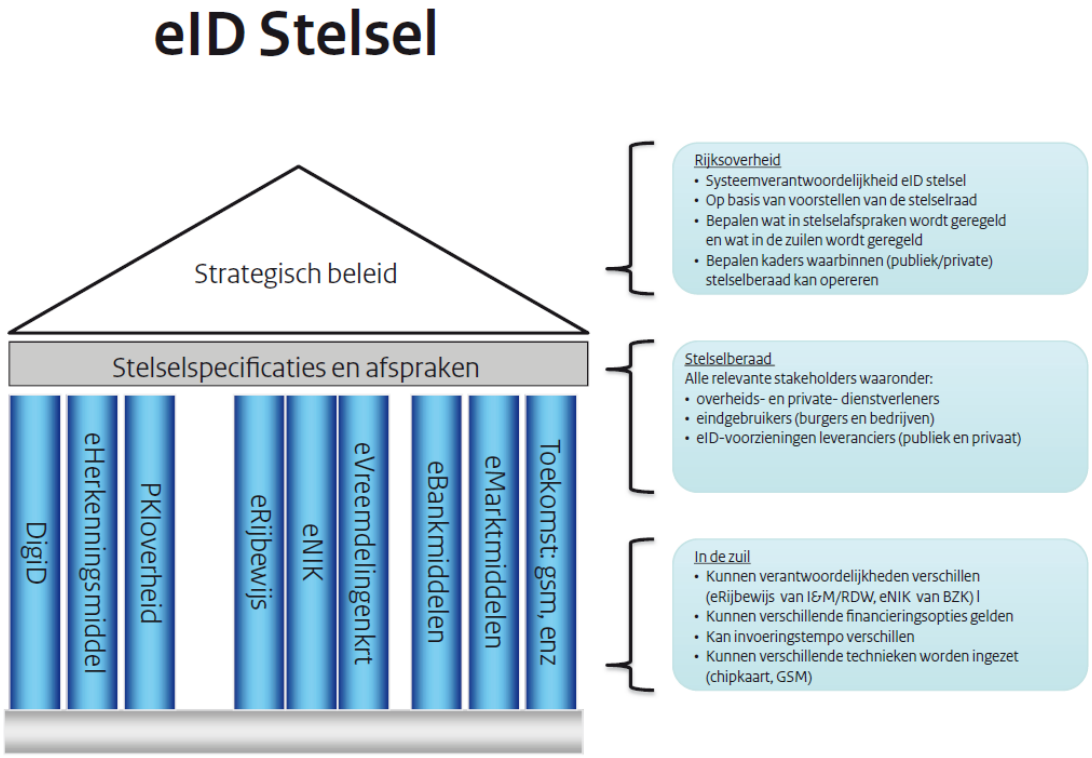

Figure 3: The Dutch eID system.

The Dutch eID system thus comprises several components of which a few will be explained below.
The system already aims to take away some problems that existed with earlier methods of identification. It will not be the service provider that determines the authentication method, but the customer can choose which method suits him best. Thus it adds ease of use. Control is however not decentralized, and as already mentioned, it can be unclear who has which responsibilities.

DigiD
Since 2004 DigiD has been in use as the digital identification method used by the Dutch government.[50] Thirteen million Dutch citizens had a DigiD-account as of December 2016. Through its history, DigiD has been plagued by security incidents. The maintenance/management of DigiD has in its beginning years not been in the hands of one organization for long time, which has stalled development and innovation, leading to the persistent use of the suboptimal username/password combination, which can voluntarily be complemented with sms-authentication. Generally speaking, for many services the security level that DigiD can provide, is too low. Logius, the curating organization, says a new identification method will become available, with an improved security level. (DigiD distinguishes three levels of security: basic, medium and high. Username/password is basic, with SMS added it's medium.) Logius says that as of 2018 driver's licenses and identity documents will get a chip. This new way of identification is part of the eID programme.
DigiD's authentication is based on persons' social security number (BSN). Therefore, use of the DigiD authentication method is restricted to organizations who have a legal permission to operate BSN data (i.e. governmental and semi-governmental organizations who have a public function/utility.)

eHerkenning
eHerkenning is similar to a DigiD for organizations. Instead of relying on the BSN, it uses the KvK-registration (Chamber of Commerce).[51] eHerkenning supports five levels of security. Though it only facilitates services between organizations, eHerkenning identities are personal. Like DigiD, in future plans eHerkenning will be placed under the Idensys umbrella if its pilots are successful.
Why it is not really DigiD for organizations, is that Logius only sustains the standard while different firms execute this standard. It is a paid service.

Idensys
Idensys is the new method for online identification for citizens/consumers. It claims to enable people to prove with more certainty that they are who they say they are. It is a public-private partnership, meant to log in to

governmental bodies, healthcare organizations and firms. It has certain principles: relieving organizations that provide services of identification bureaucracy, freedom of choice and ease of use, protection of privacy, stimulation of the market, in a technology agnostic and future-proof way. Idensys is a standard, with as little technology choices as possible. It provides multiple authentication methods, from SMS, to app, to selfies even. It will also incorporate DigiD. Future synchronization with European standards is an important aspect.[52]

iDIN
Lastly, iDIN is an authentication method offered by several Dutch banks (ABN Amro, ING, Rabobank and de Volksbank). It is sustained by the Betaalvereniging Nederland. Logging in is similar to regular online banking and iDEAL payments. iDIN has two different security levels.[53]
Banks have an excellent position to offer such a log-in method with controlled identification, since they are compelled by law to identify their customers. They have already invested in secure log-in methods to let their customers do online banking. A disadvantage of iDIN is the missing link with the BSN. This makes implementation complex with organizations who are now using DigiD.

International
Next to efforts by the Dutch government, the European Union is also trying to create a form of harmonization in electronic identification. An eID framework must spark standards of identification. If methods are compliant with this standard, they should by 2018 be usable in all member states.[54] Historically, a common legal basis was lacking preventing Member States to recognize each other's eIDs. The eIDAS Regulation provides a solution to this interoperability issue, enabling citizens and business to benefit from the digital single market. With their standards the European Commission aims to secure access to online services and to carry out electronic transactions in a safer way. This is an important enabler of data protection and the prevention of online fraud, especially in matters such as eGovernment.[54][55]

Several other countries have devised other solutions to identification. Take for example Estonia, which already has a very advanced digital identity management system, based on blockchain technology, which includes healthcare records. [56]. They are generally perceived as a forerunner of digitalization of governmental services. A smartcard gives Estonians access to more than 1,000 of such services. Their e-residency solution is available to anyone in the world, a sort of global DigiD. The e-residency solution is coupled via blockchain technology to different kinds of organizations and services. Also the electronic health records are coupled with a blockchain. The government serves as an incubator and launching customer for the start-up that has developed the blockchain solution.
In another part of the world, Dubai is taking on ambitious plans to put all of its governmental documents on the blockchain by 2020.[57]

Criticism
The fact that the proposed new log-in methods, iDIN and Idensys, are not completely centralized, is a good aspect according to the principles of self-sovereignty. The multiple methods of identification are part of a federated configuration. It is not a decentral application: control and ownership of identities is still not in the hands of the individual. There is, however, some freedom of choice and ease of use. This freedom of choice has made online retail organizations anxious about scattering of methods and lack of integration.[58] Criticism posed by the Algemene Rekenkamer was that the governance structure seems to be complicated and supervision or integral use cases are not yet there. The proposed methods do not seem to be a cure-all for the difficulties of digital identity.[59]

Noteworthy is the fact that a self-sovereign identity solution, which provides an identity infrastructure, will in itself not be a replacement for these authentication methods. It still needs authentication mechanisms to be able to identify persons, to make the translation from physical to digital. As such, a self-sovereign identity framework will only be a replacement for systems like Idensys, if a complementary service is embedded in the solution, which makes use of (an) authentication method(s).

5.5 Conclusion
In this chapter the main concepts relating to digital identity were explained. Also, the boundaries and historical developments of digital identity have been indicated. These illustrated the issues of digital identity today. With the initiatives of Dutch and European organizations in mind, a context for the applicability of blockchain technology in this field has been created.

6 Blockchain technology

Robust digital identity can only be set up with the help of sophisticated technological systems. The protocols that are used to establish authentication and personal records are the main target of innovation here. So let us take a look at blockchain technology thoroughly.

6.1 Concepts

Definition

Just as self-sovereign identity does not have a clear unique definition, the concept blockchain is not clearly demarcated. Some might define it simply as Distributed Ledger Technology (DLT) where data is added in blocks.[60] The definition used in this report will be:
'Blockchain is a distributed ledger of immutable digital records saved in a chain of units called blocks. This distributed ledger is a database which is a consensus of replicated, shared, and synchronized data spread over multiple sites, countries, and institutions. A new block contains cryptographically hashed data and is built upon the previous block in the chain, ensuring that the data in the blockchain cannot be compromised.'[61]

Concerning terminology, blockchain technology is often abbreviated to just blockchain, while blockchain technology and the blockchain ledger, the actual blockchain, are two different things. The blockchain data structure is an ordered, back-linked list of blocks of transactions. The blockchain can be stored as a flat file, or in a simple database.[62]

Network

Blockchain technology is thus based around a distributed database. This database is maintained and updated by a network of so-called nodes. This network is usually one of peers. In a peer-to-peer (P2P) network everyone acts as a server as well as a client, with equal rights and obligations for everyone. There is no server, no central service and no hierarchy in the network.[63] The original blockchain, the Bitcoin blockchain, is arranged in this way, but many other blockchain variants are not truly P2P anymore.

Although nodes in the network are equal in principal, they can take on different roles. We define four main functions of nodes. All nodes propagate and validate transactions, and all nodes discover and maintain connections with other nodes in the P2P network. This is called the network function. Some nodes also maintain a full copy of the blockchain ledger. A third function is the mining function: mining nodes participate in validating and computing blocks of the chain. The wallet function of a node is the user interface which gathers addresses belonging to one user.[62]

Nodes in the network are identified with cryptographic addresses. Usually a private key is the true identifier, with one or more derived public keys. These addresses are unique. They are used to sign and target/address messages.

Transactions

The blockchain has the purpose of facilitating transactions inside the network. These transactions have an input and an output, and they are signed and 'opened' using private keys. To participate in transactions, one needs a wallet. Actual coins do not exist, only transactions and their linked history.[64] These transactions are what is stored in the ledger that is immutable.

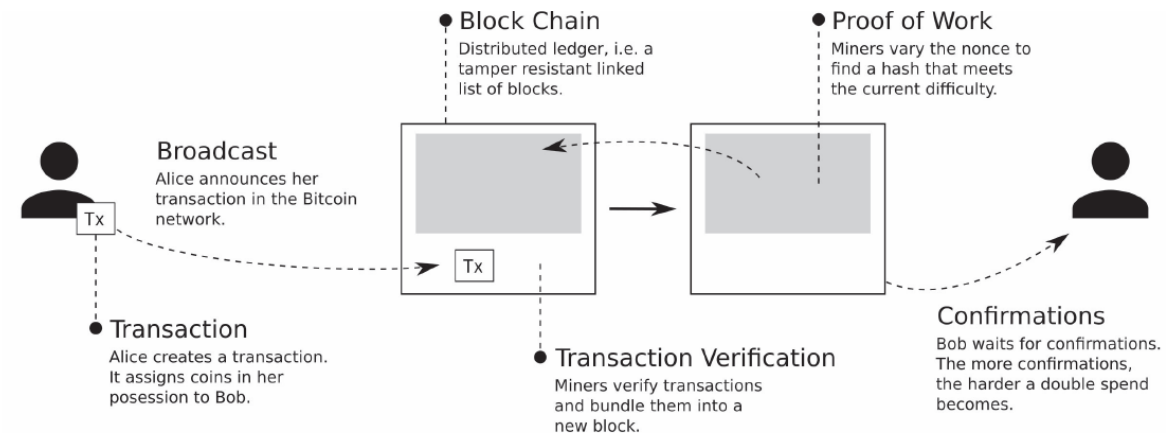

Figure 4: Schematic representation of Bitcoin transaction confirmation.

Byzantine Fault Tolerance

Since there is no central authority to decide which transactions are valid and are stored in the ledger, there should be a mechanism by which the peers can reach consensus. The trust that cannot be invested in a central authority, should be invested in a consensus protocol by which all nodes operate. The consensus protocol must also be able to handle dysfunctional or malicious nodes in the network. A consensus mechanism is called Byzantine Fault Tolerant if it tolerates the class of failures that are known as Byzantine faults.

In the Byzantine Generals Problem[67] several army factions surround a hostile city they hope to sack. Each faction is led by a general. Only a simultaneous attack ensures victory. The factions are dispersed so generals must send messages between them to relay the attack time. However, some generals are traitors and will relay the wrong attack time. It is not known which generals are loyal and which are not. How can the generals ensure a coordinated attack?

Applying this to a blockchain setting, we see that inputs (messages) to the ledger (the agreed upon time of attack) must all be trusted. These networks usually have millions of members (the generals). They are dispersed and there is no centralized governance. So how can you trust the other members and ensure that the ledger holds correct information?

Consensus

Several consensus mechanisms are in use with existing blockchain implementations, who in some way or other deal with Byzantine faults:

Proof-of-Work (PoW)

Designated nodes, known as miners in Bitcoin, work to solve a mathematical/cryptographic hash puzzle. This probabilistic task is straightforward but computationally very expensive. The computer that finds the answer first may add a new block of transactions to the blockchain. Finding the answer is a proof that he has done the necessary work. The winning miner is rewarded with some newly minted bitcoins, for example, to compensate for his invested computing resources and energy. In this way, with Bitcoin a new block is added to the blockchain about every 10 minutes.

Proof-of-Stake (PoS)

This is a category of public consensus algorithms that depend on a validator's economic stake in the network. With PoS a set of validators take turns proposing or voting on the next block to be added to the chain. The weight of each validator's vote depends on the size of a deposit he has made (his stake). These validators and their deposits are kept track of by the blockchain.

In the example of chain-based proof of stake, the algorithm then pseudo-randomly selects a validator node during a certain time slot (e.g. every 10 seconds) and assigns that validator the right to create a single new block, which points to a previous block (normally the one at the end of the previously longest chain).

Another possibility is that the algorithm randomly assigns to validators the right to propose blocks. These blocks are then agreed upon through a voting process of multiple rounds, where validators vote on a specific block each round. Here consensus on a block does not depend on the length or size of the chain after it.

Significant advantages of PoS, compared to PoW, include security, reduced risk of centralization, and energy efficiency.[65]

Proof-of-Authority (PoA)
This category of consensus algorithms is intended for permissioned or private blockchains. It is based on keeping a list of authorities, nodes that are explicitly allowed to create new blocks. A majority of authorities has to sign the chain off to make it part of the permanent record. In a consortium setting there is no disadvantage to PoA. It is more secure, less computationally intensive, and more performant than PoW. Authorities are not anonymous and can be held accountable off-chain.
Practical Byzantine Fault Tolerance (PBFT) is an example of this used by Hyperledger Fabric.[66]

These consensus mechanisms have an influence on several aspects of the blockchain:
- Throughput
- Scalability
- Finality
- Tamper-proof

The blockchain ledger
The actual ledger, the database, consists of a chain of blocks. Authorized nodes (possibly every node) can gather transactions that are valid and pool them together. According to the consensus mechanism they can add these transactions as a new block to the chain.
This block contains a header which comprises several pieces of metadata: the hash of the previous block, the block number, and the hash of the Merkle tree root of all the transactions.[64]

The intrinsic characteristics of hash functions make that blocks in the ledger cannot be altered without the alterations being noticed further in the chain. A slight modification to the input of a hash function dramatically changes its outcome. Thus, in order to spread a false transaction one has to recalculate all following blocks faster than the rest of the network does. This requires at least 51% of all computing power. That's why it is called the 51%-attack. The size of the Bitcoin network makes this nearly impossible to obtain. It is more cost-efficient to use these resources by mining honestly.
In this way, no individual or group of people is in control of what is recorded in the blockchain. Thus its decentralized trust is achieved.

When a block is added to the chain, it is propagated through the network, such that everyone can synchronize his or her copy of it.

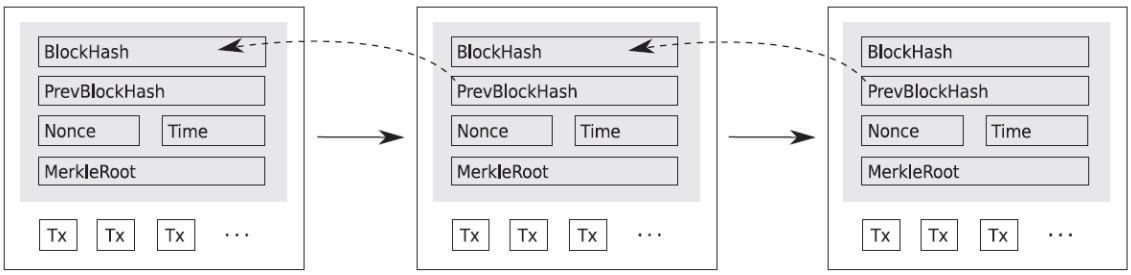

Figure 5: A simplified Bitcoin ledger.

Incentives
With Bitcoin, reaching consensus comes at a cost: large amounts of computing power and therefore energy are consumed to mine the new blocks. Miners should be given an incentive to operate. This incentive is created by adding transaction fees to every transactions and a mining reward. The one who solves the mathematical challenge first, can collect these fees and the mining reward.

Incentives don't have to be monetary: a way of incentivizing miners could also be to give the winner extra rights or access to certain data for example. In a healthcare context one can think of making health data available to research institutes who mine your transactions.

Smart contracts

Blockchain allows for sophisticated transaction flows, which can be arranged with the help of smart contracts. A smart contract is a piece of scripting language, which serves as a node in a blockchain network and gets executed when it is called for. The scripting language that is used to program (trans)actions is not the same for all blockchain platforms. The functionalities of the scripting language offer a design choice which very much determines the overall utility of the blockchain technology. The programming language of Bitcoin is rather basic, which limits its possibilities, but also makes it harder to abuse it for mischievous purposes. More powerful programming languages, which are Turing complete, make sure that complex logic and business rules can be implemented and executed automatically in a decentral, transparent way.

The smart contracts make sure that processes can be validated automatically. Thus, processes of different organisations can interact without reconciliation issues regarding data and transactions while maintaining privacy.

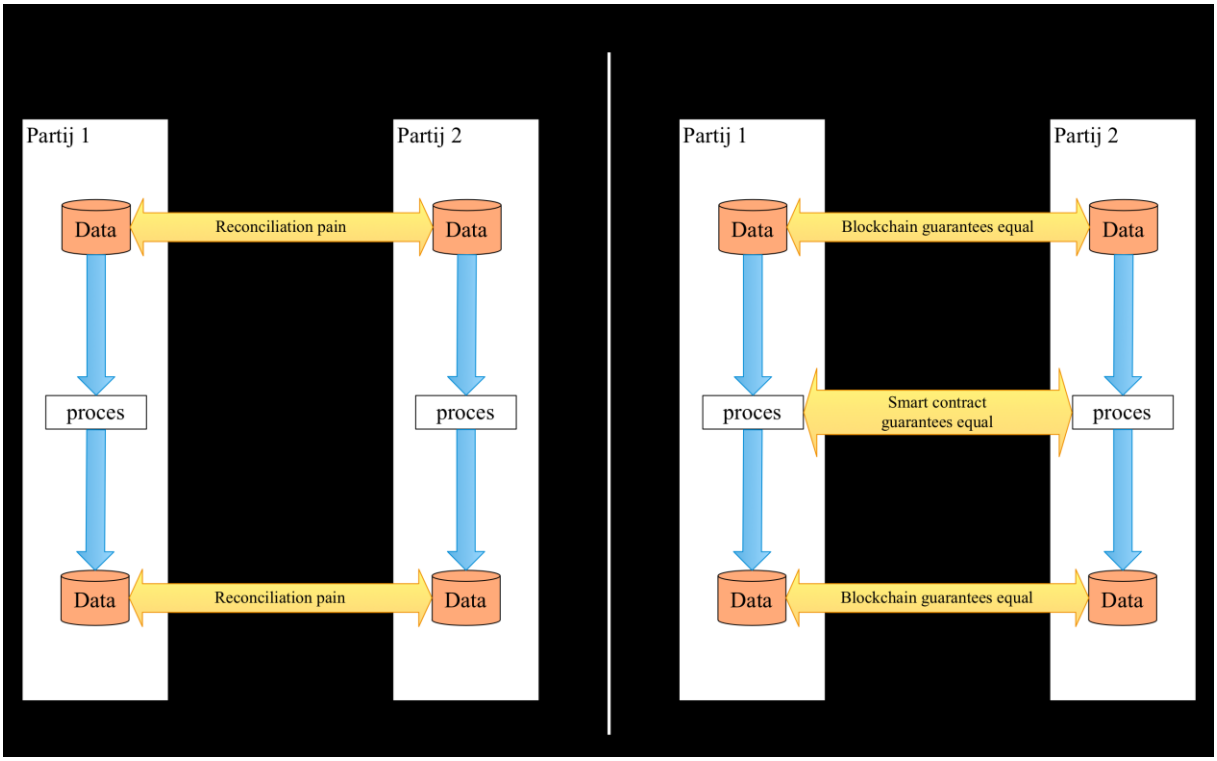

Figure 6: Smart contracts have no reconciliation issues.

Governance

Governance is a non-trivial issue with blockchain. Depending on the principals on which the blockchain platform is based, not only trust but also governance is decentralized. This can lead to fundamental discord between different users of the blockchain. An illustrative example of this is what happened with the DAO of Ethereum in 2016.[68]

Depending on what kind of blockchain is chosen, making use of blockchain means a complete overturn of existing trust models. Instead of trusting one centralized agent/party, users of the system now only trust the system and the protocols. They do not have to trust anyone in particular.

It is important to have a clear view of the governance requirements of your blockchain application before it gets operational. A dichotomy in two respects is distinguished. A blockchain can be public or private: a public blockchain can be used by anyone, while a private blockchain has restricted read or participation access. Also, permissioned and permissionless blockchains are distinguished. With permissionless blockchains anyone has the same writing permissions, while with permissioned blockchains additions are reserved for special nodes. The mentioned applications can be roughly classified like this: (Disclaimer: some platforms allow for different consensus mechanisms and configurations. As such, they are not really fixed at one point.)

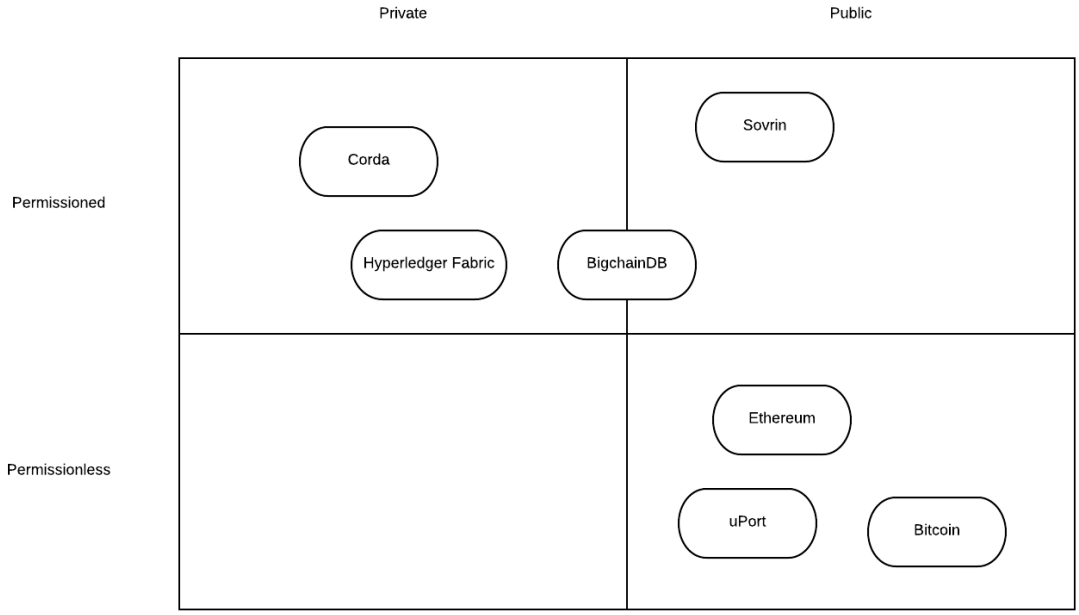

Figure 7: Blockchain platforms classification on the basis of openness and permissions.

6.2 Issues

Blockchain has been around for some years now, and it is still not widely adopted. This is mostly caused by technical immaturity and issues that have to be resolved first. The issues mentioned here concern the original blockchain implementation, Bitcoin. Several blockchain variants address one or more of these issues.

Storage

Storage requirements for the blockchain ledger at all the full nodes can be an issue with certain blockchains. In the purest situation everyone owns a copy of the complete blockchain. This already requires a relatively great amount of storage, while the user bases of the platforms can still rise exponentially when mainstream adoption arrives. Performance of the network does not scale up with the number of users. For example, at the time of writing the Bitcoin blockchain is 160 GB in size.[69]

Scalability & Performance

One of Bitcoin's greatest possible pitfalls is its scalability. The system is designed such that approximately every 10 minutes a mathematical puzzle is solved and one block is added to the chain. There is an upper limit to the amount of transactions in one block, which results in a theoretical maximum of 7 transactions per second. Compared to the 24,000 transactions of Visa per second, this is nothing.[70] Magnifying this maximum block size seems like one solution to this, but this would result in greater requirements on the computing power of the network. With the already expanding network this means that computing requirements will increase enormously. And even now already, mining is not really lucrative for miners without special mining equipment. [62]

Privacy

An identity with Bitcoin is based around a private key. The public key that derives from it can be regarded as one's pseudonym. Though Bitcoin was based on principles of anarchy and anonymity, these pseudonyms do not provide total anonymity per se. Transactions from or to the same address can be linked and analyzed. Thus the possibility of generating a new public key for every transaction is important to preserve one's anonymity in the network.

In other blockchain applications, the transparency of all the transactions is limited to a greater degree. When exchanging data, the content of the transaction is kept between the parties involved in the transaction and not the whole network. Several blockchain platforms like Corda and BigchainDB provide for this feature.[76][17]

6.3 History

Digital cash
The history of blockchain is mostly infused by a need to have secure digital cash. In the 1980s and 1990s possibilities for digital payment methods were investigated, modelled like credit- and cash-based systems. The idea of digital cash was first introduced in a paper by David Chaum[71], who in 1990 founded DigiCash, the world's first electronic cash company. His solution solved the problem of double spending: double spending of digital cash could be detected while preserving anonymity. His solution did, however, still rely on a central server; all transactions would halt if that server failed. Eventually DigiCash went bankrupt in 1998. It was hard to persuade banks and merchants to adopt the system. Because of this, and since it did not support user-to-user transactions, users were also not attracted. Credit card companies prevailed. [3]
In the meantime, prevention of spam attacks was being investigated with the help of cryptographic hashing puzzles, who can be seen as predecessors of Bitcoin's Proof-of-Work mechanism. New alternatives of digital cash like e-gold followed suit, but one problem remained urgent: security. The systems were used by criminals and raided by the US feds, and mainstream adoption was not feasible.

Bitcoin
In 2008 a new effort was introduced by Bitcoin. The mysterious Satoshi Nakamoto launched the blockchain on which it ran. In the early days it was still a niche product that served as a platform for early adopters. But over the course of a few years, people started to attach value to the coins and some started to see that the underlying technology of blockchain could be used in many more applications. This led to the general purpose blockchains of today, with much experimentation on the most diverse use cases.

6.4 Platforms
Having discussed the essential concepts and history of blockchain, we can now illustrate the current state-of-the-art of the technology. The blockchain world is very fast-paced and in flux. Hence there are numerous platforms and protocols which compete for wider acceptance. New altcoins, altchains and blockchain services pop up every day. Bigger companies and institutions start to latch onto the developments, which causes a greater momentum and focus. The open innovation environment that is harvested around blockchain leads companies to partner up, creating consortia with great capacities. In this paragraph some of the best known blockchain projects/platforms are summarized.

Bitcoin
Bitcoin is still the most widely used blockchain to-date. Its user base is growing steadily and the value of its currency has skyrocketed over the last year.[69] Other aspects of Bitcoin have been used as an example in previous subsections.

Ethereum
Ethereum is a general purpose blockchain. It does, however, still have a lot in common with Bitcoin: Proof-of-Work consensus to add blocks and a native currency, ether, serving for transaction fees and mining rewards. But the scripting language is different. Ethereum makes use of Solidity, which is a Turing complete language, although without having support of formal verification, providing for multiple possible applications to be designed on top of it. The so-called smart contracts that can be programmed, are nodes in the network that respond in a pre-determined way when ether is transacted to them. They are also preparing an upgrade with a Proof-of-Stake consensus algorithm named Casper.[73]
Ethereum is operational since 2014, in 2017 it began with the development of its private version for firms: Ethereum Enterprise.[74]

Hyperledger
Hyperledger is a project, a consortium, that was established by the Linux Foundation. As its output it has different blockchain platforms, like Fabric, Indy and Burrow. Hyperledger is aimed to be a platform construction set with which different companies (participants to the consortium) can tackle different problems with varied applications. For this, it incorporates pluggable features. These pluggable features are for example different consensus algorithms.
Hyperledger is not a public project, participation is not free.[75]

Corda
Corda spawned from a cooperation between different financial organizzations which sought to store and manage their financial agreements and records without error, where anybody can transact without friction.
The cooperation aspires to define a shared ledger fabric for financial services applications that can be deployed within existing legal frameworks and which relies on proven technologies. Its goals are engineering for the requirements of institutions, a focus on non-functional requirements and extensibility. In Corda there is no single central store of data. Each node maintains a separate database of facts known to him. No peer is aware of the ledger in its entirety. Corda makes use of contracts and states which ensure that objects have the same status.[76]
Corda has a demo running at the moment.[77]

BigchainDB
BigchainDB claims to be a solution with blockchain-characteristics with defining quality of being scalable. 1 million writes per second make for a much greater throughput than Bitcoin or Ethereum can achieve.
Rather than to scale up blockchain technology, BigchainDB starts with a normal distributed database and adds blockchain characteristics. It inherits from the database high throughput, high capacity, a full-featured NoSQL query language, efficient querying and permissioning.[17] Private, peer-to-peer communication between nodes is disallowed (except via built-in communication channel of the database), disabling malicious nodes to send different messages to different parts of the network.
Decentralized control is achieved via a DNS-like federation of nodes with voting permissions. The voting operates at a layer above the distributed database's built-in consensus.[17]

6.5 Identity applications
Identity applications that implement blockchain technology and the principles of self-sovereign identity have already been developed into products of differing maturity. In this section these will briefly be explained.

Sovrin
Sovrin is a Self-Sovereign Identity (SSI) framework devised by the Sovrin Foundation (whose sole purpose is to govern the ledger and its surrounding ecosystem). Sovrin aims to be a new public utility, a way to store identifiers, keys, pointers and proofs without relying on centralized authorities. Thus, an individual can build up a sequence of identity transactions which can reliably prove their identity.
Sovrin provides a public permissioned ledger which can deliver public access as well as governance by trusted parties. Sovrin puts people, not the organizations, in charge of decisions about their own privacy and disclosure. Sovrin uses open-source Distributed Ledger Technology (DLT). This ledger is a type of cryptographic database that is provided cooperatively by a global pool of nodes instead of a single enormous database with a central administrator. While access is public, meaning that everyone can use Sovrin, identity data is private and can only be shared under consent of the owner.[47]

No mining is required so it does not need immense computing power and can operate with a much higher throughput than permissionless blockchains. It also avoids subversion by any actor who can gain a majority of the mining resources. But it is still publicly available.[48]

Self-Sovereign Identity Framework
This is a framework for SSI, set up by a coalition of Dutch organisations. Like Sovrin, it aims to provide for a utility on which persons can manage and control their own identities, while dealing in a trustful and secure way with others.
The framework is not operational yet and is blockchain agnostic for now. The ultimate goal is for it to become a public permissionless blockchain, but it is imaginable that prototypes require permissions.
The mission of the consortium is to provide both the specifications, set of rules and a working prototype of a technical infrastructure for the exchange of identity-related data between different parties. This framework should allow for as much privacy as users like, and is 'self-sovereign', meaning that users control the identity-related data that is theirs.

Its core features are claim-based verification methods. An owner of an SSIF identity can give out claims about himself, these claims can then be attested to by trusted attesters and verified by relying parties. These verifications are immutably stored so that the individual has a public record he can rely on.

uPort

uPort is a secure, easy-to-use system for self-sovereign identity, built on Ethereum. It has three main components: smart contracts, developer libraries and a mobile app.
It consists of a public permissionless ledger, as opposed to Sovrin. But it also makes use of attestations.
A person can create an identity by means of a mobile app which holds his private keys and a smart contract that acts as his proxy. This Proxy is a smart contract that can interact with other smart contracts on the blockchain on behalf of the person. [49]

When a user wants to interact with a particular application smart contract, it sends a transaction through the Proxy contract, via a Controller contract (which contains the main access control logic). The Proxy contract then forwards this transaction to the application contract. Thus the application sees the Proxy as the interacting entity, creating a layer of indirection. The purpose of this Proxy contract as identifier is that it allows the user to replace their private key while maintaining a persistent identifier. If the user's public key was the identifier, users would lose control over their identifier if they were to lose the device which holds their private key.
In case of device loss, the Controller contract maintains a list of recovery delegates that can help the uPort user recover their identity.[49]

6.6 Blockchain innovation

Blockchain is a high-tech possibly disrupting technology. Its applications are inherently shared between different organizations with different kinds of missions, targets and incentives. Setting up internal closed innovation projects will most likely lead to failed innovations as the resulting product must be adopted by multiple players who have not been committed to the development process. Therefore, an open innovation model is most used. This is mostly expressed in consortia or open-source development. (See for example the Hyperledger and Corda consortia). Blockchain is brand new and it was not until recently that firms and big companies have started experimenting with it. This means that it will require some time before actual implementations will be market tested. We are now in the demo and prototyping phase.

Also important to consider is the type of innovation that blockchain will pose. For this there are several perspectives. Blockchain as a technology will not so much be a direct replacement of an existing technology. Instead, it provides an infrastructure on which several applications and services can be built. These applications can then be assessed and compared against comparable incumbent applications. For this we recognize three layers: infrastructure, services and applications.

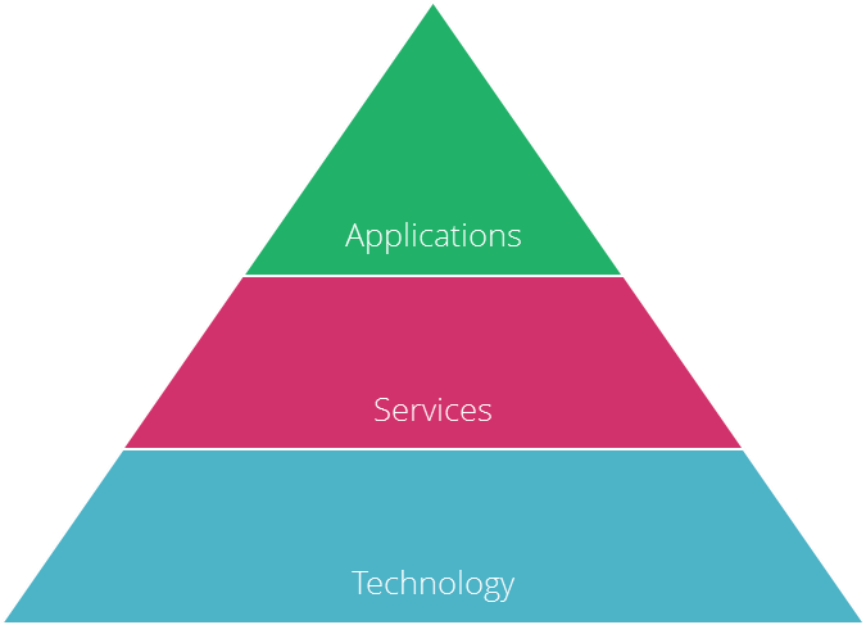

Figure 8: Blockchain layers model.

The technology/infrastructure layer deals with the basic protocols that the blockchain platform will have and how these interact. How is the blockchain constructed and how does it function? How is it governed? Examples are Hyperledger Fabric, and Bitcoin.
The services layer comprises the use of the technology for a specific purpose. Examples can be an identity infrastructure for self-sovereign identities built on top of an existing blockchain.
The applications layer consists of specific applications of these services. An identity infrastructure can for example facilitate a registration procedure at a hospital, or an application for the settling of healthcare claims.

Use cases
Fields of application for blockchain technology are recognized as the financial sector, logistics, healthcare, the energy sector and the Internet of Things. Especially in fields where trusted third parties make processes less time- or cost-efficient. International payments, micro-financing, blind voting, smart grids, container logistics, automatic billing are some examples. Relevant exploratory research can be found with [78][79][80].

Government
Blockchain can also prove beneficial in enhancing the Generieke Data Infrastructuur (GDI)[81] that the Rijksoverheid already has begun (a set of standards for data infrastructure). As activities of governments are for a great part providing central administrations in which some level of trust is invested. Blockchain seems particularly suitable to make this administrating function more efficient and less costly, by making it decentralized.[101]

6.7 Conclusion
In this chapter the principles of blockchain technology were explained. Together with a historical account of the need it fulfills and the hurdles it has taken, the state-of-the-art applications give an indication on where the field is heading.

7 Healthcare identity issues

The application of blockchain and self-sovereign identity can thus be executed inside a very broad scope. Looking at the applicability in the domain demarcated by the research goals and questions, it needs to be placed in a certain context. Therefore, in this chapter the Dutch healthcare system and the possible issues with managing digital identities will be put into relevant frameworks.

7.1 Dutch healthcare system

System overview
The current Dutch healthcare system was established in 2006 with the introduction of the Zorgverzekeringswet. Leaving institutions aside for the moment, there are three main parties in the healthcare system: healthcare providers, health insurance companies, and patients. These three parties perform different roles, and their tasks and requirements are meant to balance the system in an effective and cost-efficient way.
The role of health insurers is to buy care for its clients, the citizens/patients, in an aggregated manner. The role of providers is to provide the care. The system is depicted in the following graph:

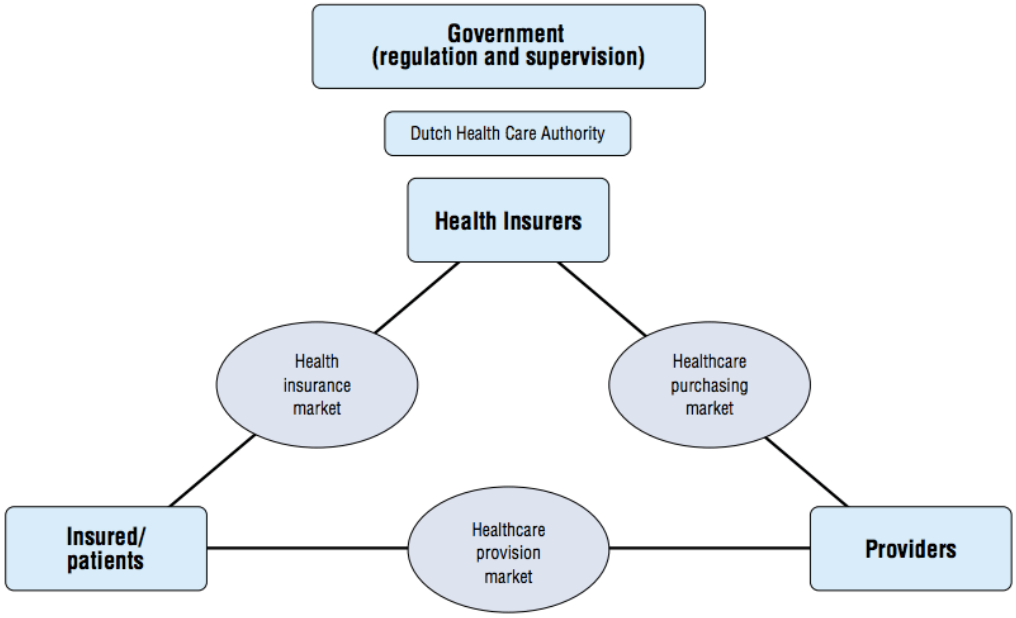

Figure 9: Dutch healthcare markets.

This model was adopted to restrain the fast rising of the costs of health care which are mostly caused by demographic change ('vergrijzing') and the increase in chronical illness cases on the one hand, and the increasingly expensive medical equipment and treatment (methods) on the other hand.

Insurers have to offer a universal package for everyone over the age of 18 years, regardless of age or state of health – it's not allowed to refuse an application or impose special conditions. This is called the basic insurance. In contrast to many other European systems, the Dutch government is responsible for the accessibility and quality of the healthcare system in the Netherlands, but not in charge of its management.[82]
While still being a public utility, healthcare has become more of a market-driven sector. There is freedom of choice for the consumers (they can choose which health insurer), in order to stimulate competition and lower pricing of care in general, while maintaining its quality.[83]

Oral care/dental care
Oral care is the subfield of healthcare which deals with the care provided by dentists, oral hygienists and dental surgeons. It takes up a special place in the constellation: it is a mostly isolated field, where patients mostly go for preventive care and screening, while not the most privacy-sensitive data is dealt with. This makes oral care

an appropriate field for bottom-up introduction of blockchain technology in healthcare: small experiments can later be extrapolated to other fields in healthcare.

Oral care for minors is in principle included in the basic insurance. For adults only some treatments are included in the basic insurance. However, all insurance companies offer some kind of additional dental insurance.
Prices for oral care are not handed down to the market. This has been experimented with, but with little success.[84]. Because of this the margins for dentists are very small and they often choose not to contract health insurance companies. Dentists usually don't have contracts with health insurance companies about the care they provide. Rather, a certain percentage of the contracts that they commit to are mere regulations on modes of payment to enhance the ease of use for the patients.[85]

Rabobank has investigated trends in the dental care sector. They perceive that the demand for dental care is slightly increasing while the amount of dentists is decreasing.
Dental chains and group practices are becoming increasingly popular. These are especially suitable for part-time dentists and allow for more cost-efficiency.[86]
Demand for complex and cosmetic dental treatment will increase because of the greater amount of old people, and also because orthodontic treatments are becoming more common for adults.

Besides these characteristics, oral care is very much alike other fields of healthcare, with the same way of billing, and the same configuration between executing, paying and supervising actors.

Stakeholder analysis
A mapping of the stakeholders in this field is presented in this section. The system of innovation is one that crosses sectoral boundaries, so also actors that play a part in the self-sovereign identity developments are included with the healthcare organizations.
The patient is put in a central position. A self-sovereign identity solution will have the patient as its end user and thus as the person in control. Links that are shown in the diagram depict relations between actors in processes in which the patient plays a direct or indirect active role. For example, a patient is involved in the claims process which explains the four-cornered cycle (patient-healthcare provider-VECOZO-health insurance company). On the other hand, patients are not involved in the process of 'buying' healthcare from providers, so there is no link between healthcare providers and health insurance companies in this diagram.

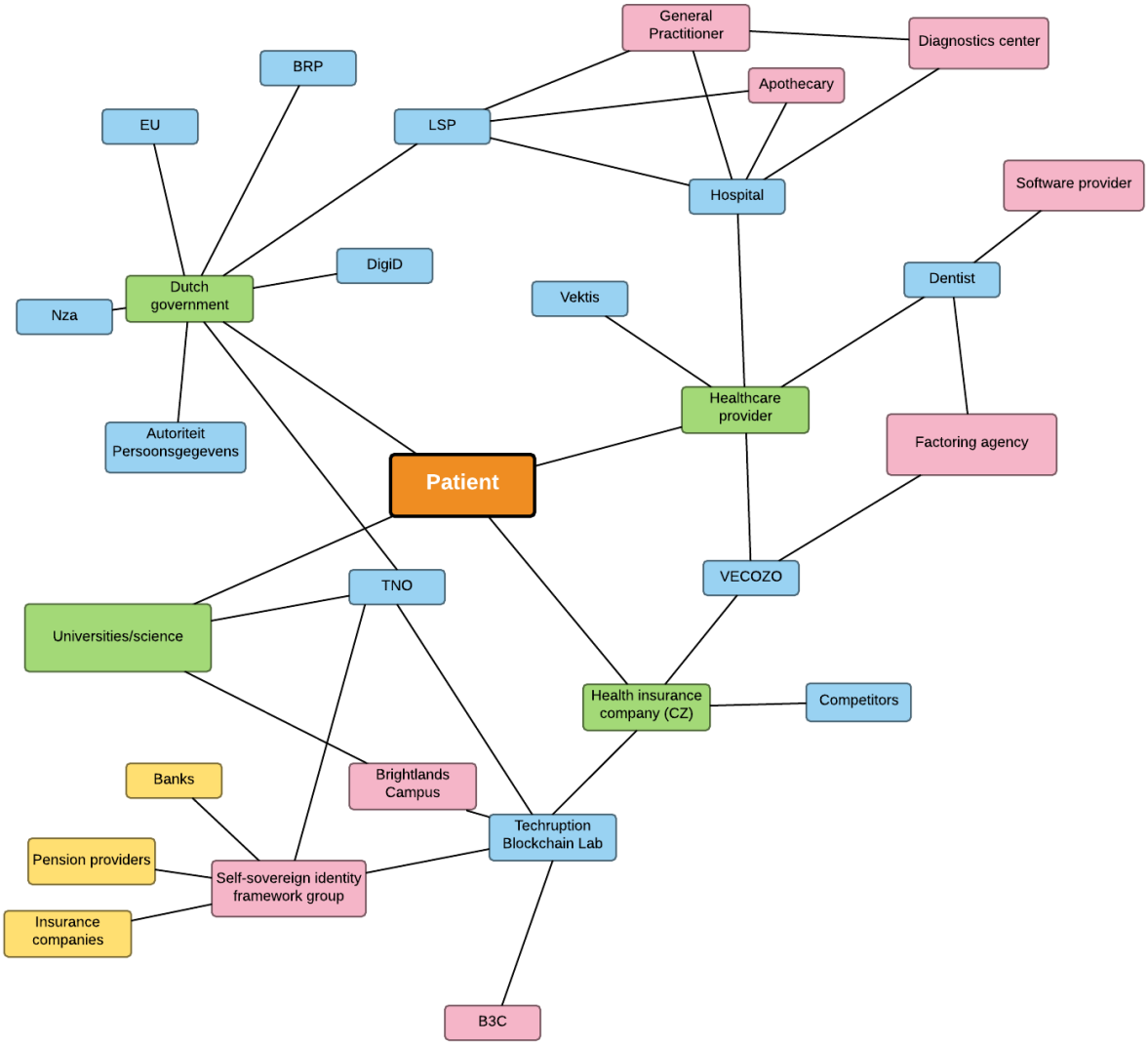

Figure 10: Stakeholders in Dutch dental care and self-sovereign identity

7.2 Incentives of the different stakeholders

As exemplified in the history of electronic cash systems, innovations should bring added value to all actors which are involved. Else they will not succeed. When we are looking at re-inventing the system of trust and identification, especially using a blockchain solution, we need incentives to cooperate, or at least to participate, for every stakeholder. We again look at the three main stakeholder groups.

Patients have two driving forces concerning health care: they want to get good quality healthcare for as low a price as possible. Current trends are also that people want to avoid risks and they want to be in control themselves.

Healthcare providers have the incentive to be able to perform their profession properly. Other incentives and requirements have been examined during the interviews (see chapter 8).

Thirdly, health insurance companies are an important player in the healthcare buying market and health insurance markets. They have to outcompete the other insurers by buying qualitative healthcare at good prices. In order to ensure that only legitimate and efficient care is provided for and thus reimbursed, health insurance companies have the legal obligation to check claims.

Patients

Patient requirements for healthcare are further elaborated upon in this subsection. Patient demands and requirements are more important than ever. The commonly acknowledged and continual trend of patient centered care shows no signs of abating.[87] These trends and patients' requirements are expressed in the

following framework the Dutch patients' federations have established in 2014.[88] It consists of criteria for the quality of care, subdivided into ten main areas of interest:
1 Control over care
2 Effective care
3 Accessible care
4 Continuity of care
5 Information, counselling and education
6 Emotional support, empathy and respect
7 Patient-oriented environment
8 Safe care
9 Quality of care transparent
10 Costs transparent

The problems that are recognized by patients in oral care are especially the future affordability of oral care. People have questions whether desired treatments or interventions will not become too expensive. Furthermore, people express a need for clear openness and access to costs, be it prior to or after treatment. Also clarity about which treatments are reimbursed fully, not or for what part is pressingly desired and apparently oftentimes not for everyone clearly insightful. [88]

Ten goals pertaining to the ten aforementioned fields of interest are:

1. The patient can make, if possible and desired, his own choices regarding treatment and care. The healthcare provider leaves him enough space to have as much own control as possible.
2. The patient is offered the treatments and counselling that are most effective.
3. The care for the patient is available in time, easily accessible and affordable.
4. The patient knows who is responsible for his care. The patient experiences seamless transitions between healthcare institutions, between departments and between healthcare providers.
5. The patient experiences understandable information, counselling and education, that is based on his preferences and capabilities.
6. The patient has a sense of being listened to and understood and he gets support on a psychosocial level where possible.
7. The patient experiences an appropriate and comfortable (treatment)environment.
8. The patient experiences a safe (treatment)environment.
9. Patients and their nearest and dearest have insight on the (organization of the) healthcare provider and the results of the care provided.
10. Patients and their nearest and dearest have insight on the costs of treatments/care and the reimbursements of these.

It should be noted that improved or strong identification is no requirement of patients. This indicates that authentication and identity are not urgent problems.

Health insurance companies
By looking at the mission statement of CZ and their goals, a closer look is granted at the incentives of health insurance companies.[89]

CZ's mission is 'Everything for better healthcare.' This is expressed in a vision of being a directing actor in healthcare, and a strategy that aims to add value to customers as well as to society.
The means they have formulated to achieve this can to a greater or lesser extent be linked to blockchain and self-sovereign identity innovation.
The most relevant ones, that will be used further on in this report, are:

- Personal service delivery
- Flawless administration
- Health innovation
- Patient empowerment
- Deployment of CZ data and knowledge for better healthcare.

Most urgent needs that were identified during conversations with colleagues from CZ regarded timeliness of claims processing. Especially in oral care the speed of warrants does not meet the Key Performance Indicators

(KPIs). This is, however, mostly due to the workload on medical advisors in assessing treatment plans. The added value of a blockchain solution in this is debatable.
These conversations were mostly aimed at getting insight in current processes and their deficiencies, so new added services were not discussed.

7.3 Relevant trends

Assessing future demands is just as important as knowing current requirements when you want to do innovation. Therefore, relevant trends are included in the system of innovation.

Personalized healthcare and patient-controlled data
New technology brings new possibilities. With the advent of big data and data analytics a much more personal way of treating patients is possible: one size fits all is nog longer seen as the best way to manage illness and care.
Wearable technology will enable patients to better monitor their own health and the easier access to data and information will also change the relationship between patients, providers and insurers. This pervasive health monitoring can help toward preventative, predictive, personalized, and participatory medicine. And thus play a key role in reaching sustainable healthcare.[92]

Alongside of this, there is a patient demand for patient-driven health information.[90] To seek diagnosis or better care, many patients are taking steps outside traditional doctor-patient relationships. But such patients have found no easy way to get copies of their electronic health records (EHRs).

Closely related to patient-centered care is the notion of personalized care. A more tailored approach is possible as more data about a patient become available.
The Precision Medicine Initiative of the U.S. government is a good example of how extensive data, including environmental, lifestyle and biological factors, can be used in research to improve health and make treatment less uniform but adapted to more precise needs.[91]

Cybercrime and healthcare
Cybercrime is becoming an increasingly common threat to society in general. The worth of personal data cannot be underestimated. In the United States on the dark web personal information is more valuable than credit card details and incidents of data theft are becoming more frequent.[93]
In spite of this, patient misidentification may not necessarily involve criminal activity. Often medical identity issues arise due to the inadequacy of name and birthday as current identifiers. Even if the identity of a patient is verified, there is a significant chance that other patients in that system share the same name or birthday, and sometimes both.[93]

Be that as it may, especially healthcare organizations are not properly armed against cyber-attacks.[94] Health providers are mostly preoccupied with their core business, providing health. And they provide a lucrative target. Healthcare service providers have huge database that serve as a repository of customer information that's more extensive than any other industry or organization: the type that, when stolen, cannot be easily replaced.[94] In the interviews with oral care providers it was assessed if they recognize the threats they are faced with.

7.4 Current identification process

The current mode of identifying persons in the care process will be expounded in this section. Exchange of personal data in the identification process is visualized below, which has the purpose of identifying the most important data sources for patient records and the registration process:

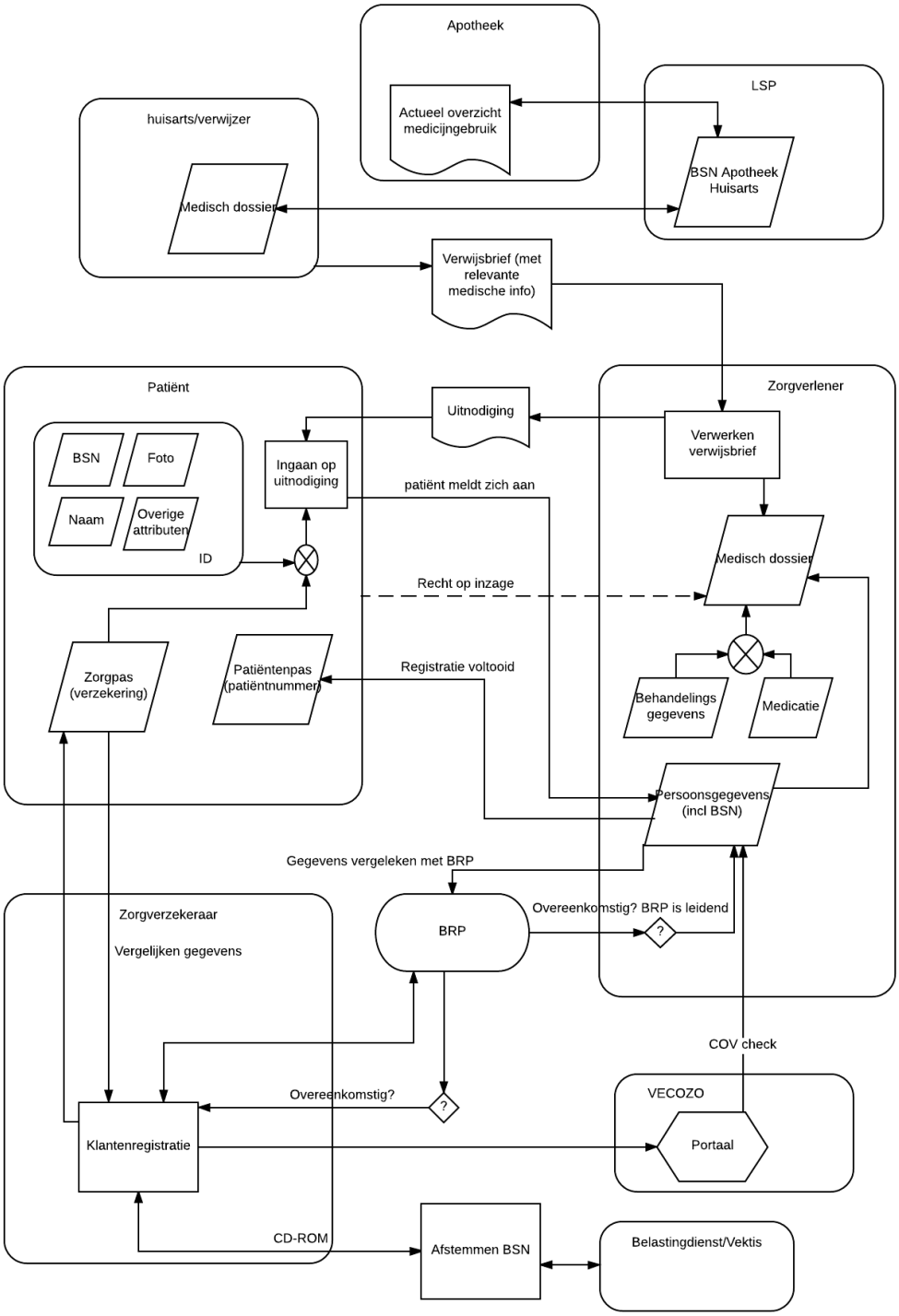

Figure 11: Identification and personal data management in dental care.

This process was verified and modified on the basis of findings during interviews with the healthcare providers. This process introduces some concepts and parties that need explanation.

LSP

Most notably, the 'Landelijk Schakelpunt' (LSP) which serves as a national electronic health record ('landelijk Elektronisch Patiëntendossier') for general practitioners and apothecaries. The original intention of creating such a record has not succeeded, since it did not make it through parliament.[95] The situation now is that general practitioners and apothecaries can individually decide if they want to ask patients individually for

permission to store their data there. Oral care is excluded from this national record, presumably since the privacy risks of including them were not proportional to the added value of these added connections.

Via the LSP citizens can see who has exchanged information on their person, but they cannot see the actual information. In the end, the LSP still places the general practitioner in a central position instead of the individual whose information it is. Online access to your own medical files is still not possible, partially because the authentication strength of DigiD is too low. There is however access to see who has requested access to your records via VZVZ (Vereniging Zorgaanbieders Voor Zorgcommunicatie). Ultimately, visiting your general practitioner is necessary to get insight in what is in your files. This is a costly and time-consuming process and it does not accord with the demands posed by patient wishes and legislation around personal data.[96]

Data sources

Basisregistratie Personen (BRP)

Healthcare providers as well as health insurers operate in the so-called BSN-domein, which means they can complement a social security number retrieved from an identity document with personal and address data automatically. All interviewees said they update their data from this source regularly. Modules to do this are included in the software package dentists use.

VECOZO

The insurance data of patients is also updated daily by most providers. They are able to do this by functionality of VECOZO, a portal where the relevant data is stored. This check is called the Controle Op Verzekering (COV). This process is what was illustrated in an alternative self-sovereign way in chapter 5. The scale and throughput of the current system are not easily matched by a blockchain solution.

Identity documents

Identity documents are required at the first registration. Also the validity of the documents is checked. Some dentists also record the profile photos of patients. This check is enforced by law.

Recognition/oral

When profile photos are kept in personal files, these are checked when the patient reports for an appointment. Multiple dentists say that for identification one relies on information orally given by patients, like name or date of birth. These verification questions are the main identification method for follow-up appointments and communication over the phone. About half of the interviewees mentioned that patients get a patient ID: a bar code or a number.

Referral

When patients come to a dentist on referral, they are treated as a regular new patient. Referrals do, however, not occur often, unless the dentist has a specialty in a certain treatment.

Follow-up appointments

With follow-up appointments patients are mostly recognized by means of authentication factors that they know (name, date of birth). In a situation with many passers-by, like a hospital, this seems very unsafe.

7.5 Legislation

Laws and regulations are important institutions which have a strong influence on innovation processes, and as such also on the possible reconfiguration of the identification process. Now also the European Union is trying to protect its citizens in a digital age, by exerting its legislative power to limit the possibilities for citizens of losing data and identity. Also globalization requires new social phenomena to be arranged by law, so it is not more than logical that the EU is trying to perpetrate some standardization of privacy law across its nations.

Current legislation in the Netherlands is de Wet bescherming persoonsgegevens. This is maintained by the Autoriteit Persoonsgegevens. It will soon be superseded by the European GDPR regulation.[12]

Data Processor and Controller

Legally speaking, several roles can be taken on while dealing with data. The data controller is the person (or organization) who determines the purposes for which, and the way in which, personal data is processed. As opposed to that, a data processor is a person (or organization) who processes personal data on behalf of the data controller (excluding the data controller's own employees). This could also include storage of data, for example on a third party's server.

The GDPR will impose more responsibilities on data processors.

GDPR

The General Data Protection Regulation (Dutch translation: Algemene Verordening Gegevensgebruik (AVG)) which has been voted for by the European Commission in 2016 and which will be in effect as of May 25th 2018, is a regulation aimed to comply with the new trends within privacy and security. The GDPR was designed 'to harmonize data privacy laws across Europe, to protect and empower all EU citizens' data privacy and to reshape the way organizations across the region approach data privacy.'[97]

The law is also intended to alleviate administrative burdens for organizations by harmonizing legislation across Europe. It constitutes a simplification of the rules for companies in the Digital Single market, where for example e-commerce also is a part of. The regulations must also strengthen and unify data protection for all individuals within the European Union.

It addresses the export of personal data outside the EU. Without such address the whole effectiveness of the new restrictions would be annihilated, since data can be easily transferred across intercontinental channels.

Scope

GDPR has a stricter applicability than its preceding directive. It will apply to the processing of personal data by controllers and processors in the EU, even if the processing does not take place in the EU. Also if the processing of the personal data of data subjects in the EU is done by a controller or processor not established in the EU will fall under GDPR, if it relates to offering goods or services to EU citizens and the monitoring of behavior that takes place within the EU.

Penalties

Organizations violating GDPR can be fined up to 4% of their annual global turnover or 20 Million euros (whichever is greater). This is a maximum fine for the most serious infringements. There is a tiered approach to these penalties.

Consent

Consent management is also bound to change under GDPR. Companies will no longer be able to use long unreadable privacy statements full of legal jargon, as the request for consent must be given in an intelligible and easily accessible form, with the purpose of the data processing also stated clearly. Furthermore, consent must be as easy to withdraw as it was to give it.

Rights of data subjects

- Breach notification: data processors must notify their customers, the data controllers, if they become aware of a data breach within 72 hours.
- Right to Access: this is already part of Dutch legislation currently, but a customer will have access to all his data and the processing of which it is part, upon request.
- Right to be Forgotten: this entitles the data subject to have all his data removed by the data controller and to cease further processing of it (also by third parties).
- Data portability: this is new with GDPR, it is the right for a data subject to receive personal data concerning him, in a commonly used and machine readable format, and he has the right to move this data to another processor.

Privacy by Design

Privacy by Design calls for the inclusion of data protection from the onset of the designing of systems, instead of being a later addition to it. This also comprises the notion of data minimization, that is, only holding and processing the data that is absolutely necessary for the stated purposes, as well as limiting the access to the personal data to those who actually process it.

Data Protection Officer

A company processing a certain amount of personal data will be required to have a Data Protection Officer, who will supervise the processing and data management. This can consist of hiring one or working with one on a contract basis.

7.6 Innovation system

This legislation is a significant part of the innovation system or context that is relevant for this research. Taking a closer look at the totality of this system will give a better overview of the opportunities and limitations blockchain-based identity will be faced with.

Innovation has long been an elusive concept. To understand where a blockchain-based identity system can add value, one must look at the type of innovation that such a system can be. Other relevant elements of the innovation system are the life cycle of the technology and the system of innovation in which it is embedded.

In chapter 6 we saw that blockchain has the potential to be innovative on three levels: infrastructure, services and application. Looking at a self-sovereign identity framework there seem to be two possibilities: 1. It is a completely new blockchain protocol and thus a new infrastructure, 2. It is implemented on an existing blockchain infrastructure. Either way, it can serve as the playground for multiple services and applications (to be built on top of it).

Types of innovation

Innovations are often subdivided into categories. For now, we recognize four types: distinguished in terms of technology progress and market impact. We recognize incremental, disruptive, breakthrough and radical innovations.[99]

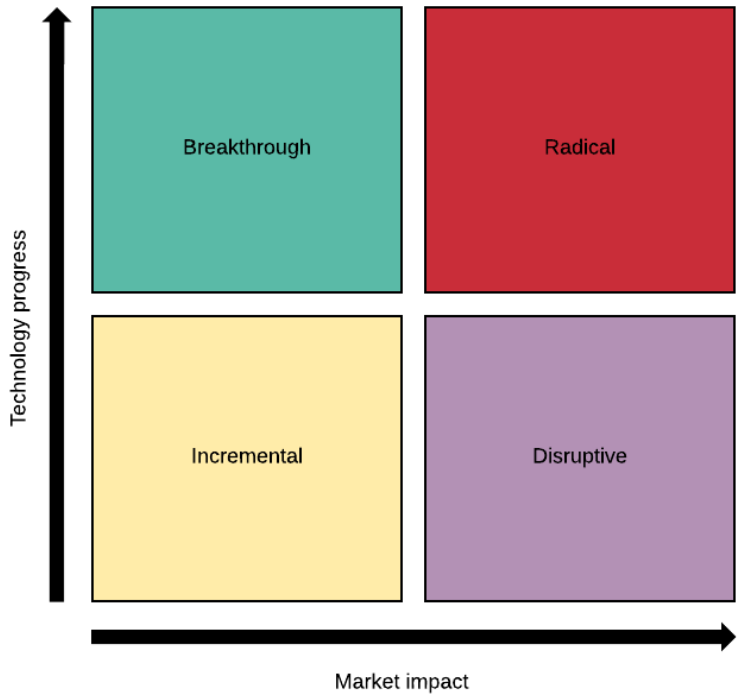

Figure 12: Four zones of innovation.

An incremental innovation is competence enhancing, building on existing competencies in organizations and will for example consist of a new model of an existing product, with the same features but some small changes. A disruptive innovation has a severe impact on the market that an organization can attain. A breakthrough innovation changes architectural components of a product or service. In this way, enormous progress can be achieved in efficiency or performance. Lastly, a radical innovation combines the best elements of a disruptor and a breakthrough: it provides new technical architecture and grants access to new markets.

Adoption of new technologies mostly takes quite some time, so these definitions make that only after some years after initial adoption one can assess in what zone an innovation belongs. Looking at blockchain technology, this promises to be a radical innovation. Different sectors have dived onto the subject to experiment with its possibilities. Organizations foresee different business models and system shifts. Looking at a more

technical level, IT-infrastructures can be rearranged by blockchain. The information flow can change and therefore also the relations between different actors.
The fact that blockchain has got this potential, does not mean that it will become widely adopted, since it might be that it will not bring an improvement towards the current processes. The real influence and scope of blockchain are thus still insecure.

Technology scope
Inside this model we should regard the scope: the technology can be blockchain in general, the self-sovereign identity framework, or an identity application in healthcare.
The identity application in healthcare is the most important point of focus, but this cannot be done without regarding the generic adoption of self-sovereign identity, e.g. by governments, banks and central institutions. This adoption will be essential for the success of such an application in the healthcare field.

The Dutch innovation system
The Dutch innovation system has been examined by the OECD in 2014.[oecd] The strengths that have arisen are:
- Overall good framework conditions for innovation, including solid institutions and a supportive business environment.
- Tight integration in the global economy. Multinationals with global reach, including in R&D and innovation.
- Specialisation in services.
- Highly developed infrastructure, including ICT.
- Strong technological capabilities and performance of Dutch firms.
- Innovative approaches, design, and delivery of innovation policy.

Opportunities:
- Further development of innovation in services.

Dutch healthcare entails the highest costs after Social Security and the Labour Market. Worldwide our hospital care has the second most high administrative costs after only the United States.[100] 20% of all costs go to administration. Likewise, different sectors and cooperation chains have high administrative burdens.
Society is becoming more and more interconnected, but complex and bureaucratic IT systems are not very adaptable and have an increasingly harder time delivering.[101]

The Dutch government is already taking steps in digitalization and necessary innovation. A 'digicommissaris' is appointed to enable fully digital contact with the government by the end of 2017. Also the Generieke Digitale Infratstructure (GDI), consisting of common standards, has been started. This framework can be used by governmental bodies, public organizations and sometimes also private organizations.
As several governmental functions seem suitable for a blockchain implementation, the blockchain can change the business model of the Dutch government and make governance an export product instead of a debit entry. This role is advocated by the Dutchchain consortium.[101]. Like software-as-a-service, where the customer pays on the basis of actual use and volume, the Dutch government could offer a digital infrastructure as a service to the international community: governance-as-a-service. If registrations like Kadaster, RDW or Chamber of Commerce can be innovated on the blockchain, other countries can immediately be using this ecosystem.

The Dutch government has a position of international trust[103], and is internationally very well connected.[102]. There is a good cooperation in the triangle: government, knowledge institutes, business. The Netherlands is traditionally very strong in public-private partnerships.
The Dutch ecosystem has other factors facilitating (blockchain) innovation:
1. Highly estimated research institutions, much highly educated talent;
2. An active start-up culture
3. A topsector approach
4. Companies with a strong international network.
5. A government that internationally has a trustworthy reputation, who can serve together with citizens and firms as a founding partner and launching customer. The government also has a strong international network.
6. Cooperative mentality. ('Polderen')
7. The components of the GDI that are already in place provide a head start.

8. Highly sophisticated network of banks who are active in blockchain developments.[101]

Blockchain
Also important is that the Dutch government is already active in stimulating blockchain pilots.[104]
And as already mentioned, the blockchain innovation system is fairly open. Of course there are companies who do research on their own, but the amount of consortia is also quite big and many developments are open-source. This means that boundaries are porous: sectoral boundaries are not applicable since consortia harvest organizations from different sectors and the relevance of national boundaries is also ambiguous.
On the one hand, much of the code material is published open source and available worldwide. And also global consortia like Hyperledger are influential. On the other hand, national consortia like the Dutch Blockchain Coalition, Techruption and Dutchchain advocate Dutch solutions to problems. This is more in line with a national system of innovation.

On the basis of the insights of the blockchain experts that were interviewed, their ideas will be held against the framework that the SI approach provides in the concluding chapters.

8 Discussion with healthcare providers

We are looking at solutions that cross organization boundaries and are relevant to all parties in the healthcare sector, including end-users, like healthcare providers and patients. To assess the perceptions that healthcare providers have, a group of users that is close to patients, and whose view might be conflicting with those of the commissioning organization, these interviews were held.
The following model describes the approach to the interviews:

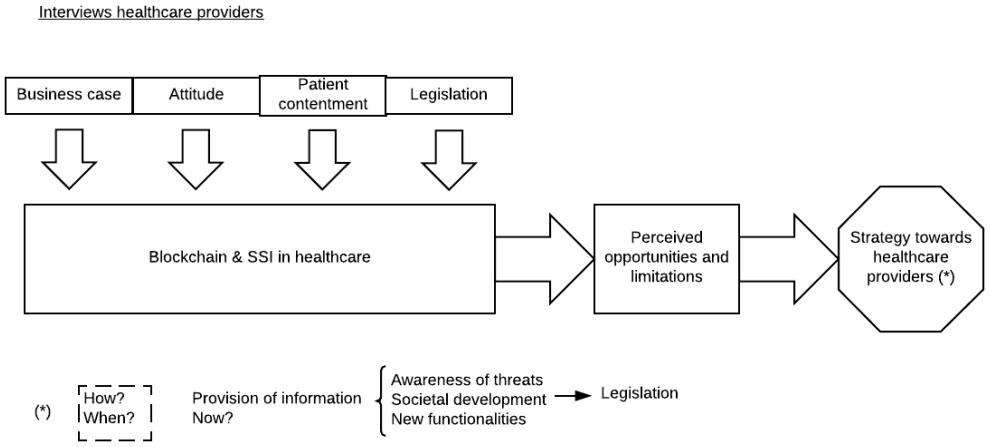

Figure 13: Approach to interviews with healthcare professionals.

These interviews were also held to enlighten the details of the identification and personal data usage in the current processes of dentists. Technical details about these are included in chapter 7.3, while remarkable findings are expanded upon here.

For privacy and readability purposes, the 8 interviewees are named Participant A, Participant B, …, Participant H. Results are grouped according to the thematic coding that was executed on the text of the interviews. These groupings are mostly in accordance with the aforementioned model for the interview.

Legislation
Familiarity:
To see whether healthcare providers are aware of the risks and the changes they are facing with respect to privacy and personal data regulation, they were asked about their familiarity with the GDPR.

Level	Meaning	Who?
1	Not aware	B, C
2	Only heard of it	A, F, G
3	Most important implications	D, H
4	Very familiar	E

Most healthcare providers are not fully aware of the impending changes in legislation. Important to note with this, is that dentists don't come into direct contact with this legislation, while an operational manager or a security officer does. That's why they were the ones having more knowledge of this new regulation. It also appears to be that participants from larger organizations, dental chains, are slightly better informed. Solo practices to a high degree trust software providers to take care of legal compliance. One of the dentists explained that most of their knowledge is based on the information they get from professional bodies. Those make guidelines and protocols for dealing with legislative changes.

Preparations:
The providers were also asked if they were taking any preparations to comply with this new regulation.

Level	Meaning	Who?
1	No preparations	C, G
2	Unknown to participant	A, B, F
3	Near compliant	D, E, H

All in all, the necessary preparations are mostly outsourced to other colleagues or organizations.
The dental chains make sure they are compliant. Information evenings and internal communication are in place to keep dentists up-to-date with relevant information. Participant H says his organization is busy with a new ICT-infrastructure to facilitate the growth of the chain, and at the same time he can make sure that it is compliant with GDPR.
Participant E's organization is one of the earliest, most well-prepared to comply with GDPR. As Data Protection Officer (DPO), he has written a policy statement for the whole organization. But he admits that there is still some vagueness as to details that the legislation brings with it. For example: when do you need a Data Protection Officer as an organization? Participant E says that in principle it's based on the amount of data you process. But you can choose if you want this DPO to be in-house, or on certain preconditions you can assign someone from a legal bureau as your DPO. In the past the Autoriteit Persoonsgegevens had direct supervision over organizations or the organizations could choose whether to install a DPO. Now it is compulsory for certain companies to have one.

Pros:
What do participants perceive as pros of the new GDPR legislation?

Argument	Who
Harmonization	D, E, F, H
People know their rights and obligations	E
Actualization of regulations according to societal developments	E
Stricter privacy	F
Data security	F
Transparency and control for patients	E, H

Good characteristics of the GDPR are its harmonization across Europe. This feature is especially mentioned by people for who this is relevant, e.g. dentists in big chains and the security officer who is closely linked to GDPR, and by the researcher who is involved in European research projects.
Participant H mentions that harmonization is a noble goal, and that a unified ICT infrastructure could be an advantage. But in the end, requirements for oral care are country-specific. In the Netherlands, care providers work with VECOZO-standards for example. Also the advent of chains is fairly new in Europe, which means that there are no standard packages for multiple countries.

Other arguments for the new regulation that are mentioned: stricter privacy, better data security, more transparency and control for patients, actualization of legislation in accordance with societal developments, and a better more universal understanding of people's rights and obligations. Only half of the participants mention advantages at all. But according to Participant G, GDPR at least doesn't worry regular dentists.

Cons:
What do participants perceive as cons of the new legislation?

Argument	Who
Conflicting laws	A
Administrative burden	D, E, F, H
Too strict for dental care	D
No urgency or need for priority	D
Makes research more difficult	F
Hard to comply with GDPR for healthcare organizations	F

Generally speaking, the healthcare providers regard the added administrative burden as their greatest concern. This burden can be felt in the workplace as well as in a research environment. At the same time, the dentists do not acknowledge that the data they deal with necessitates such strict regulation.

Participant E mentions that stricter privacy regulations like GDPR inevitably bring a greater administrative burden. You have more responsibilities when a patient asks you to remove his data, for example. Participants D

and H agree that the practical usefulness of these strict rules is questionable. They doubt if the benefits/added value outweigh the costs and administrative burden. Extra tasks for healthcare providers, especially dentists, are not desirable. Dentists want to work on their principal tasks. New legislation is good as long as it is executable. The added requirements for consent don't seem practical to them.
Participant F adds to this how GDPR can pose a limitation for research, especially when there is really no question of privacy. Using data is costly, mainly because of strict privacy rules. At the same time giving privacy a value, is not a bad thing.

Participant D argues that the legislation should be less stringent for oral care, since there is no question of very sensitive information. Data breaches in oral care are not desirable, but neither are they very harmful. He thinks in the enforcement of the law distinctions should be made between branches. He also argues that other, greater problems in oral care should be addressed first instead of the protection of personal data.

Important aspects of identity systems
Several factors essential to an identity system were mentioned: proper identification, scalability/performance, privacy, security, legal compliance, interoperability, transparency and ease of use.

Proper identification
The identification process should be able to properly identify persons that come to the dentist. This aspect is mentioned by different participants in slightly different tones. The lawful obligation to know a patient's identity is emphasized. One dentist stresses the importance of this in clinics with many passers-by. One of the more traditional dentists, Participant C, having his own practice, didn't acknowledge the importance of having a good-quality identity system altogether. His most important argument being the lack of privacy sensitive, important data. And also the lack of passers-by and the abundance of regular clients do not create a need for a good identification system with according measures.

Performance
Performance/scalability is also an important factor. There are organizations that have quite some 'patient movements' per year, so to ensure ease of use for the patients a scalable solution is necessary. Delays, or waiting times should be as short as possible, especially for patients. (Noteworthy in this respect is that current solutions perform quite well on this aspect, at least from a system operational point of view.) At the same time some dentists don't think they have that much personal data of patients. Participant D makes a clear case of what data should be instantly available. Informing patients whether they can apply for reimbursement and how much reimbursement, should be executable à la minute. Processing of claims also should be within a week. Thus it appears that there is a difference between practical needs and societal expectations of quality.

Scalability is especially relevant since chains of dental clinics are becoming increasingly prevalent. The IT-infrastructure is now mostly fashioned for individual practices while these chains have other requirements and should be able to process data centrally. Participant H says a connection between local and global infrastructure is not trivial.

Privacy
Healthcare providers do acknowledge the privacy aspect of the data they hold as an important one, though it be not on the dental care files per se. Relative to other sectors within healthcare, Participant D is not convinced of the importance of dental records. Participant H says that all information related to your dentals is privacy sensitive. (He gives examples of dental fillings and periodontitis.) Likewise, Participant F argues that when you are dealing with data on a personal level, instead of aggregated data, then privacy is important. Especially since giving data away (like people do on social media websites) is another matter than pulling data away by organizations.
Participant G sees the personal data and the medical anamnesis included in the records as the most privacy sensitive.

Security
Especially the security officer stresses the importance of security. He mentions the value of personal data and medical files to criminals. The awareness of these risks was not confirmed in the other interviews and the worth of dental data oftentimes marginalized.
Data breaches are however considered unwanted by Participant H, but no clear argument for this is given.

Legal compliance
Participant C had legal compliance as the only requirement. Two other participants also mentioned it as an important aspect.

Interoperability
Not all participants did see added value in a system with interoperability between different healthcare providers. While for other healthcare areas it can be, in oral care it is not really relevant. For example, in emergency situations, which do not often happen with oral care.
Others do mention the importance of linkages between data held by dentists and data held by the apothecary for example. Also Participant E mentions the relevance of the linkages and he mentions that we should have a closer look at the workings of LSP. He stresses the fact that GPs, apothecaries, diagnostic centers, hospitals and dentists all take care of a patient in a chain of care. Thus, it is important that their activities are linked together smoothly. Exporting data from one to the other, using standards for file sharing can really improve the healthcare pathways of patients.

Transparency
Participant F mentions that a balance should be found in the level of transparency. A transparent system is in the best interest of the society as a whole, but there are limitations: you don't want your neighbor to have access to your medical history, for example. Also, it really is a question of transparency for who? Increased transparency for patients might mean decreased transparency and freedom for healthcare providers. If a healthcare provider is constantly watched and supervised this might hamper his intrinsic motivation as a caregiver. Too strict control of health insurance companies could be bad for the intrinsic motivation of providers and thus decrease their proactive solutions.

Ease of use
Two dentists mentioned ease of use as an important requirement. Participant H said that ease of use is essential for a system to work in the clinics. Participant G preferred systems with a high level of automation.

Judgment of current situation
A generalized form of the current identification process and the resulting record management system is visualized in chapter 7.

General issues
Most issues with current IT systems were related to data exchange. The other issues are stated here:
- There is a mismatch between regulation and IT: Participant D mentions that as of recently 16- and 17-year-olds should get their own claims/bills, while they have a youth plan that runs until someone is 18. Therefore, IT systems are structured for a division between 18+ and 18- and the new rules pose an unnecessary administrative burden.
- Single Point of Failure: A central electronic health record is not desirable, because eventually it is very vulnerable.
- DigiD is not really secure, according to Participant E.
- The medical anamnesis requires a certain level of patient's responsibility: at the moment there is an individual responsibility for the patient to tell all his conditions. The providers must rely on this.

Data exchange
The participants were asked in what way they exchange data with other actors in the system.
In this respect, Participant F argues that communication about data, and the jargon, are not integrated into the healthcare sector, providers don't know the right terms. This makes talking about information processes and flows very difficult.

Channels

Data sent by (e-)mail	Who
Personal/appointments	B
Medical/dental	D
No data	
Data sent by physical mail	Who

Post	E, H
Data sent by encrypted channels	Who
Cryptshare (to municipalities)	B
Zorgmail	C

There is a remarkable inhomogeneity in the means of exchanging data with other parties. There is consensus that medical or dental data should not be exchanged over the phone, but only data about appointments and complaints. But email services in use are secure in different measures.
Participant E mentions the future use of DigiD as a means to allow patients and providers digital access to their data. They use EDIFACT to exchange messages and they are looking at implementing XDS, a messaging standard in healthcare for records. His organization uses different methods to return their diagnostic results to the requesters.
Participant H mentions that communication with dentists outside his chain is very old-fashioned. It is mostly done by physical mail. For internal communication between clinics inside the chain, maybe in the future they want to make use of encrypted email services.

Health insurance companies
There is not much direct contact with health insurance companies. Except maybe for authorizations but this is mostly relevant for large dental chains. Also, not many dentists have contracts with health insurance companies. Participant C thinks that contracts with insurers are pretty strict. They put a lot of requirements on providers. He has a relation with his patients, not with the insurers. Most of dental care is not in the basic insurance so in most cases it is a matter of a relation with a patient. Also, some dentists use a factoring agency to communicate with health insurance companies.

The VECOZO-portal is favourably reviewed by most dentists. They regard it as safe and secure, while it is also easy to use. Only Participant H is not too satisfied with the speed and ease of use of VECOZO for all purposes.

Participant F argues that providers are generally unwilling to share much of their information, since the information asymmetry gives them a position of power. Between actual dentists there is no real consensus on the appropriateness of the data exchange. Participant C says that most dentists do not have any contact with insurers and he is unaware of what data he could share with them if asked. Participant D says that it is sometimes inconvenient when they ask for information because they are not well-informed. It was also said that the demanded information is fairly accurate. Participant H admits that it is sometimes a point of discussion between providers and insurers, what information is needed to assess it.

Other dentists
The dentists agree that exchange with other dentists is cumbersome, and must go through secure difficult-to-use channels with explicit consent. Or via paperwork. Only one dentist says the opposite: their software package provides for easy information exchange with other dentists.

LSP
Dentists are not included in LSP, whereas hospitals are. Participant D thinks this is because of less added value in terms of functionality, while enhancing the privacy risks. However, Participants D, F and G perceive the added value of medication insights. Nevertheless, dentists should not have full access to medical files of patients. This would be exaggerated.
Participant E is already busy with creating a link with LSP for his organization.

Issues
Perceived issues with data exchange are:

What	Explanation	Who
Digitalization	Easier than paper, but suitable for old users?	A
Work division	Cumbersome translation from paper to digital is put with the providers	A, B, H
Integration oral care and other care fields	Other ICT systems etc. Correlation in care needs?	A, E, F

Single up-to-date source of truth	Keeping data up-to-date is costly	A, D, E
Bureaucracy	Too many business rules, slow batch runs, too much information sent	A, B, D, E, F, G, H
Limited data transfer	Amount and size of photos	A
Missing data	Corrections needed, no data for research	D, F, G
Too much control	No autonomy for providers	F
Emergencies	Automatic identification in case of emergency	H

Participant D argues that missing data on medication and heart issues are much more relevant to dentists than most people think. For patient safety during anesthesia, for instance, this could be of help. The link to the data does not have to be two-way. Participant F adds that such a one-way link would be very helpful to research. Most research now is based on the limited data of health insurance companies.

Software provider

Exquise is mentioned most as the used software (3 times), but also Novadent and Chipsoft are named. Participant H says that these software solutions are mostly tailored to individual clinics, so they are not fully satisfied with it. As a chain they also have a different relation with their software provider: they bring suggestions and requirements, while single dentists will most likely accept the package as is.

Hiatus

Providers say they have no redundant data about their patients, and most of them say they do not lack any information. Though medical information could be more securely provided by apothecaries instead of patients.

Period of use

Dentists need the data of patients mostly during treatment. Sometimes they need it a day before, or some days before, for complicated treatments. Otherwise, only when a patient calls to reschedule an appointment for example.

Transparency

Interviewees were asked about the transparency that is provided for patients. Participant D says he writes elaborate treatment plans for special cases, but also that others are not as diligent as he is.

Patient's access

Patients have a right to access their own data. It differs on how they can access it. Some get a physical copy while others can only see a digital copy. Participant E is trying to make a portal for patients.
Some dentists say patients can get photos on a CD or DVD. Participant G says that he prints a physical copy if patients ask for it. When a patient moves to another dentist this transfer is mostly done digitally.
Participant F questions if patients really have a want to see all their own data.

Patient's information is shared between the treatment team. Some participants did not know how much colleagues would have access. But mostly a treatment relation should exist. Participant E says his organization holds a register of processing, which states who can access what data and for which purposes. Thus they try to be compliant with GDPR.

Costs

Participant B, the hospital, says that costs of treatment are not clearly communicated to patients. Several factors are important in this, the slack pricing, the dependence on whether it is insured care or not. This should be improved.
Dentists are legally obliged to make a budget estimate if the treatment costs are higher than 250 euros. These estimates are for the insight of the patient and can be given to him on paper. Participant F thinks with oral care that patients want to be well-informed since they are in additional insurance. Therefore, the counselling is generally good. He also mentions that explaining all the options can be tough, especially when there is a conflict of interest: a (young) dentist's income might depend on which treatment the patient chooses.

A few dentists say they always consult with their patients when there are multiple treatment options: patients can get such a treatment plan. If a patient requests a budget estimate, then they give it. It can be very important to be transparent in this, since otherwise it is hard for patients to know what is right.

Technology acceptance
Several factors have an influence on the adoption or acceptance of a new solution. Participant E stresses that there are two options: 1. You should take all aspects of the health ecosystem into account, or 2. You should start small by offering something that doesn't exist yet and from there grow.

Factor	Explanation	Who
Trust	- People only see the front-end, vague back-end, secret services, hackers, it should be safe - Integrity and a sense of control (of the processing)	A, E
Transparency	- Blockchain contracts - No secretive passing through of information	A, D, E
Ease of use	- Simple for patients - Easier for providers - Complex systems are not suitable in practice - Not much more work all of a sudden - Link with Exquise - Practically implementable - More efficient	A, C, D, E, F, G, H
Security	- Losing personal keys - No access to unwanted intruders	A, B, E
Rights and access	- Maintenance - How to deal with corrections - Monitoring (NSA) - No islands - Authorizations (legally incapable)	A, B, E, G
Compliance	- In accordance with the law	B, G
Added value	- Added features?	C
Efficiency	- No redundancy - Less 1-on-1 relationships	D, E
Awareness	- Value of personal data - Risks of cybercrime - Patient control on dynamics of data - Importance of sharing data - Politics	E
Patient centered	- Patient control	E

Participant E says it depends on what kind of person you have whether he will find ease of use or privacy more important. The tradeoff is generally perceived as that ease of use is more important.

Use case assessment
A high-level use case was presented to the healthcare providers to see what at first glance would be their reaction. The use case presented a system in which personal data would be uncoupled from medical data, except during patient-controlled time slots. This should relieve a certain honeypot aspect from healthcare providers.

Participant A noted that the front-end, the user interface, is an important aspect. What should the patient bring with him? Participant E argues that a solution should be agnostic in terms of user interface.
Participant G mentions that the information that a system gives to the patient is very important: only then can a patient properly decide whether to give consent or not.

<u>Strengths</u>
The following aspects were seen as strengths:

Patient control	- Explicit consent - Specified consent - Only care that the patient wants	A, E, F, H
Time slots	- Time dimension to privacy - No need of data all the time	B, F, G
New links for providers	- Request data - Medication	B, D, E, F, G
Service	- Service for the patient	D, G
Less risk	- Less coupled data - Less strict relations	E, G
Compliance	- Legal framework	E
Low maintenance	- Lower costs - Automatically up-to-date	E, G, H
Data available for research	- Measuring quality of care	F

Participant F poses questions on the definition of patient-centered care and he suggests a hybrid form: patients should be able to choose how involved they are. Participant H agrees that a patient should be in the lead, but adds that providers still have to be able to do their job.

Participant E says that small organizations like general practitioners will have trouble arranging for GDPR, and legal compliance. If you could arrange data storage on a higher (provincial) level this would make life easier for them. Some of these strengths are regarding a central EPD. Participants F and G mention the added value of medication data. Participant G says that when something is a service for the patient, that it should also be executed in the patient's time.

Participant E says that taking away part of the honeypot by providing a more elegant access to patient data, is really better for a provider's risk. Also a blockchain solution might cost less because information is less redundant.

Weaknesses

The following aspects were seen as possible weaknesses of the solution:

Fraud	- No link with reality - No personal check	A
Limited control provider	- Time slots, bad idea - Mystery guest - Not only access when patient is present, - As long as the job can be done.	A, B, D, G, H
Emergencies	- Mechanisms for exceptions	A, F
System complexity	- Patient understanding	A, G
Contacting patients	- No personal caretaking	D
Relying on patients	- No/slow reaction - Not suitable for every patient - Pro-active role providers?	A, D, E, H

Participant A says that this new system does not take away the troubles of identifying people. There is no link with the human, though it's technologically water-proof.

Participant D mentions patients who don't pay their bills. Ideally they are not allowed to make new appointments so this debtors information should be available to the dentist at all times.

Governance

Most healthcare providers advocate a balanced governance, between different actors, in order to keep trust in the system. Mutual understanding and influence is important. Also professional bodies have an important role. VECOZO could be suitable for governing.

Participant F reacts that especially in oral care providers are fond of their freedom, so a common software package will be hard to implement.

There is agreement on an important role of the national government in this. At least in a facilitating role, but also one of supervision. Participant E argues that, together with the government, health insurance companies should push these developments.

9 Discussion with blockchain experts

Healthcare providers were in general to a lesser extent acquainted with blockchain technology and the fundamentals of self-sovereign identity. To complement their market-pull insights with more technology-oriented expectations and recommendations, direct participants in the blockchain innovation landscape were consulted. In appendix B, the professions and links with blockchain innovation of the respective participants are outlined.
Noteworthy is that all participants have more affinity with the business part of applying the technology than with the technical details of the technology itself. Their ideas seemed more relevant to this research than the technical views of developers, for example.

The following model describes the approach to the interviews:

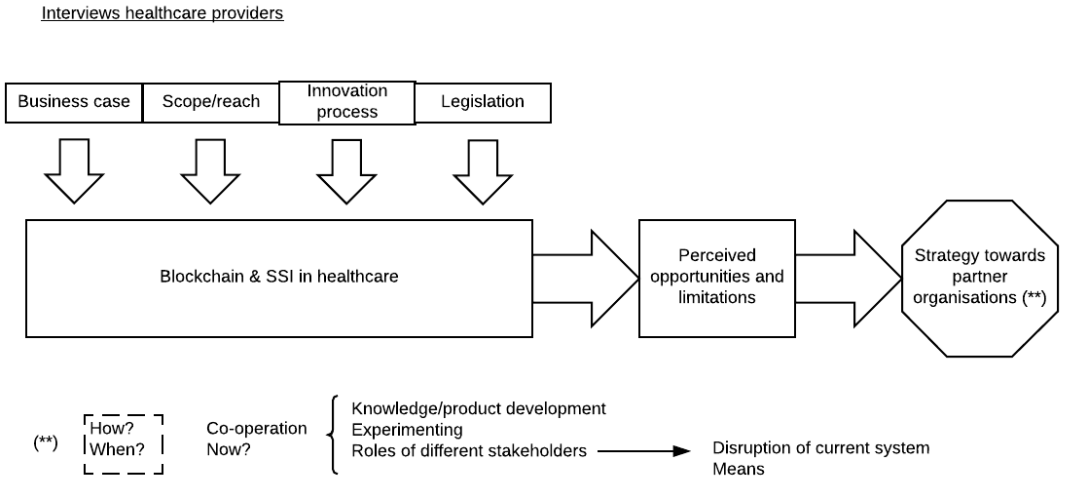

Figure 14: Approach to interviews with blockchain experts.

To improve privacy and readability, participants are named Participant V, Participant W, ..., Participant Z.

Blockchain: added value for identity
Participants were asked for the specific added value that blockchain can bring in identity systems.

Insight in processes
One side-effect of the blockchain hype is that companies all of a sudden start looking at their processes. They start questioning what it means to go from centralized to decentralized. They get a much better view of how their current processes are working; how they identify their customers and why. Participant V argues that it becomes not so much a question of who someone is, but more of knowing if he is authorized to do something with some data.

Take away redundancy
Using each other's onboarding processes can really make identifying customers more efficient. Participant W says that the same process does not have to be repeated multiple times. A central database can help with this, or one can arrange this in a decentralized way with blockchain. Ideally, power shouldn't rest with one organization, especially not a commercial one. This would be a big honeypot for criminals.

Control for the individual
Because of its decentralized character and the use of cryptography, blockchain can truly give control to the user. You want to have a folder, with all sorts of files digitalized. Participant W argues that self-sovereign identity can bring into being a digitalized version of a personal folder with all sorts of files. Self-sovereign identity really puts the person in the center, the interest of the individual. Often company philosophies are also customer-centered. It's not a solution in the best interest of the government or the companies, but for the autonomy of the individual. Participant Z adds that self-determination on personal data is important. Blockchain makes it possible to turn around the model of who owns the data.

Regulate admission rights
According to several participants, the added value of blockchain is that you can regulate admission rights and attributes much better. You can add more attributes on the basis of which you can do business. You can place authorizations better in their respective contexts without losing security. (Participant X says you don't need blockchain for that, per se, but since blockchain will become important you will have to embed this feature in a blockchain solution.)

Smart contracting and identity for the Internet of Things
Smart contracts can arrange for time slots of access, and for a limit on the amount of times someone can have access. But if you want to work with smart contracts, you will have to have some kind of identity on the blockchain. Identity in the broadest sense, so for persons, organizations and for Internet-of-Things (IoT). Your fridge can be a derivative of your identity once it submits orders for you.

Irrefutability and robustness
Experts agree that a blockchain can make for a robust identity which is secure-by-design. It enables one to know if someone is or has something, irrefutably. The immutability of the blockchain also gives the user an irrefutable account on who can use his data when and for what purposes. This identity is not dependent on some provider, it is immutable and transparent in terms of history. Several experts say this is a clear link with blockchain.

Blockchain added value in general
This perceived added value cannot be assessed without looking at the overall expected influence of blockchain. In general, blockchain is going to really change the world, and be very disruptive. Not only in terms of identity, but also general applications, according to Participants V and X. Trusted third parties are less needed.
Also, according to Participants W and Y, blockchain can create new digital products and services. This is relevant in many sectors, including pensions and healthcare. The technology might not be mature enough to overturn the world, but it can cause a revolution.

Possible limitations
Perceived points of concern are the aspects of scalability, and the volatility of the technological developments, according to Participant Y. Together with this performance aspect, when you need to send data along the line, maybe blockchain is not the most ideal tool. Participant X mentions that encryption methods have a life cycle, so also the ones used by blockchain. In the future there will be smart hacking methods and better computer technology. So finally you will have to update your methods, but what happens with the information that is stored on the blockchain then?

Issues with current processes
The mentioned strengths of blockchain technology are also induced by issues with current processes. Experts say current processes are not user-friendly and prone to error. The user does not have any grip on his personal data, while companies store too many data they don't need. There is consensus that there are too many portals, closed doors, and intransparency.
A completely opposite model, such that all your data lies with you and that companies have a subscription on this, will also probably not be the future model according to Participant Z. Rather an in-between form is desirable. Some general information like NAW, which many organisations need of you, will be in your own personal vault, while more specific data will rest with the organization you deal with.

Privacy legislation
Participants were asked for their view of the impact of the new GDPR legislation.

Enforcement and consequences
Participant V believes GDPR is really going to mean a lot for companies, structurally. But scanning the field he does not see a lot of solutions to this, or eagerness to come up with such solutions. He questions if CRM systems will still be necessary altogether. You should give your customers access to part of your own database, this is quite drastic. Current systems are not suitable to really comply with the GDPR. In that sense the legislation is ahead of the reality (while usually it is the other way around). Because of this, enforcement of the new law will probably not be that strict in the beginning. This would be a relief especially for smaller organizations who are not familiar with legal considerations. But there will be a slack period probably, like with IBAN. GDPR is enforcing a new data model with more control for customers.

On the other hand, Participant Y says GDPR is in many respects an extension of current legislation, so things are going to change, but not so drastically. A new aspect is the data-portability, which will require mutual agreements to create uniformity. From a compliance perspective he thinks all is very well doable. A more interesting aspect is how you are going to service a new form of transparency. From a strategy perspective there are also opportunities: maybe if you combine data from different sources, you can deliver new services (making use of the new transparent model). Participant W adds that the impact on grand Dutch companies will on the whole not be that big. Banks, insurance companies and similar firms will not have great difficulty to comply. It is another matter for non-European firms and smaller organizations.

Desirability of GDPR
GDPR is unanimously perceived as a good development. Participant W says that by giving more control to persons, organizations are forced to ask for permission decently. This might also generate more transparency for customers and they might even get some extra value in return for their personal data. Many people will be willing to share data if it gives them something in return and if firms are explicit about their use of it. The privacy and protection of the individual in a digitalizing society is also mentioned by Participants X, Y and Z. It is also interesting that you can now ask for commercial profiles that companies make of you. It's a good signal stimulating the companies to think about these matters. It creates momentum.
Participant X finds the harmonization also good. Nevertheless, he thinks enforcement will most likely be different in different countries.
Only Participant Y mentions the ambiguity: while bringing new opportunities, GDPR also brings more workload.

Impact on healthcare
Participant W thinks the impact of GDPR on healthcare will not be that big: because healthcare providers are not commercial, they are already obliged to handle their patient data with care. Health insurance companies, however, can come into a shady area if they're going to recommend certain services to improve patient recovery.
Participant V stresses that new ethical dilemmas will emerge. On the one hand, it is a good development that patients get more control. On the other hand, you should protect patients from themselves. Sometimes it is not ethically sound to know everything about your own health, and maybe you don't want to know. He adds that extra security and privacy in oral care is a good thing, but this must not get in the way of practicality: often a tiresome identification process each time is not really desirable. In a hospital, with more passers-by as patients this is maybe more urgent than with dental care.
Customers have a latent need for a new model regarding privacy and their personal data, according to Participant Z. The only question will be, whether a patient wants to share his data with organizations or not. If these organizations can give something in return, he probably will.

Alignment with blockchain - pro
Consensus is that GDPR and the principles of blockchain technology are in alignment. Participants X and Z say that the overall goal and bigger picture of GDPR are in line with blockchain and self-sovereign identity. Participant V goes so far as to say that blockchain has characteristics that really can solve challenges posed by the GDPR. People can use encrypted data, in control of the customer who can give tailored access for certain time slots. These are things blockchain can facilitate. Furthermore, especially for admission rights, blockchain seems essential.
Participant W explains the relation of GDPR with the SSIF consortium. GDPR is not the reason for starting with SSI, but it is an extra reason to say: having such a framework we are compliant and even better than with current systems. GDPR is not a threat to blockchain developments, is actually very much in accordance with it. Organizations will have to ask for data much more explicitly than is now the case. Very much in line with the explicit consent of GDPR, self-sovereign identity facilitates rights and access per item. This does not have to hamper the ease of use: there will probably be a few variants of how much data you can share with a certain company, so you don't need the overly long privacy statements of contemporary services.

Alignment with blockchain - con
Possible issues that can arise through GDPR while working with blockchain, are for example juridical conditions on an international level when working with smart contracts. Legislation also falls behind on technology generally. So while it is technically feasible to only know that someone is over 18, Participant X questions if it will legally be enough for giving him alcohol.

Participants X and Y say the right to be forgotten will be difficult to embed into a blockchain solution. For example, even now taking photos off the Internet is very problematic. In a blockchain environment possibly you can solve this by removing not the data itself, but the pointers to the data. A similar issue is whether you want to create a society where all pieces of data are tagged and traceable. GDPR is going to provide for such situations.
A more ethical dilemma is what data you can entrust to your customers, says Participant Z.

Self-sovereign identity: future
Importance
Participant Y says that for parties like health insurance companies and pension providers identity might not be that relevant at the moment since they are in the so-called BSN-domain. Identity information is automatically extracted from services like BRP and VECOZO, so there is no problem or urgency. However, there are constructions where you need additional information about a client: is he/she student, is he/she alive? This does not go automatically. But mainly it is important to prepare for a future where the relation between customer and organization is going to change. This relation will become more mutual and one-on-one. If you want to do additional services, outside of the regular pension or insurance execution, you have a shifting relationship with your customer.
In short, for now there are no urgent problems with identity for many organizations, but a shifting relationship with their customer, can be important in the future.

Reach/scope
Generally, participants have high expectations of the reach of self-sovereign identity in the future. It might become the standard of identification in the future. Participant X expects that all the persons, companies and IoT-devices will be having such identities. There will even come companies who are going to help you in a service-like manner to arrange your control over your identity.
Interviewees say there is momentum to make self-sovereign identity a success. A lot of organizations say they want it that way. But for all we know, according to Participant Z, maybe a model where you mindlessly give away all your data, will still prevail in the future.
Participant Y does not know whether SSI will prevail. He says there are lots of other mechanisms and movements, like iDIN by the banks etc. So he does not dare predicting. Maybe Google or Facebook will come up with their own solution too. Participant Z adds we must wait and see what will be the most accepted, not the best, standard for this.
Participant W says SSIF aims for implementation in the Netherlands and Europe, and ideally in the whole of the world. Participant V and Y add that you can only attract international companies if you have an international solution and that local efficiency solutions do not use the radicalness of blockchan. SSI can enable many products and services that you cannot even think of now, maybe even giving a push to a world with another way of living, idealistically thinking.

Adoption factors
The adoption factors for the technology were also discussed. Participant W argues that to let a platform grow, you need users, but these users will not come if you do not have enough companies and governments who use the platform, and provide data. These two user bases should evolve at the same pace, that will be the greatest challenge, next to technology. (Enough health insurance companies, hospitals and others should join before it is interesting for customers.) If companies/organizations do not join and do not make their data available, users will never be able to use that data, so there also will not be any services built around that data. This is illustrated by three required steps:
1. The organizations that have the customers' data at the moment, must take the step to make this data available;
2. The customer must take the step to create an account and a vault, by which he can share and control his data;
3. Organizations should develop products and services making use of these data.
Participant X says the consortium yields new possibilities. All other companies and sectors should decide for themselves what to do with that.

Experiments will most likely start with applications which users would use incidentally (like buying a house), but according to Participant Z making the step to regular daily services is essential (like filling in forms).
People will not pro-actively create such an identity, you should give them the option when they come to you for a mortgage for example by providing them with the option. It will be a step-by-step adoption curve. Here ease of use will be very important. Making data-intensive processes easier will appeal to customers.

In the process maintaining the decentralized character of the solution will be a challenge, since going from centralized to decentralized is a very fundamental change to society.

Roadmap
Participants agree that mainstream implementation of SSI will yet take some years. At the same time, Participant W says that it will not take 15 years before such a digital identity is commonplace (the time it cost for paying with PIN to become standard), since communication is easy with Internet. Maybe in 2 years already 20% of people will use such an identity in some way or other. Participant X agrees, in a year the first self-sovereign identities will be used. In two years the user base will have grown slightly and then it will take flight. In 3 to 4 years there will be a fairly large group of early adopters who use it. After five years also outside these early adopters, people will start using it. Other participants agree that it will take about five years before mainstream adoption.

Participant Z says that important data providers should be on board of the movement, and there should be a platform that is mature enough to experiment with. If so, in 2018 there could be a Proof-of-Concept (PoC) up and running. It is added that the further you get towards real implementation, the more questions/issues will emerge.

Relation to DigiD, Idensys, and other identity platforms:
Participant W says the government currently does not ask any permission to use your data, they are just there at MijnOverheid.nl. This data processing without your consent is not ideal. DigiD and Idensys provide authentication methods, which are something different from an identity. If you authenticate with an organization who thinks to know who you are, you can add identity attributes to this. But identity attributes are not directly linked to an authentication, though the one cannot exist without the other. SSIF focuses solely on identity and not on authentication for the moment. So you still need the authentication methods of the different organizations.
Participant X thinks the minimum viable product of SSIF won't include authentication schemes or mechanisms, but eventually this will become a part of it. This will pose some tough challenges.
Participant Y says these platforms are both competitors and complementary solutions. On the one hand, identification with DigiD can be a part of the SSIF framework as an authentication method. But from a framework perspective, if people are satisfied with iDIN as identity, for example, then it is competition.

Self-sovereign identity: innovation process and roles
Competition
There are multiple (40 as claimed by Participant X) initiatives around the world to construct self-sovereign identity systems based on blockchain technology. Participants were asked about the role of competition.
The blockchain-identity system of Estonia is mentioned. Participant V says it would not be wise to re-invent the wheel.
Most participants say the level of competition is not very high. Ideas are openly shared with other consortia, which is perceived as a benefit. It is said that both SSIF and Sovrin are not-for-profit, though of course there are underlying motives, but basically they want to prepare for a future solution. Participant W adds they also try to learn from other initiatives and combine the best elements. There is no business case to developing the SSIF platform, though eventually the goal is for it to become self-sustaining. Also there is no need to creating the winning platform, interviewees say that it would be fine if another platform would become the standard.
It is also important to give openness about your own ventures and making everything open-source. Thus you can ask for feedback and see what others have to say about it. You should also give openness on GitHub for example, so as to ensure that you do not miss out on details. Thus, general opinion is that open-source development is most beneficial. Also, because in consortia non-disclosure agreements can trouble the sharing of insights.

Consortium - goal
With some of the participants familiar with the SSIF consortium, they were asked about the goals of the co-operation. It does not work if one company brings such a product on the market with the threat of a lock-in aspect. Compare Microsoft Passport and other past ventures. As such, according to Participant Z the consortium approach is the right way.
Participant W says that there are other initiatives in other countries, but the approach of SSIF was to learn about the technology. To try and develop this by yourself (in a consortium) is a good way to really get to know the

troubles and requirements with respect to technology and security. By committing to this interactive learning process, you can eventually make a well-funded choice for a solution in the market perhaps.
The learning process is not the only goal. Participant Y mentions that the goal of the consortium is to develop a working implementation that can grow autonomously (Autonomy meaning that participants to the consortium do not have to stimulate it by building new applications on top of it, but rather external organizations see the benefits and start using it.) But there is no business model besides that.

However, Participant X says that only learning requirements is not the right approach per se: requirements tend to capture the past instead of the future situation.

Consortium – pros and cons
The current state of the consortium was also discussed. The interviewees stressed that many participants are now involved in the consortium. There is now a large conglomerate of organizations: from companies to governmental bodies to research institutes. These organizations all agree that such an identity platform is needed. Participant Y says that there is the realization that this digital identity is a necessary next step. All organizations work together on plans and business cases. This creates momentum for the technology.
According to Participant Z, the organizations realize that you cannot do such a thing on your own. It is an ecosystem where companies agree they want a standard to share their data with their customers. This is not only a want, but also enforced legally by GDPR.
Also by working together, companies thereby will not mistrust each other and will be willing to join in the data sharing. Because no one, and thus everyone, owns the solution. This will also increase the trust of customers. The Dutch 'poldermodel' is very suitable for these partnerships. The first steps should be taken together, and then afterwards organisations can compete.

Participant X thinks the common learning process is essential. By building and developing yourself, not only thinking but doing, you get a better view on what it can actually be and what are bottlenecks. By doing it yourself, you get much more insights. It is too complex to solve it only theoretically.

Steps to take-off
1. You should together come upon a set of standard protocols for sharing data and giving these back to users.
2. Leading companies should try to use these standards in PoCs. (It depends on which standards are being used the most, this does not have to be the best one.) Step by step, around a certain number of use cases.
3. Making an account or vault should be fairly easy for customers. Startups should then get to see that they can get a far more direct relationship with customers, also in terms of financing.

It is also mentioned that the amount of actors involved in the consortium can be a downside. All these actors want to keep something the way it is. This could slow down the pace of the innovation. Besides, most radical solutions, the new protocols that are really going to change something, will most likely be devised open-source. Not from a collection of organizations who principally want to keep themselves alive.

Healthcare participation
Interviewees were asked what this means for the participation of the healthcare sector. Participant W thinks health insurance companies and the health sector in general should actively participate in the consortium. They should join now, so they can build knowledge on the challenges and the opportunities and to help out in complex health-related issues. Especially in healthcare there is quite some complexity, with authorizations of family members, claims et cetera. It is rather complex to get that right, digitally. Arguably, 80% of human activity can and will be pursued digitally, so healthcare should probably have an interest in getting on board.
Participant X agrees with this: healthcare should think together with the consortium, else very weird constructions in the future when SSI is commonplace will be needed to adapt to it.

One participant says in healthcare an identity is not that important, the body is important. Maybe one can give the body an identity, that can be coupled to a person in some cases. Participant Y does not know if it would be very relevant for healthcare to give direction to the consortium, or if identity is really relevant now or in the future. However, he says claim-based verification can be important in multiple sectors, so also in healthcare, regarding electronic health records for example.

Interviewees say that for the consortium it is good to have a broad representation/range of sectors on board. Healthcare would be a good addition since they have their own view on their own use cases.
Participant Z adds that the overturn of the data model within your own organization is not that easily made. Thus it can be very fruitful for a health insurance company to start this process by joining the consortium and actively think about their own processes. If this self-sovereign model is eventually arranged, maybe as a health insurance company you can generate new services. Combine new data from customers to be able to service them more or buy better healthcare.

Regarding the competition with other health insurance companies, interviewees think many applications and services are going to be possible on the basic SSI infrastructure. Cooperating to get this basic infrastructure is very important, then you can afterwards compete each other on top of this shared infrastructure. Creating your own corner of the basic infrastructure, only accessible to you, is not in line with the self-sovereign philosophy. Organizations need one another to make it a success. Only if you have a basic infrastructure, on top of that, you can distinguish yourself with unique services or data combinations.

Governance
Several actors in the system of innovation have several roles. Participants were asked their view on this.

Role of the government
Although the technology is still in an early phase, sometimes things happen that require some form of regulation. ICOs are an example of this. Thus, however immature blockchain implementations are, users start to see that it would be convenient if some institution like the government or AFM poses preconditions. And that some activities can only be pursued after some regulation has been put in place. Participant Y agrees with this in mentioning that the government should protect the citizen. This can be achieved by additional legislation. At the same time this regulation should not be too strict: this could harm the innovation process. A legislative role is, however, not the first step.

Participants agree that a facilitating role for the government is important, but a stimulating, leading role can really speed up the innovation process.
The government should take on a facilitating role, and they are good at that, according to Participant X. Public-private partnerships are important and the Netherlands are traditionally good at this. Also creating political foundation is important, and awareness of the importance. He emphasizes that the Netherlands is a country of distribution, with its airport, seaport and strategic position. In this respect, a leading role could be very good for the Netherlands. Participant Y thinks it could be very cost saving for the Netherlands to let the government take a leading role in this.
A facilitating role could be important: when someone loses his private key, some sort of support should be devised. Current troubles with Bitcoin and taxes is named as an example.

According to Participant Z, the bulk of the exciting data lies with the government. If they would join by disclosing their data, that would give enormous momentum. Other interviewees agree that the government can lead by example. If the government steps into it, it will immediately become much more interesting for other organizations to join in, since then interesting data will be available. The government thus has a facilitating role, but they should also be decisive.

The subsidizing role is stressed less. It is mentioned by one participant. But Participant X says it does not deal with great amounts of money, and current policies don't have to be adapted for it. He also mentions the role of European government. Stimulating micro-financing initiatives and letting loose the structure of top-down centralized control can prove disruptive on a global scale.

Roles of other parties
Some participants envision a more governing role to the people instead of some central institution. For example, a situation is mentioned where your neighbours can have influence on what kind of insurance you can get. Participants W and X say governance will be comparable to that of the Internet. Some new parties will be created that will manage the necessary maintenance of the networks and protocols. New parties will emerge, next to existing institutions, with the authority to validate claims, who will be able to declare people's authenticity. There will come a shift in the system.

Other aspects

Ease of use

Participants explicitly name that ease of use for end-users should be guaranteed by a SSI solution. One aspect of this is the interaction design, the apps and the websites that a user has to deal with. The front-end should be logical and simple. The second aspect is that there should be applications/services on the platform which have an added value for the user. Thirdly, not only the happy flows should be enabled by the platform, also the bad flows.

Platform

Blockchain platforms can be divided into four types (see chapter 6). Participants gave their view on what kind of platform seems suitable to them.

With SSIF there is discussion on what kind of platform, but no decisions yet. Participant W says that for now the SSIF has been made blockchain agnostic, since the technology is not really stable yet. If you chose a platform, you are stuck with it most likely. Eventually an unpermissioned public blockchain would be the ideal case, since everyone should be able to participate and check each other. At the same time, currently in terms of trust and openness, a permissioned blockchain would be a safer first step. Willingness with people who have never heard of blockchain to immediately make use of such a public chain is probably low. As the user base grows, you can go further towards unpermissioned gradually.

Whatever platform eventually might be chosen, Participant Y says the tendency is to store as less personal information on the blockchain as possible. There are no personal data on the blockchain, just claim verifications.

10 Discussion

Tying the findings from the literary search and the interviews together, we are now in a position to discuss the general outcomes. For this we recall the framework that was first shown in the introduction:

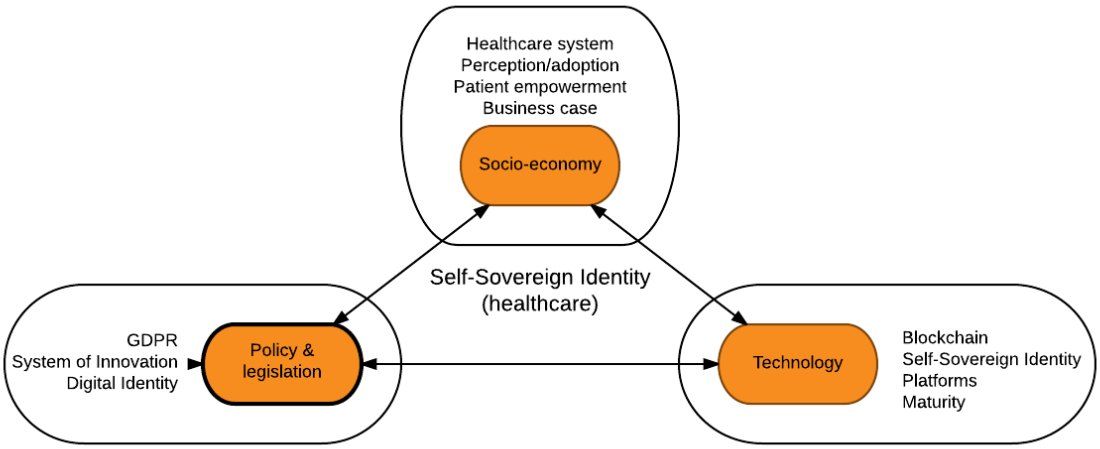

Figure 15: Framework for self-sovereign identity in healthcare.

The components in this framework can now be addressed. Some of them are more extensively treated than others, according to the emphasis laid in the research.

Healthcare system

The complexity of the healthcare system is not really stimulating for radical innovation. Path-dependency and lock-in are the reason for this. Instead of a top-down overturn of existing systems, a more incremental approach with experiments and applications in relatively closed and riskless environments is suitable.
In this respect, oral care is a good experimentation garden. Dentists like to have a lot of freedom and not much of them are contracted by health insurance companies. This made that uniformity was not really apparent in IT-systems and identification processes. By one interviewee it was acknowledged that implementing one standard IT solution would be problematic. A central portal like VECOZO is, however, generally favourably perceived.

Perception

The perception of the problem by actors in the dental care domain is also not beneficial. From the perspective of the healthcare providers generally speaking there is no sense of urgency for a new IT-infrastructure concerning personal data of patients. There is room for improvement with regard to aspects like bureaucracy, and data silos, but generally the privacy risks in oral care are deemed fairly low.
Thus, with the implementation of a new system not only raising awareness of patients, but also of providers seems essential. The implications and the particulars of the GDPR are not commonly known to dentists.
Because problems with the current situation are not fully perceived, a new system should first and foremost bring added value in terms of functionality to convince oral care providers to implement it.

For patients, identification also does not seem to be a top priority. It is not mentioned in the quality indicators list for healthcare. General digital identity management is, however, seen as problematic.

However, the consulted blockchain experts perceive a positive momentum for self-sovereign identity: companies are getting together, legislation gives a push in the self-sovereign direction and the government also seems willing to participate. There is a shared sense of a need for the next step: a platform where people can have control of their own identity. Alternatives to future digital identity with other principles are recognized, but the experts believe there really is a willingness to make self-sovereign identity a commonplace.

Business case

The perceived benefits of a blockchain-based system for healthcare providers can be divided into linking missing data sources and unlinking unneeded data links. Unneeded redundancy of data and easier implementation of a

single-source of truth that is always up-to-date and accessible is another perceived benefit of blockchain technology in healthcare.
Benefits for patients, as structured in the Patient Federation's framework, are also recognized by interviewees. Blockchain promises to deliver added value to at least control of care, efficiency, accessibility of care and transparency regarding treatments and costs.

The interviewed healthcare providers were interested in added functionality or services that self-sovereign identity could bring, as long as their own working conditions were not impeded by it.
The health insurance companies' benefits vary between different blockchain use cases. Efficient and justifiable healthcare are important values for them, which can be enhanced by transparency and robustness that a blockchain solution can bring. Also defragmentation of data sources can make it more cost-efficient and valuable.

Nevertheless, there are significant differences between what healthcare providers and blockchain experts see as opportunities or threats. The difference between the interviewed healthcare professor and the blockchain experts is evident with respect to research: the professor sees the new legislation and blockchain as a threat to the research possibilities while the blockchain experts only see the added value of blockchain. They say it can add much to a more tailored form of providing data to researchers. According to them, patients will be willing to share more of their personal data as long as they have the feeling they are in control of it and can perceive the added value of sharing it.
The 'anonymous' data sharing that a blockchain can facilitate, stimulates a pro-active attitude for care providers, leading to more preventive treatments which can be less costly than curative treatments and also give more accurate direction to research and treatment needs.

A benefit of using bockchain for identities is the possibility of providing smart objects with an identity. The Internet of Things (IoT) which will become more relevant as patients measure their own data with the help of wearables, will pose serious privacy issues. These issues are arguably resolvable by blockchain technology and self-sovereign identity.

There are however, also weaknesses. The immutability of the blockchain ledger is at the same time perceived as a strength and as a threat. On the one hand it provides a robust record on which the individual can rely and prove his rights. On the other hand, difficulties with the right to be forgotten will occur. This should be obviated by minimizing the amount of actual data on the blockchain ledger.

Technology: SSI
These business considerations are not the only factors of influence. The actual technology is also not a static object. The state-of-the-art and maturity of both blockchain and self-sovereign identity are discussed.

Self-sovereign identity solutions are becoming operational and the technology seems to be ready for real-world experimentation. Before actual implementation can be, organizations and firms should however, get a good idea first of what their requirements are for such an identity platform.

Three enabling factors are necessary for the widespread adoption of SSI. There are several phases/factors required in this process:

1. Leading companies (banks, insurance companies, governments) should make (some of) their data available for experiments and clients.
2. Individuals should start using and managing their personal data.
3. Organizations should develop applications and services on top of the SSI infrastructure, which are relevant to clients.

These three factors should develop in a balanced way: for example, if patients start to manage their personal data and there are applications that can create value by this, this will not work if organizations do not make the data they have about persons available. Keeping this balance in the innovation process is recognized as the greatest challenge.

Participants are mostly positive on the future of self-sovereign identity. General expectations are that a platform that protects the individual's identity is a necessary next step to a more digital society. Thus, they expect that in the future everyone will have some sort of self-sovereign identity.

This development is reckoned to be more disruptive in developing countries where many people do not even have a legal identity as yet. Here they could possibly facilitate micro-financing and other services at the moment not available to many people there. Gains in western civilizations like the Netherlands will be more incremental, but eventually for international interoperability this will also give many benefits and necessity.
Ultimately self-sovereign identity could help facilitating a new way of living or a new form of society.

But the roadmap as they foresee it, is that it will be at least five years until mainstream adoption of SSI applications. Early adopters will start using it to some extent in the coming years, but many barriers (as explained by the 3 factors) still have to be overcome gradually.
In our age of digital communication progress is, however, not expected to take as long as with the adoption of the internet, purely because means of communication are much faster nowadays.

Technology: Blockchain & Platforms
The maturity of the blockchain 'sector' is often debated. The fact is that there is no consensus on which platforms will prevail in coming years or on how these platforms will develop. This makes organizations cautious on committing to certain platforms. For example, the SSIF consortium is blockchain agnostic for now. Choosing a platform for experiments in a testing environment is not easy, but for a truly operational application it can be very risky. Support for many platforms is scarce and continuity of them is not guaranteed.
In the interviews with blockchain experts often future scenarios were envisioned in which the possible disruptive capabilities of blockchain are fully exploited. In these cases a model of true peer-to-peer business relationships was mostly seen as ideal, or at least interesting. The need of a gradual, incremental innovation in the public healthcare sector was, however, recognized. Thus identity-solutions with a private and permissioned character are admitted as necessary first steps.

GDPR
Important institutions in this system of innovation are the current frameworks for digital identity and the GDPR legislation.
Neither healthcare providers nor blockchain experts were much intimidated by the impending GDPR legislation, though some recognized the possible difficulties of complying with it. There was consensus that current Dutch privacy rules are already quite strict.
The compliance will mainly be important to discuss with dental software providers and management of the bigger dental chains. The software providers are the main party on which dentists rely for their digital communication, and with a not much scattered market implementing new functionality or modules linked to their products is maybe the most effective option. On the other hand, the rise of dental chains can stimulate new developments in dental patient software, so also their participation is important.
Healthcare providers are mostly daunted by a possible administrative burden that strict privacy regulation, not particularly GDPR, brings. With a blockchain system it should therefore be an important aspect that compliance with GDPR is smoothly built-in.

The harmonization that the regulation brings is hailed more or less by the chains, but it doesn't appeal in other respects: some say that oral care data is not really privacy sensitive and posing strict demands on sharing this information can really hamper research or the actual caretaking.
Harmonization can be good for a uniform ICT-infrastructure, but in the end country-specific healthcare systems make country-specific solutions desirable.

There is some discrepancy among the experts about the practicality of the GDPR legislation. They agree that the bigger companies (who are familiar with legal constraints) will not have that much of a problem complying, but smaller SME organizations can really get into trouble and incur extra financial or administrative burdens, depending on their field of activity. One participant says that he does not see how organizations can comply with GDPR at all with current IT-systems. Others say that this won't be much of a problem, but that only non-European companies will have significant trouble adapting to this.

Despite these enforcement difficulties, the legislation is generally perceived as a good development within modern society, better protecting citizens in a digital age. The experts are unanimous about the good alignment of GDPR legislation and the principles of blockchain and SSI. The control and insight that GDPR wants to give to the individual, is supported by blockchain/SSI, they say.

Possible limitations regarding the right to be forgotten are scantily mentioned. Experts expect that a way around this can be found, by storing pointers to data on the blockchain instead of actual data. Most experts are very positive on the potential of blockchain in this respect.

System of Innovation & Digital Identity

Government

Experts mention multiple roles for the government, from a practical point-of-view, on how they can be optimally integrated in the innovation process. The most efficient role would be an actively participating role: if they would make their data available to PoCs and experiments this would very much stimulate the innovation process. Since the government is owner of much valuable personal data, their participation would make use cases more interesting for other organizations.

When developments are getting operational (out of the experimental phase), the legislative and protecting power of the government should be wielded more, since people negatively affected by new solutions are unwanted if you want the general development to take off. (ICOs provide a good example of these risks.) The government should make sure citizens have a safety-net.

Subsidizing is also relevant, but not problematic, since it is not dealing with huge amounts of money and policies do not have to be adapted.

Governance

Governance of SSI frameworks and applications is a matter of debate. Healthcare providers stress the need for a balanced role of different actors: health insurance companies, professional bodies and the government, are mentioned. This should ensure the trust of end-users. Experts chime into this, from a practical point of view: an initiative by a single company won't work. Something owned by no one and thus by everyone has much more chance of succeeding because of the great implications to communication and business. An Internet-like governance model is possibly also needed for keeping the blockchain network running.

A shift from centralized to decentralized society or business is massive: because of this, in practical terms a gradual transition from permissioned private to permissionless public identities is probably needed to slowly build acceptance and familiarity. Eventually, from an idealistic point of view, a permissionless public ledger is desirable for SSIF, so everyone can truly have equal control over his identity.

Consortium

The relation of SSI towards current identification processes is twofold: on the one hand, the minimum viable product that is now being developed still needs authentication mechanisms to be implemented with it. These could still be provided by DigiD or Idensys.

Otherwise, these mechanisms like iDIN can also be regarded as stand-alone identities and if the public is happy with them, SSI will have a challenge replacing it.

Interoperability and cross-nation standards are important goals of Europe's and Dutch eID programmes. This seems fitting with blockchain or SSI initiatives which can provide for an international infrastructure/protocol, on which national applications can be built.

Between the experts there is consensus that blockchain requires an extensive learning process and if you are in a leading position in your sector that you should start experimenting with it in an early stage. Expectations are that blockchain and identity can really turn around your existing models, so adapting to this requires time and effort. Potentially, it's not a small change of some IT-architecture that only some employees will be faced with: going to a truly decentralized model requires a different approach in all the layers of the organization.

The need of an extensive learning process is reflected in the operating form of the consortium: hereby participants aim to learn co-operatively in a hands-on but efficient way. Important bottlenecks, considerations and opportunities cannot solely be spotted by theorizing about it. The problem is too complex for that. Working together in a consortium is thus a good possibility.

The goal is not necessarily to construct the implementation to be used in the future. But the learning process can also enable organizations to make a well-funded choice for a platform in the market.

No company can do this on his own, but will a group of companies with all kinds of underlying interests and business models be able to devise a truly disruptive solution together? Perhaps open source efforts are hard to coordinate so these are of less strategic importance to CZ's own efforts, but these can be more serendipitous and stimulating to truly radical innovative protocols or models.

Healthcare system

Consortium

Consensus among experts is that the healthcare sector should be actively involved in the development of a basic identity infrastructure. Especially in a sector with sensitive data and complex relations between actors, their requirements and needs should by design be supported by a new SSI infrastructure. This is not trivial, since claim-based verification is not a cure-all for identity processes (as mentioned by some participants).

Participation by the healthcare sector would be beneficial to the consortium because their insights could help in constructing a solution that can really be implemented in a wide variety of societal areas. This makes for a greater possible user base and thus more functionality and opportunities.

Also for the healthcare sector itself it could prove beneficial as the blockchain experts (and to a lesser extent the healthcare providers) envision many promising use cases for health care. Besides, re-arranging internal business processes to make them decentralized instead of centralized requires an intensive learning process and evaluation of current structures. This learning process can be streamlined by interactively learning together with other firms.

Health insurance companies might be leading in the health sector: their operations range over all the subsectors and they are the biggest in terms of financial means and customer bases. Also, their data is in the current situation more used than the data of healthcare providers, so maybe sharing it in a blockchain-like configuration is not really radical.

Health insurance companies also have a strong business case for taking this lead. In a market-oriented field new cost-efficient systems are an important prerequisite to keep a healthy competitive position. Also, the various possibilities of devising new applications and services, which are mentioned by several of the blockchain experts, make sure they transition to a future-proof business model.

Competition with other health insurance companies is not really in place just yet. First, a basic identity infrastructure should be created. The applications that can be built upon such an infrastructure provide enough room for competing services and products between health insurance companies.

If the health insurance companies take the lead in this, one might get an efficient roll-out to the entire healthcare spectrum.

Noteworthy is the perceived shift from a landscape of lone dentists to a field with large chains of clinics. This poses some difficulties and new requirements to software packages. These can be combined with the implementation of a more blockchain-like solution. A need for an improved software package and more bargaining power for the chains as opposed to dentists might be an opportunity.

Use cases

The use cases that was most often approved of, was the addition of a link between medication data and the dentist. Medical anamneses are time-consuming and prone to error, especially with the patients for whom these registrations are most relevant: elderly people who regularly take a myriad of medications maybe could be relieved by automatizing this process.

Medication data are very relevant in the daily activities of dentists. Medication conflicting with certain operations or anesthesia should be properly known up-to-date by a dentist.

A medical anamnesis can at the same time be a compromise to a patient's privacy. A dentist who has a proposed treatment does not need all the information in an anamnesis, he just needs to check possibly conflicting medicines or conditions. A customized or attribute-based disclosure of information is thus suitable to this situation. Control for the patient is important in this disclosure.

A first implementation with these data can, in case of success, pave the way for wider implementation across healthcare subfields. Leading to self-sovereign electronic health records.

Access management to Electronic Health Records is a commonly mentioned use case for blockchain-based identity. A single source of truth can be very beneficial in maintaining health records of different healthcare providers pertaining to one individual. Keeping records up-to-date and in synchrony is not trivial without blockchain. Estonia is a leading example of a country which has managed to digitalize its healthcare files and make them more transparent for its residents.

If patients/individuals are going to gather personal data with the help of wearables and personal health monitors, they can set up their own Personal Data Stores. This data can be stored under their own self-sovereign

identity and with the use of smart contracts be made available to different parties like health insurance companies, healthcare providers or researchers in exchange for a certain service. This service can be a discount, research findings, or the provision of preventive and pro-active care.

The proposed use case of unlinking personal data from dental/medical records to reduce the honeypot of the dentists was received with mixed enthusiasm. However, blockchain experts do see the added value for this. Also, the reservations of the healthcare providers can probably be taken away if the solution does not impede their current operations and if this can be made clear to them.

11 Conclusion

We come back to the research questions to evaluate how they were answered in the research.

What is blockchain technology and what are its main characteristics?
A blockchain is a combination of protocols allowing for a decentralized control over shared ledgers where transactions are irrefutably recorded and added with a consensus mechanism. During the research it came to the forefront that several characteristics of blockchain could be relevant for this topic. Especially the decentralized character which allows for cryptographically secure rights and access and possibly anonymity, are relevant. Blockchain technology can provide for consent and access management in complex fields with many actors participating in transactions.

What is self-sovereign identity?
Self-sovereign identity is a framework for digital identity (on whose definition there is no consensus), which consists of a set of principles which must be satisfied. As such different implementations are imaginable, but as of now blockchain is widely used to be able to give individuals true control over their own identity. It can generate a shift in data access and data ownership models.

What is the current state-of-the-art of blockchain applications in health- and identity-related problems?
Blockchain applications are not widely adopted, with only Bitcoin having a significant user base. In terms of identity there are some general applications, in development phase or roll-out even. But these are not tailored for healthcare applications as yet. However, Estonia has made its health records accessible with a blockchain mechanism.

What interactions and legal boundaries with external stakeholders concerning identity does a health insurance company maintain in the Dutch healthcare system?
Interactions are numerous and complex. The data exchange and management is forced by several regulations and laws. Healthcare is for the most part in the BSN domain, actors are obliged to know their patients and in the near future the GDPR regulation will pose significant demands and restrictions to operations.

What requirements must a feasible blockchain application meet to provide a desirable identity system between a health insurance company and an external stakeholder?
This question was focused on healthcare providers in oral care. Their arguments could be more or less translated in ease of use for themselves and for their patients. Privacy and security considerations were of secondary importance to most of them.
For a health insurance company efficiency and time bounding are important indicators of the added value of new applications, so this holds also for blockchain. Identity in itself is not regularly mentioned as an issue, so digital identity is important but not urgent. Health insurance companies are, however, the most influential organizations in healthcare so their active role can be to take the lead in this.
Of course, the application must be compliant with relevant legislation.

To what extent does self-sovereign identity technology fit these requirements?
Self-sovereign identity has a good fit with the impending new privacy legislation GDPR. Ease of use is not immediately clear, since it might mean a shift of responsibility to the patient and a manner of dependence for healthcare providers. Several applications and use cases can be imagined that have added value for all parties.
SSI provides for a more personal approach to data and modern principles in alignment with contemporary society.

What could self-sovereign identity technology add in terms of business value?
Looking at the three main actors in the healthcare market, the following added value is distinguished. For the customer, a position of control is made possible. 'Regie over zorg' is a role aspired by patients. This should also come with enhanced ease of use. Self-sovereign identity can mean something in this respect by enabling the automation of certain processes. For the healthcare providers certain risks can be taken away: relieving them of several data links and storage needs, can make their data records less vulnerable to cyberattacks. Customized rights and access to other health data can generate added services to patients.

For the health insurance companies immediate benefits are not really clear. Processing time of claims in dental care are too long, but it is questionable whether SSI can make this faster. It can make it patient-dependent, though. Added services and functionalities are, however, also vital to health insurance companies. Easy sharing of certain medical data can provide new insights and facilitate a more pro-active preventive role for healthcare providers. This can in turn increase efficiency and reduce the costs for curative treatments.

What should be the role of the different actors in the system of innovation?
Healthcare providers prefer to see a shared governance between different stakeholders, for a balance of power and to retain trust. This trust is also recognized by experts, who say that sectoral boundaries should be breached to foster truly disruptive new services and products.
Without the aid of the government it will take some time to create momentum.

These findings are combined to give an answer to the main research question:

Can self-sovereign identities using blockchain technology improve the management of identities and access in the interactions between a health insurance company and its external stakeholders in a cost-efficient manner within Dutch and European legal boundaries?

SSI can certainly bring improvements in terms of compliance with new legislation and a paradigm shift of data management (patient-centeredness). This can help organizations become more service-oriented and improve their products or applications. Also in a healthcare context multiple use cases can be devised. Due to the prematurity of the technology conclusions about cost-efficiency are not easily put. What is certain, is that a shift towards a decentralized 'world' requires a complete turnover of existing systems, a lot of time, effort and thus costs. But this will be essential to prepare for the evolving digital world we live in.

It appears that self-sovereign identities can be cost-efficiently implemented, since they can take away redundant onboarding activities and efficiently provide for the access and verification of data. Nevertheless, the data ownership and thus business models are bound to change, and thus new economic configurations should be envisioned. Besides, technology should mature further to see if it can actually provide for all the requirements and at the same time be scalable.

Taking a step back and reflecting on the research, what was perhaps the most remarkable result is the missing sense of urgency for digital identity within healthcare. Not only providers, but also the health insurance companies were mostly not aware or not impressed with the risks of current-day identification. Nevertheless, as shown in the literature study, healthcare is one of the most vulnerable sectors with respect to cybercrime. The importance and urgency of finding new digital identity solutions which are better harnessed against threats, is vital. Blockchain and self-sovereign identity are just one manner to solve this issue. Solving this broader problem is of great interest to many actors, and the healthcare sector should be wary that it does not lag behind on other sectors in terms of security.

12 Recommendations

A first step in every blockchain innovation will be to find use cases which add value to different stakeholders. Otherwise, time and resources spent on the experimentation will likely be misdirected. The finding of these use cases specific for healthcare can be stimulated by creating a workgroup with this sole purpose.

There are no perceived urgent issues with healthcare providers and health insurance companies regarding identities, since they operate in the BSN-domain. Therefore, at the moment blockchain technology will not add much value in the identification process. However, the importance of digital identity is great. In the future, with more mature blockchain and self-sovereign identity technology this urgency or opportunities for new services might come.
The scattered landscape of small dental organizations, and their sometimes precarious relation with health insurance companies, are not beneficial to this sense of urgency. It will require much effort to widely infuse them with the willingness to use a new solution that is provided to them.
Raising awareness with other stakeholders and relations of the value of personal data and the risks of cybersecurity that individuals and organizations face together is an important precondition for innovations regarding (self-sovereign) identity.

Blockchain and self-sovereign identity are just possible solutions to a much broader problem of secure digital identity. Possibly other solutions like the IRMA project can eventually provide a method that is just as desirable as blockchain. But without convincing stakeholders and internal employees of the urgency and necessity of improved security standards, healthcare will stay vulnerable.

An important side effect of the blockchain hype is that companies start thinking about their processes and their handling of personal data. This is also relevant for health insurance companies. Actively thinking about these processes with a future perspective of new services and joint initiatives with other organizations can be very beneficial. Banks are aware of the troubles with future digital identity and invest many resources in tackling these issues. For healthcare organizations, assigning employees to boundary spanning activities and trying to increase implicit/tacit knowledge for the organization is valuable. Joining a consortium like Techruption, but also SSIF, can be an example of this. There is also momentum to generate this knowledge. Many organisations are joining in these efforts.

Innovations in public systems, like healthcare, tend not to go via overturns of disruptive new technologies. Rather, big changes can be achieved by incremental, evolutionary steps. An overturn by completely arranging it according to blockchain principles will cost too much time. When finally achieved the technology will be already obsolete. Rather, gradually more and more services will become available using self-sovereign identities. These can be implemented one-by-one in the healthcare field. Thus, simple use cases with trusted partners and which don't require many data sources are needed as first steps in the innovation process.
Expanding upon this is only possible when support and conviction increase in the organizations. Bringing this knowledge also into a consortium which has a more general approach than healthcare alone can help to create standards and basic infrastructure.
In this respect, co-operating with competitors in spotting bottlenecks and important requirements for healthcare use cases could be better than avoiding them.

This bottom-up approach can also be valuable in other particular healthcare fields. Oral care is not the ideal experimental garden per se. The blockchain experts also spontaneously came up with use cases for other fields. Use cases with other stand-alone fields like physical therapy and apothecaries can be other starting points for experimentation.
The dental care landscape consists mostly of solo practices. In mental healthcare and hospital care (GGZ and MSZ) for example, organization structures are different, possibly providing better innovation resources and needs.

Much valuable data is held by the government and the government has also shown it is willing to experiment with blockchain technology. Thus, opportunities lie with use cases in which they are involved. Actively seeking cooperation with the government and involving them early in the innovation process can generate some of the most valuable use cases.

When going to pilot phases with actual patients the government should be involved for legislative protection of the individual. Public perception of blockchain/Bitcoin is not very positive, so one should be careful with this. Cooperation with other organizations in consortia is one method to create leverage and bargaining power with the government.

11.1 Limitations and further research

Because of the broad nature of the problem and the limited time and means for the research, several further explorations and research can add to the literature about the technology.

Some stakeholders have not been actively involved in the research. For example, VECOZO which is the communication platform between health insurance companies and health providers. Since blockchain could have impact on their role it would be a good next step to investigate their position in this. Also patients' interests and desires have only been gathered from secondary sources. Especially when focusing on particular use cases their opinions and requirements are invaluable. It would be interesting to know to what extent they want control over their healthcare data.

Because of the immaturity of the technology, the uncertainty about the disruptiveness of the developments to come, and the generality of the research topic, it was not feasible to include cost estimations and efficiency gains in the results.
Blockchain and self-sovereign identity are not the only solutions to the digital identity problem. A comparative study with other solutions could give more insight in steps to be taken.

During the interviews several use cases of self-sovereign identity were mentioned by participants. The most often mentioned ones are stated in this report, but other individual cases can be evaluated and possibly pursued further.

Legislation has only partially been included in this research. The GDPR poses an important change organizations will have to deal with, but there is other legislation concerning identity and business transactions which was left aside.

References

[1] Satoshi Nakamoto. *Bitcoin: A peer-to-peer electronic cash system.* 2008.

[2] Gartner. (2017). *Gartner Identifies Three Megatrends That Will Drive Digital Business Into the Next Decade.* 15-08-2017. URL: http://www.gartner.com/newsroom/id/3784363

[3] Narayanan, A., Bonneau, J., Felten, E., Miller, A., Goldfeder, S. (2016). *Bitcoin and Cryptocurrency Technologies.* Princeton University Press.

[4] Coinbase website. URL: https://www.coinbase.com/about?locale=en

[5] Blockchain.info Wallet Stats. URL: https://blockchain.info/charts/my-wallet-n-users

[6] Vermeend, S., Smit, P. (2016). *Blockchain: de technologie die de wereld radicaal verandert.* Einstein Books.

[7] Gartner. (2016). *Gartner's 2016 Hype Cycle for Emerging Technologies Identifies Three Key Trends That Organizations Must Track to Gain Competitive Advantage.* 16-08-2016.

[8] Website US Department of Health & Human Services. (2016). *ONC announces Blockchain challenge winners.* 01-09-2016.

[9] Portaal voor iStandaarden in de Zorg en Ondersteuning. *Blockchain: Mijn Zorg Log.* URL: https://www.istandaarden.nl/izo/innovaties/blockchain-mijn-zorg-log, accessed 15-08-2017.

[10] Ito, J., Narula, N., Ali, R. (2017). *The Blockchain Will Do to the Financial System What the Internet Did to Media*. Harvard Business Review, 08-03-2017.

[11] Techruption website. URL: http://techruption.org/#about, accessed 17-3-2017.

[12] European Commission. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council* (General Data Protection Regulation). 27-04-2016.

[13] Vonne Laan. (2016). *Privacy, Security and Blockchain*. Van Doorne Blockchain Team.

[14] Deloitte Consulting LLP. (2016). *Blockchain: Opportunities for Health Care*. August 2016.

[15] Brodersen, C; Kalis, B; Leong, C; Mitchell, E; Pupo, E; Truscott, A. (2016). Blockchain: Securing a New Health Interoperability Experience.

[16] Nictiz. (2017). *Blockchain in de zorg.* 31-01-2017.

[17] McConaghy et al. (2016). *BigchainDB: A Scalable Blockchain Database*. 08-06-2016.

[18] Edquist, C. (1997). *Systems of Innovation: Technologies, Institutions & Organizations.* Routledge.

[19] Edquist, C. (2001). *The Systems of Innovation Approach and Innovation Policy: An account of the state of the art.* DRUID Conference, Aalborg, June 12-15, 2001.

[20] Janssen, M. (2016). *Situated Novelty: A study on healthcare innovation and its governance.*

[21] International Organization for Standardization. (2017). *ISO/IEC 24760-1:2011. Information technology -- Security techniques -- A framework for identity management -- Part 1: Terminology and concepts*

[22] Techopedia website. *Digital identity.* URL: https://www.techopedia.com/definition/23915/digital-identity, accessed 04-07-2017.

[23] Chew, M., Stamm, S. (2012). *Contextual Identity: Freedom to Be All Your Selves.*

[24] Wiedmann, K., Buxel, H., Walsh, G. (2002). *Customer profiling in e-commerce: Methodological aspects and challenges.* The Journal of Database Marketing 9, no. 2 (2002): 170-184

[25] Gaehtgens, F., Allan, A. (2017). *Digital Trust — Redefining Trust for the Digital Era: A Gartner Trend Insight Report*. 31 May 2017.

[26] Fleischhacker, N., Manulis, M., Azodi, A. (2014) *A Modular Framework for Multi-Factor Authentication and Key Exchange*. SSR 2014: Security Standardisation Research pp 190-21.

[27] Computer Security Resource Center website. *Attribute Based Access Control.* URL: https://csrc.nist.gov/projects/attribute-based-access-control, accessed 01-08-2017.

[28] IRMA website. https://privacybydesign.foundation/irma/, accessed 03-10-2017.

[29] Forum Standaardisatie. (2014). *Betrouwbaarheidsniveaus voor authenticatie bij elektronische overheidsdiensten (versie 3).*

[30] European Network and Information Security Agency. (2011). *Mapping security services to authentication levels.* 08 March 2011.

[31] KYCMap Website. Netherlands – Know Your Customer (KYC) Rules. URL: http://kycmap.com/netherlands-know-your-customer-kyc-rules/, accessed 23-07-2017.

[32] Ministerie van VWS. (2007). *Factsheet: Identificatie en opvragen BSN.* December 2007.

[33] Website Overheid.nl. Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg. URL: http://wetten.overheid.nl/BWBR0023864/2017-07-01

[34] Ecorys. (2016). *Business Case Inloggen in het BSN-domein.* 9 November 2016.

[35] Tobin, A., Reed, D., (2016). *The Inevitable Rise of Self-Sovereign Identity.* Sovrin Foundation whitepaper.

[36] CBS. (2017). *Cybersecuritymonitor 2017: Een eerste verkenning van dreigingen, incidenten en maatregelen.*
[37] Javelin Strategy. (2017). *Identity Fraud: Securing the Connected Life.*
[38] Florêncio, D., Herley, C. (2007). *A Large-Scale Study of Web Password Habits.* Microsoft Research.
[39] McDonald, A.M., Cranor, L.F. (2008). *The Cost of Reading Privacy Policies*. I/S: A Journal of Law and Policy for the Information Society.
[40] Dashline. (2015). Online Overload – It's Worse Than You Thought. URL: https://blog.dashlane.com/infographic-online-overload-its-worse-than-you-thought/
[41] TNS Opinion & Social [on behalf of the European Commission]. (2015). *Special Eurobarometer 431: Data Protection.*
[42] ID2020 website. URL: http://id2020.org/, accessed 03-09-2017.
[43] United Nations. *Sustainable Development Goals.* URL: https://sustainabledevelopment.un.org/sdg16, accessed 03-09-2017.
[44] Sullivan, C. (2011). *Digital Identity: An Emergent Legal Concept.* South Australia: University of Adelaide Press.
[45] Allan, C. (2016). *The Path to Self-Sovereign Identity*. Life with Alacrity. April 25 2016.
[46] Self-Sovereign Identity Framework consortium. (2017) *A Self-Sovereign Identity Framework (SSIF)*.
[47] Tobin, A., Reed, D., (2016). *The Inevitable Rise of Self-Sovereign Identity.* Sovrin Foundation whitepaper.
[48] Sovrin Foundation whitepaper. (2016). *The Technical Foundations of Sovrin.*
[49] Lundkvist, C., Heck, R., Torstensson, J., Mitton, Z., Sena, M. (2017). *uPort: A Platform for Self-Sovereign Identity*. Whitepaper 21-02-2017.
[50] Vlug, J. (2012). *DigiD: goed geregeld? Het verschijnsel DigiD rechtsstatelijk bekeken.* Digitale publicatiereeks Recht en Overheid 2012.
[51] eHerkenning website. URL: https://www.eherkenning.nl/inloggen-met-eherkenning/wat-is-eherkenning/, accessed 06-06-2017.
[52] Idensys website. URL: https://www.idensys.nl/over-idensys/, accessed 06-06-2017.
[53] iDIN website. URL: https://www.idin.nl/, accessed 06-06-2017.
[54] European Commission website. e-Identification. URL: https://ec.europa.eu/digital-single-market/en/e-identification, accessed 10-08-2017.
[55] European Commission website, *Trust Services and eID.* URL: https://ec.europa.eu/digital-single-market/en/trust-services-and-eid, accessed 10-08-2017.
[56] e-Estonia website. URL: https://e-estonia.com/solutions/healthcare/e-health-record/, accessed 25-09-2017.
[57] Cryptocoins News. *Dubai Set to Achieve Goal of Becoming First Blockchain Government by 2020.* 24-07-2017. URL: https://www.cryptocoinsnews.com/dubai-set-achieve-goal-becoming-first-blockchain-government-by-2020/
[58] Veenstra, S. (2017). *iDIN en Idensys: nieuwe identificatie diensten onder de loep.* 09-02-2017.
[59] Binnenlands Bestuur website.(2016). *Rekenkamer: Plannen eID-Stelsel Voldoen Niet*. URL: http://www.binnenlandsbestuur.nl/digitaal/nieuws/rekenkamer-plannen-eid-stelsel-voldoen-niet.9547018.lynkx, 08-09-2016
[60] UK Government Chief Scientific Adviser. (2016). *Distributed Ledger Technology: beyond block chain.* Government Office for Science.
[61] Ghosh, D. (2015) *How the Byzantine General Sacked the Castle: A Look Into Blockchain.* URL: https://medium.com/@DebrajG/how-the-byzantine-general-sacked-the-castle-a-look-into-blockchain-370fe637502c, accessed 02-10-2017.
[62] Antonopoulous, A.M. (2015). *Mastering Bitcoin: Unlocking digital cryptocurrencies.* O'Reilly Media.
[63] Schollmeier, R. (2002). *A Definition of Peer-to-Peer Networking for the Classification of Peer-to-Peer Architectures and Applications.* Proceedings of the First International Conference on Peer-to-Peer Computing, IEEE (2002).
[64] Tschorsch, F., Scheuermann, B. (2016). *Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies*. IEEE Communications Surveys & Tutorials, Vol. 18, No. 3, Third Quarter 2016.
[65] Ethereum Proof-of-Stake FAQ. URL: https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ, accessed 09-10-2017.
[66] Castro, M., Liskov, B. (1999). *Practical Byzantine Fault Tolerance.* Proceedings of the Third Symposium on Operating Systems Design and Implementation, New Orleans, USA, February 1999.
[67] Lamport, L., Shostak, R., Pease, M. (1982). *The Byzantine Generals Problem.* ACM Transactions on Programming Languages and Systems. 4 (3): 382–401.

[68] Coindesk (2016). Understanding the DAO Hack. URL: https://www.coindesk.com/understanding-dao-hack-journalists/, accessed 12-06-2017.
[69] BitInfoCharts website. URL: https://bitinfocharts.com/, accessed 29-09-2017.
[70] Visa Inc. (2017). *Visa Inc. Facts & Figures.* January 2017.
[71] Chaum, David (1983). *Blind signatures for untraceable payments.* Advances in Cryptology Proceedings of Crypto. 82 (3): 199–203
[72] Bitcoin Wiki. *E-gold*. URL: https://en.bitcoin.it/wiki/E-gold, accessed 19-08-2017.
[73] Coindesk. (2017). *Seeing Ghosts: Vitalik Is Finally Formalizing Ethereum's Casper Upgrade*. 07-09-2017.
[74] Ethereum website. URL: https://ethereum.org/, accessed 04-05-2017.
[75] Hyperledger website. URL: https://www.hyperledger.org/, accessed 04-05-2017.
[76] Gendal Brown, R., Carlyle, J., Grigg, I., Hearn, M. (2016). *Corda: An Introduction.* Whitepaper August 2016.
[77] Corda website. URL: https://www.corda.net/, accessed 09-10-2017.
[78] Orcutt, M. (2017). *How Blockchain Could Give Us a Smarter Energy Grid*. MIT Technology Review. 16-10-2017.
[79] Everex. *Blockchain-Powered Money Transfers and Microfinance Services.* URL: https://www.everex.io/, accessed 03-10-2017.
[80] Tsung-Ting Kuo, Hyeon-Eui Kim, Lucila Ohno-Machado. (2017). *Blockchain distributed ledger technologies for biomedical and health care applications.* Journal of the American Medical Informatics Association, Volume 24, Issue 6, 1 November 2017, Pages 1211–1220.
[81] ICTU. (2016). *Monitor Generieke Digitale Infrastructuur 2016.*
[82] Econlife. (2017). How Much Healthcare?. URL: https://econlife.com/2017/02/healthcare-coverage/, accessed 20-07-2017.
[83] Ministerie van Volksgezondheid, Welzijn en Sport. (2016). *Het Nederlandse Zorgstelsel.*
[84] Tandarts.nl. *De tandartstarieven in 2013*. URL: https://www.tandarts.nl/tandartstarieven/2013, accessed 03-07-2017.
[85] Nederlandse Zorgautoriteit. (2014). *Zorginkoop: Monitor en Beleidsbrief*. January 2014.
[86] Rabobank. (2017). *Rabobank Cijfers & Trends: Tandartsen en orthodontisten.* URL: https://www.rabobankcijfersentrends.nl/index.cfm?action=branche&branche=Tandartsen_en_orthodontisten, accessed 15-07-2017.
[87] Jarousse, L.A. (2013). *Accelerating patient-centered care.* Hospitals and Health Networks 87, No. 7: 53.
[88] Nederlandse Patiënten Consumenten Federatie. (2014). *Kwaliteitscriteria mondzorg: Geformuleerd vanuit patiëntenpespectief.*
[89] CZ groep. *Jaarverslag 2016*. 29 March 2017
[90] Mandl, K.D., Kohane, I.S. (2016). Patient demand for Patient-Driven Health Information. 9 May 2016. URL: https://catalyst.nejm.org/patient-demand-for-patient-driven-health-information/
[91] National Institutes of Health. *All of Us Research Program.* URL: https://allofus.nih.gov/, accessed 22-05-2017.
[92] Andreu-Perez, J., Leff ,D.R., Ip ,H.M., Yang, G.Z. (2015). *From Wearable Sensors to Smart Implants-–Toward Pervasive and Personalized Healthcare.* IEEE transactions on bio-medical engineering 2015 Dec; 62(12): 2750-62.
[93] Medical Identity Fraud Alliance.(2015). *Fifth Annual Study on Medical Identity Theft*, February 2015.
[94] Kruse, C.S., Frederick, B., Jacobson, T., Monticone, D.K. (2017). *Cybersecurity in healthcare: A systematic review of modern threats and trends*. Technology and Health Care, vol. 25, no. 1, pp. 1-10, 2017
[95] Eerste Kamer der Staten-Generaal. (2011). *Eerste Kamer verwerpt unaniem voorstel landelijk EPD.* URL: https://www.eerstekamer.nl/nieuws/20110405/eerste_kamer_verwerpt_unaniem
[96] Innovalor website. URL: https://innovalor.nl/personal-data-store/, accessed 20-09-2017.
[97] EU GDPR Portal. URL: http://www.eugdpr.org/, accessed 13-06-2017.
[98] Conway, S., Steward, F. (2009). *Managing and Shaping Innovation*. Oxford University Press.
[99] Kalbach, J. (2012). Clarifying Innovation: Four Zones of Innovation. URL: https://experiencinginformation.com/2012/06/03/clarifying-innovation-four-zones-of-innovation/, accessed 13-06-2017.
[100] Himmelstein, D.U., Jun, M., Busse, R., Chevreul, K., Geissler, A., Jeurissen, P., Thomson, S., Vinet, M., Woolhandler, S. (2014). *A Comparison Of Hospital Administrative Costs In Eight Nations: US Costs Exceed All Others By Far*. Health Affairs 33, No. 9 (2014)

[101] Van Zuidam, R. (2016). *Government-as-a-Service: Het nieuwe Nederlandse exportproduct*. DutchChain whitepaper.
[102] Bloomberg. (2016). These Ten Countries Are The Most Globally Connected. URL: https://www.bloomberg.com/news/articles/2016-02-25/these-ten-countries-are-the-most-globally-connected, accessed 18-09-2017.
[103] Global News website. Canada back on top of world's most reputable countries list. URL: https://globalnews.ca/news/3567232/canada-back-on-top-of-worlds-most-reputable-countries-list/, accessed 18-09-2017.
[104] Dutch Government Blockchain Projects website. URL: https://www.blockchainpilots.nl/, accessed 02-10-2017.
[105] Rijksoverheid website. *Digitale overheid.* URL: https://www.rijksoverheid.nl/onderwerpen/digitale-overheid/veilig-makkelijk-inloggen-overheidswebsites, accessed 11-09-2017.
[106] Gartner. (2016). *Gartner Says Worldwide Information Security Spending Will Grow 7.9 Percent to Reach $81.6 Billion in 2016.* August 9, 2016.

Appendices

Appendix A -- List of interviewees

Healthcare professionals

Interviewee	Job title (Company type)	Date of interview
Participant A1 Participant A2	Applications specialist (Department of Dentistry of a university medical center)	19-7-2017
Participant B1 Participant B2	Policy officer central care administration Project manager (Hospital)	20-7-2017
Participant C	Dentist (Solo practice)	24-7-2017
Participant D	Dentist (Group practice/dental chain)	26-7-2017
Participant E	Security officer (Diagnostics center)	27-7-2017
Participant F	Professor of Quality and Safety of Oral Care (Dental faculty of a university)	24-8-2017
Participant G	Dentist/professor (group practice/dental faculty of a university)	30-8-2017
Participant H	Operational director (dental chain)	5-9-2017

Blockchain experts

Interviewees	Job title (Company)	Date of interview
Participant V	Innovation Lab (Chamber of Commerce)	22-8-2017
Participant W	Project manager/consultant blockchain (Bank)	25-8-2017
Participant X	Teamlead Demand and Portfolio management IAM (Bank)	8-9-2017
Participant Y	Strategy consultant (Pension provider)	13-9-2017
Participant Z	Innovation manager (Bank)	15-9-2017

Appendix B -- Interview guides

The here mentioned interview guides were loosely followed during the interviews. Interviews were held in Dutch. Likewise, interview guides were composed in this language.

Healthcare professionals

Goals:
- Clarification of the current structure of various identification and data processes.
- Measuring familiarity with and urgency of privacy and identity issues.
- Determining the vision of healthcare providers on the added value of self-sovereign identity in healthcare.

No.	Question	Subject
1	Who are you and what are your primary activities?	Acquaintance
2	What do you know of the impending GDPR legislation?	Privacy legislation
3	How is your organization preparing for the new privacy legislation? - Why?	GDPR
4	What are the most important requirements an identity system must satisfy? (notions: privacy, security, performance, data ownership, scalability)	Requirements
5	When a patient registers with you for the first time: what personal or medical information must he deliver? - What constitutes the medical health record? - How does identification go at follow-up appointments? - Do you have additions/corrections to this process scheme?	Process: identification
6	How do you use data during treatment of a patient?	
7	How do you manage your own personal attributes? (Patient records, AGB-codes, certifications) - Who has access to which data? - Do you have insight in who has access to which data?	Proces: data management
8	What is your opinion about the data exchange with VECOZO and health insurance companies? (speed, security, amount/efficiency)	Proces: data exchange
9	How do you inform patients and health insurers on treatments specifics and costs?	Transparency
10	What are the issues with the current identity system? (fraud, bureaucracy, costs, no transparency)	Summarizing: issues
11	What kind of factors play a role in the acceptance of a new identity system by you and your patients?	Technology acceptance
12	Is a system based on self-sovereignty possibly appropriate for identification in healthcare? - Why/why not?	Estimation of added value SSI
13	What are, at first glance, strengths and weaknesses of this new system?	Use case SSI

<u>Blockchain experts</u>

Goals:

- Validating wishes and opinions of healthcare providers.
- Estimation of potential for self-sovereign identity in healthcare.
- Assess compliance blockchain with privacy legislation.
- Determine if and how blockchain is essential in the system.

Nr.	Vraag	Onderwerp
1	Who are you and what are your primary activities? - What is your link with blockchain and self-sovereign identity?	Acquaintance
2	On what aspects can blokchain offer added value in terms of identity? - Privacy, efficiency, security?	Blockchain strengths and weaknesses Important aspects ID-system.
3	What do you know about the coming European GDPR regulation? (in this case related to medical data)	Privacy legislation
4	Are blockchain and GDPR reconcilable? - If not, what will this mean for the future?	Blockchain, privacy legislation

5	To what extent are you familiar with identification processes in healthcare? - Explanation	Healthcare context
6	Should healthcare organizations and insurance companies already actively involve in blockchain innovation?	Innovation roles
7	To what extent are your familiar with self-sovereign identity? - Explanation	SSI
8	What are your expectations regarding SSI? - Will it become a standard way of identification? - What is the goal of SSI?	SSI scope
9	Are systems based on attestations potentially valuable for identification in healthcare? - Why/why not?	SSI in healthcare
9	Is blockchain technology essential for such a system?	Role blockchain
10	What type of blockchain platform would be best suited for facilitating such an identity system?	Platform
11	What should governance of such a system look like?	Governance.