Master's thesis

NTNU
Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Department of Computer Science

Eivind Solberg Rydningen, Erika Åsberg

Exploring the IOTA Tangle for Health Data Management

Master's thesis in Informatics
Supervisor: Letizia Jaccheri
Co-supervisor: Marte Hoff Hagen

June 2022

NTNU
Norwegian University of
Science and Technology

Eivind Solberg Rydningen, Erika Åsberg

Exploring the IOTA Tangle for Health Data Management

Master's thesis in Informatics
Supervisor: Letizia Jaccheri
Co-supervisor: Marte Hoff Hagen
June 2022

Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Department of Computer Science

NTNU
Norwegian University of
Science and Technology

Abstract

Context: The IOTA Tangle is a distributed ledger designed for the Internet of Things that presents new possibilities for innovation in health data management. The possibilities may include improved interoperability between hospitals, secure and private data storage solutions, and immutable and tamper-proof communication of data.

Objective: The objective is to demonstrate how the IOTA Tangle can provide reliable and secure health data management, and how it should be implemented.

Method: A systematic mapping study was conducted to investigate the literature on the research topic. Additionally, two experts were interviewed and a prototype development and evaluation process was conducted. The prototyping applied a design and creation approach, including two iterations of development and subsequent testing.

Results: The results indicate that the IOTA Tangle can provide reliable and secure health data management through its unique directed acyclic graph data structure and the IOTA Streams tool. Further, a Rust prototype successfully demonstrated the steps necessary to exchange private health data from an Author to one or several Subscribers. Finally, the results provided regulatory, design, and technical guidelines for implementation.

Conclusion: The research concludes that the IOTA Tangle has potential for health data management, and the successful prototype demonstration confirms that it is feasible. The main limitation of the research is the scope of the prototype. Future research could build on the knowledge regarding how to improve and implement health data management systems with the IOTA Tangle.

Keywords: *Health Data Management, Internet of Things, Distributed Ledger Technology, Blockchain, IOTA Tangle, IOTA Streams, Systematic Mapping Study, Software Engineering*

Sammendrag

Kontekst: IOTA Tangle er en distribuert hovedbok designet for Tingenes Internett som presenterer nye muligheter for innovasjon innen helsedatahåndtering. Mulighetene kan omfatte forbedret interoperabilitet mellom sykehus, sikre og private datalagringsløsninger, og uforanderlig og manipulasjonssikker kommunikasjon av data.

Målsetting: Målet er å demonstrere hvordan IOTA Tangle kan gi pålitelig og sikker helsedatahåndtering, og hvordan dette bør implementeres.

Metode: Det ble gjennomført en systematisk kartleggingsstudie for å undersøke litteraturen om forskningstemaet. I tillegg ble det gjennomført to ekspertintervjuer og en prototypeutviklings- og evalueringsprosess. Prototypingen brukte en design- og utviklingstilnærming, inkludert to iterasjoner av utvikling og påfølgende testing.

Resultater: Resultatene indikerer at IOTA Tangle kan gi pålitelig og sikker helsedatahåndtering gjennom sin unike rettede asykliske graf datastruktur og IOTA Streams verktøyet. Videre demonstrerte en Rust-prototype de nødvendige stegene for å dele privat helsedata fra en *Author* til en eller flere *Subscribers*. Resultatene gir regulatoriske, design og tekniske retningslinjer for implementering.

Konklusjon: Forskningen konkluderer med at IOTA Tangle har potensial for helsedatahåndtering, og den vellykkede prototypedemonstrasjonen bekrefter at det er gjennomførbart. Hovedbegrensningen for forskningen er omfanget av prototypen. Fremtidig forskning kan bygge på kunnskapen om hvordan man forbedrer og implementerer helsedatahåndteringsystemer med IOTA Tangle.

Nøkkelord: *Helsedatahåndtering, Tingenes Internett, Distribuert Hovedbok-teknologi, Blokkjede, IOTA Tangle, IOTA Streams, Systematisk Kartleggingsstudie, Programvareutvikling*

Preface

This Master's thesis is written by two students at the Norwegian University of Science and Technology (NTNU), as part of the course IT3920 Master in Informatics. The research has been performed at the Department of Computer Science, NTNU, Trondheim, supervised by Professor Letizia Jaccheri and co-supervisor PhD Candidate Marte Hoff Hagen.

Acknowledgement

We would like to grant a special thanks to our magnificent supervisor Professor Letizia Jaccheri for excellent guidance and feedback. We would also like to thank our brilliant co-supervisor Marte Hoff Hagen for her support and outstanding help throughout this project. Lastly, we would like to thank J. David Patón-Romero for assisting our research.

Contents

Figures

Tables

Code Listings

Acronyms

CE Conformité Européenne. 32, 73, 80

DAG Directed Acyclic Graph. 9, 26, 29, 30, 69, 70, 79

DLT Distributed Ledger Technology. 1, 2, 5, 7, 8, 12, 29, 30, 70, 71

EHR Electronic Health Record. 5, 6, 69, 71

EMR Electronic Medical Record. 5, 6

GUI Graphical User Interface. 54, 55

IDE Integrated Development Environment. 53

IoMT Internet of Medical Things. 7, 26, 27, 72, 73

IoT Internet of Things. 1, 2, 5, 7, 26–30, 72

ISO Organization for Standardization. 32, 73, 80

M2M Machine-to-Machine. 28, 30

MAM Masked Authenticated Messaging. 26, 27, 30, 70, 72, 73

NSD Norwegian Center for Research Data. 19

PHR Personal Health Record. 5, 6, 71

RQ research question. xv, 12, 13, 21, 24, 26, 73

RQs research questions. 1–3, 11, 12, 14, 17, 21, 37, 41, 69, 73, 79

SMS Systematic Mapping Study. 1–3, 11, 12, 15, 21, 26, 30, 41, 69–73, 77, 79

Glossary

IOTA An open-source distributed ledger and cryptocurrency designed for the Internet of Things (IoT). 2, 30–36

IOTA Streams Streams is an organizational tool for structuring and navigating secure data through the IOTA Tangle. 5, 10, 26, 41, 52–54, 58, 70, 72, 74–77, 79, 80

IOTA Tangle An innovative type of distributed ledger technology (DLT) that is specifically designed for the Internet of Things (IoT) environment. xiv, xv, 1–3, 5–10, 12, 15, 18, 26–30, 32, 33, 37, 41, 52, 58, 66, 67, 69–77, 79–81

Chapter 1

Introduction

This master's thesis is part of the project *Software for a Better Society*, led by Professor Letizia Jaccheri, where the goal is to establish new knowledge regarding how technological advances impact various aspects of society. The overall target of this thesis is to develop software for inclusion using cutting edge technology. The aim is to demonstrate how health data management can become reliable and secure with the IOTA Tangle, integrated with Internet of Things (IoT) technology. The following research consists of a Systematic Mapping Study (SMS), expert interviews, and a prototype development process, looking to answer if the findings supports this goal.

The introduction contains four subsections; Section 1.1 presents the motivation behind this project, Section 1.2 presents the research questions (RQs), Section 1.3 defines the research objective, and finally, Section 1.4 outlines the rest of the thesis.

1.1 Motivation

IoT and Distributed Ledger Technology (DLT) together represent a new paradigm in Information Technology and present new innovation opportunities. Both avenues have been discussed for some time, however the combination of the two is rather novel. Lund et al.[1] conducted a SMS on DLT and sustainability that focused on smart grids and supply chains, and found that very few papers described real-world implementation experiences. It is asserted that most research in this field is still discussing how to implement practical use cases. The novelty of DLT and IoT technology, and especially the novelty of them combined, drives the desire to explore and advance this field.

Another key motivation is the work of Farahani et al. [2], which examined the opportunities and challenges of IoT and DLT convergence. This study argues that DLT has the potential to address several issues found in traditional Cloud/IoT systems, such as security- and interoperability issues, while also offering new benefits like scalability, immutability, and traceability. While there currently exists thousands of cryptocurrency projects, DLT is still in its infancy and more research is needed in order to fully exploit the opportunities.

The IOTA Tangle, which will be presented in Chapter 2, is one of the DLT projects developed with the IoT in mind. It aims to provide a sustainable and lightweight network solution that scales to accommodate transactions between the millions, maybe billions, of devices that is going make up IoT in the coming years.

The monitoring of a diabetic patient's blood glucose levels is a practical example of how IoT, DLT, and health data can be combined. A sensor worn by the patient would collect blood glucose data and periodically send it over the IOTA network. The data could be shared with authorized personnel, such as a general physician or an endocrinologist. Further, information regarding the patient, such as their medical history, prescriptions and test results, is then stored securely and privately on the IOTA network. In essence, this would lead to a more accessible, interoperable platform to manage patients' health data both for the patient and the caregiver. This could decrease fragmentation of data between various storage solutions and open up the possibility of real-time monitoring and data analysis. A motivating demonstration of an IOTA based health data management system was developed by Hawig et al. [3].

1.2 Research Questions

This thesis seeks to answer questions related to implementation of the IOTA Tangle in the health care sector and how this could be beneficial. The investigation is divided into two aspects. The first aspect looks into answering how and if the IOTA Tangle could become a solution for health data management systems. The second aspect explores how to implement this technology in a real life system. Based on these descriptions, the following RQs were formulated:

- **RQ1: How can the IOTA Tangle provide reliable and secure health data management?**
- **RQ2: How should a health data management application built with the IOTA Tangle be implemented?**

The IOTA Tangle will be explained in detail in the background, Section 2.4.5. RQ1 is answered by a preliminary SMS conducted during the fall of 2021 along with knowledge collected from expert interviews. RQ2 is answered by a prototype development process involving two iterations of development and testing.

1.3 Objective

This research project aims to present several aspects of developing a health data management application prototype with the use of the IOTA Tangle. Among these aspects are regulatory, design, and technical considerations. Through conducting a SMS and expert interviews the research will answer whether or not the IOTA Tangle is suitable for a health data management prototype. Based on this knowledge, prototype development with usability testing and functional testing will be conducted to answer to how a health data management application built with the IOTA Tangle should be implemented. The final goal of the research is to present a prototype that people can use to monitor, collect, and securely share their health data with authorized parties.

1.4 Outline of Thesis

This thesis consists of nine chapters. Chapter 1 introduced the motivation, RQs, and objective of the research project. In Chapter 2 the background and key concepts relevant to the research topic are presented. Chapter 3 explains and justifies the research method. Chapter 4 summarizes the literature review, conducted as a SMS during the fall of 2021. Chapter 5 presents the expert interviews. In Chapter 6 the development process of the prototype is presented as two iterations of development and testing. Chapter 7 presents an outline of the results collected from each prototype development iteration. Chapter 8 discusses the RQs in perspective of all the information gathered from the research. Lastly, Chapter 9 presents the conclusion of the thesis.

Chapter 2

Background

This research exists in the convergence of DLT and IoT, and their potential for improving health data management. The following chapter establishes a foundation of knowledge and concepts relevant to the research. It is divided in four main topics, as illustrated in Figure 2.1. The IOTA Tangle is the main topic of investigation for this research and forms the bridge between the topics of DLT, IoT, and health data management. Health data management and IoT is connected through Internet of Medical Things (IoMT), which is medical IoT devices that measure health indicators in patients. The use of DLT may improve health data management systems through security and privacy, while the combination of DLT and IoT may improve interoperability and scalability.

Initially the Background chapter presents the topic of health data management in Section 2.1, followed by an introduction to the IoT and smart health devices. Section 2.4 outlines what DLT is and its main features, which is then followed by a description of blockchain, the IOTA Tangle and IOTA Streams. Finally, Section 2.5 summarizes the chapter.

2.1 Health Data Management

Three data storage options for health data are available in the market today; Personal Health Record (PHR), Electronic Health Record (EHR), and Electronic Medical Record (EMR) [5]. With PHR, the patients can access and control their own generated health data and functions as a personal data storage. EHR and EMR, on the other hand, are used and managed by medical professionals, such as physicians. The main difference between these two is that EMR is for internal use in a single institution, while an EHR is meant to be shared across multiple institutions.

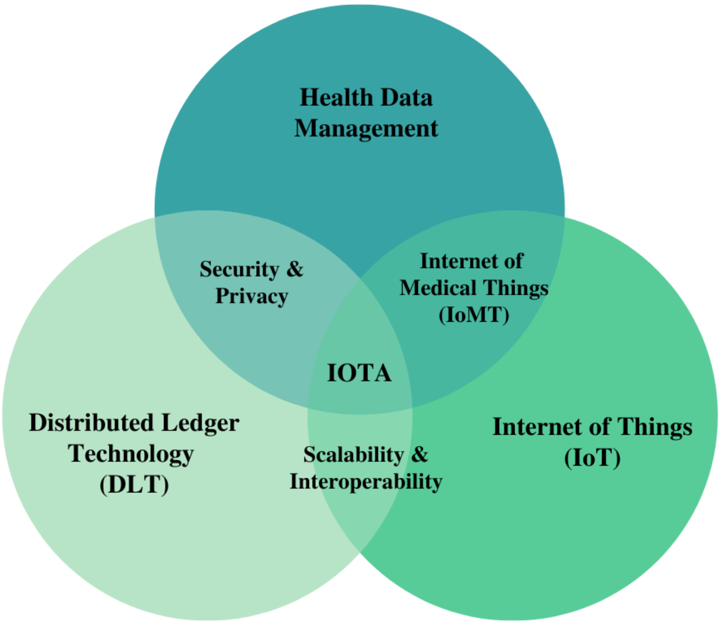

Health Data Management
Security & Privacy
Internet of Medical Things (IoMT)
IOTA
Distributed Ledger Technology (DLT)
Scalability & Interoperability
Internet of Things (IoT)

Figure 2.1: Diagram of the main topics in the background and their relation to each other, Rydningen and Åsberg [4].

Developing countries are increasingly implementing EHRs as a replacement for health records on paper according to Jamshed et al. [6]. The advantages of this transition is that medical records become more flexible and accessible, with improvements in the quality of care as well as lower costs. However, the main disadvantage is that EHRs may be vulnerable to privacy abuse and may be accessed by malicious actors if they are not stored securely.

The ethical priorities for EHRs; Privacy and confidentiality, security, preventing data inaccuracies and ensuring good system implementation are described by Jamshed et al. [6]. To ensure privacy and confidentiality, access to the health data need to be strictly controlled, in addition, the records must have strong privacy and security policies. To reduce the risk of security breaches an EHR should implement antivirus software, intrusion detection, firewalls, and strict procedures for the management of the data, in order to maintain the integrity of the EHR. System implementation is important because the system needs to have an intuitive user interface, and all stakeholders need to be well informed of how the system works and best practices need to be standardized. These steps reduce the chance of data inaccuracies due to reduced risk of user error. Data inaccuracies may also occur in the transfer of data, therefore, the transfer needs to be tamper-proof, immutable and secure.

Figure 2.2 illustrates what combining all patient data in an interoperable system, built with the IOTA Tangle, could look like. In other words, the idea is to research the potential of the IOTA Tangle to combine the concepts of PHR, EHR, and EMR together into one system. Data from smart health devices, health records from your physician, results from laboratory tests and prescriptions would be accessible, secure and interoperable.

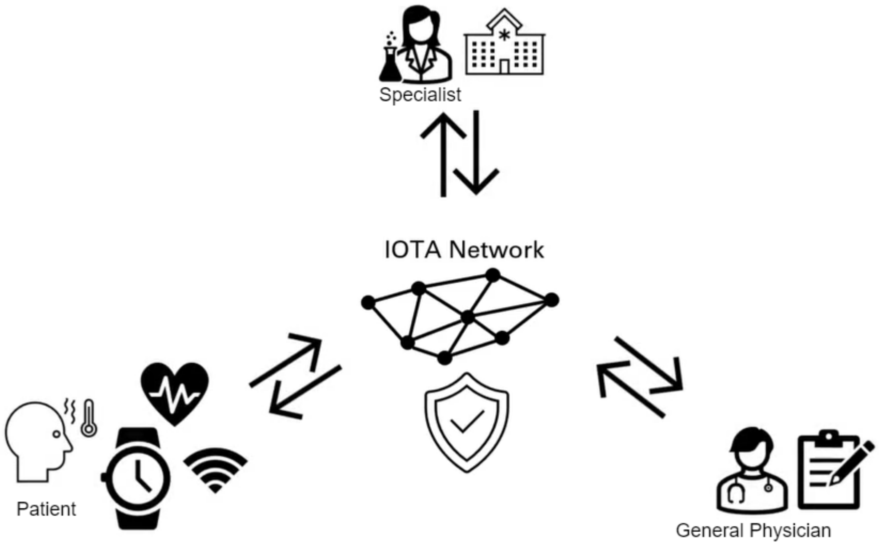


Figure 2.2: Illustration of health data management with the IOTA Tangle.

2.2 Internet of Things

The IoT is when physical objects with processing ability, sensors and software, are connected to the internet and exchange data with other devices. The concept of the IoT is not a new idea [7], but it is not until recently that it has seen broader adoption due to advances in technologies such as embedded computers and sensors, as well as improvements in bandwidth and connectivity over wireless networks [8]. Today, IoT technology is adopted in several sectors, such as smart homes, wearable sensors, industrial production and weather data collection [9].

2.3 Smart Health Devices

A sector that has increasingly adopted IoT technology is the healthcare sector. Smart IoT devices are now used to measure health indicators in patients, such as heart rate, blood glucose levels and respiratory rate. When IoT devices are used in a medical setting it is by some referred to as the Internet of Medical Things (IoMT) [10]. Although sensors are not new to healthcare, connecting them to the internet enables new opportunities like remote patient monitoring and real-time health data analysis. It may also contribute to defragmentation of patient health data, which may typically be stored across various databases, devices and paper records [11]. As the exchange of health data between sensors and devices becomes easier, data is also more accessible to different stakeholders, but this interoperable exchange of data does not come without security and privacy risks. The following section introduces DLT, which may assist in resolving some of the potential risks [11].

2.4 Distributed Ledger Technology

A distributed ledger is a type of database that is replicated across multiple locations, and participants in the network collaboratively reach consensus on the state of the network [12]. The technology enables users to exchange and store data securely by applying cryptography. Cryptography is a secure communication technique using public and private keys to encrypt and decrypt messages, in order to only allow the sender and intended receiver of a message to view it. The following sections discusses decentralization, immutability and interoperability, which are three important aspects of DLT. Then follows a description of blockchain and finally an introduction to the IOTA Tangle, which are both examples of DLTs.

2.4.1 Decentralization

Decentralization is a central concept in DLT. Distributed ledgers are managed and secured in collaboration by multiple participants instead of a central administrator [12]. Each transaction is stored as a record in the distributed ledger and this record of the network state is stored in every participating node. This is in contrast to traditional database architectures, where data is controlled and stored by a central authority, such as Google or Amazon Web Services.

The main advantages of DLT is that all participants are equal and no single actor in the network can shut it down or sabotage it. In addition, there is no single point of failure in a decentralized network, if one node loses its data record, every other node holds a copy and the data is therefore not lost. This makes it harder for attackers, since it is not enough to infiltrate one node to control the network. Network integrity is maintained since every transaction is validated by potentially thousands of nodes [13].

2.4.2 Immutability

Immutability is an important trait of DLT. Immutability means that once a transaction is validated by the network participants and stored on the distributed ledger, it cannot be altered or reversed. Therefore, a DLT has a single "source of truth". Modifications to the ledger record that do not comply with the network protocol are immediately revealed and rejected [13].

2.4.3 Interoperability

Interoperability revolves around the ability of multiple systems to exchange data between each other. DLTs can act as a bridge between systems so that they can securely exchange data, and by enabling interoperable communication new use cases may be realized [14].

2.4.4 Blockchain

Blockchain is an example of DLT that records transactions. With blockchain, transactions are stored in groups called blocks and each block is connected to, or chained to, the hash of the previous block. The blockchain structure is the most common architecture used in the DLT space today [15]. With blockchain you typically separate between two types of participants, users, or devices that want to send or receive transactions, and users that lend processing power to solve cryptographic puzzles that are essential to securing the ledger. The latter are often referred to as miners. Therefore, users that want their transactions processed in the network must pay a fee to the miners. Bitcoin and Ethereum are the two blockchain based cryptocurrencies with the highest market capitalization according to CoinMarketCap [16].

2.4.5 IOTA

The IOTA network protocol, is developed by the IOTA Foundation, which is a not for profit foundation. The official IOTA website describes it as a scalable, open source communication protocol. Their goal is to develop a system for transaction and data exchange for the IoT. To achieve this the Foundation has focused on creating a ledger that is fast, scalable and where users can send transactions without having to pay fees to miners [17].

IOTA Tangle

The IOTA Tangle is the architecture developed by the IOTA Foundation and is characterized by its unique Directed Acyclic Graph (DAG) structure, which is a data structure where each transaction on the ledger refers to two or more previous transactions, whereas blockchain only refers to the previous block. If a user wants to issue a transaction over the IOTA Tangle, they must first contribute in the validation of previous transactions. Since users that want to utilize the network must also assist others in utilizing the network, it can operate without the need for miners. Since the system has no miners that expect a reward for their contribution, the network can operate without transaction fees. Figure 2.3 illustrates the difference in data structure between blockchain and the IOTA Tangle. Each block is a transaction and the arrows indicate which previous transaction it references. The DAG structure allows for transactions to be processed in parallel, which contributes to the efficiency and scalability of the ledger.

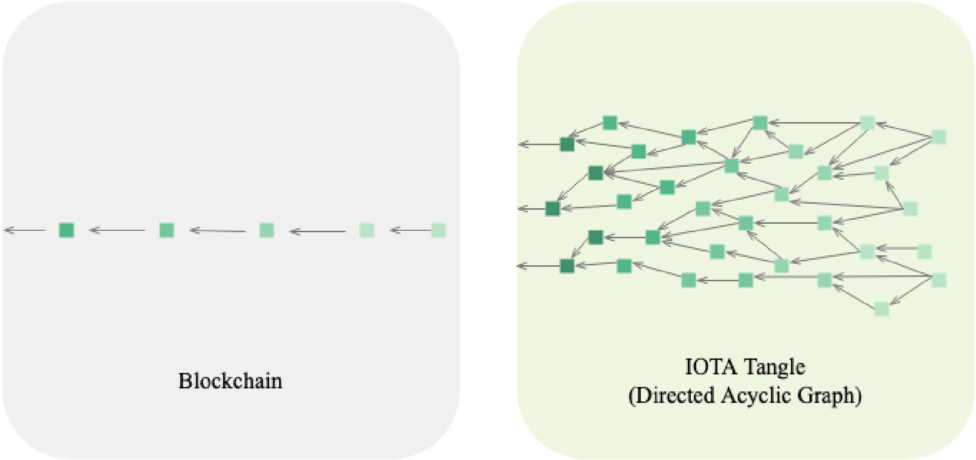


Figure 2.3: Blockchain compared to the IOTA Tangle. Adapted from CryptoMarketsWiki [17].

IOTA Streams

In order to realize data sharing between authenticated and authorized parties over the IOTA Tangle, the IOTA Foundation has developed the IOTA Streams organizational tool, previously known as Masked Authenticated Messaging (MAM). It makes it possible to structure and publish encrypted data on the IOTA Tangle in channels known as Streams. The publisher of the data determines which users can access the data, and data authenticity is guaranteed since all branches of a Stream reference a common root branch connected to the the original publisher. Publishers can either send non-encrypted data that is public or restrict access using public key encryption. Subscribers can fetch data as well as contribute to different Streams on the IOTA Tangle. Establishing a data stream between two parties is similar to a three-way handshake [18]. IOTA Streams is a central component for the realization of decentralized health data management with the IOTA Tangle. The tool is available as open source libraries written in Rust, C or WebAssembly.

2.5 Conclusion

The background chapter serves as a basis of knowledge and assists in connecting the topics of health data management, the IoT, DLT and the IOTA Tangle. One of the major issues in health data management today is that data is fragmented across multiple sources and that there is little interoperability between medical institutions. Using a distributed network, such as the IOTA Tangle as a secure communications layer may contribute to more efficient, secure and interoperable health data management systems.

Chapter 3

Research Method

This chapter is mainly inspired by the book of Oates [19]. It specifies the importance of defining how research can contribute to knowledge, and defines three roles a research project can approach; 1) The IT product itself is a contribution, 2) the IT product is a vehicle for something else, or 3) the IT product is a tangible end-product, but the contribution lies in the development process. Our project falls under the "vehicle for something else" role. The contribution to knowledge is based on a SMS, expert interviews and a prototype development and evaluation process.

This chapter presents the research method, describing the process in general, data gathering methods, and data analysis. Further, the chapter introduces the participants and ethics related to the project, and explains how the research data is collected and stored.

3.1 Process

The initial phase of the process occurred during the fall semester of 2021, consisting of experiences, motivation, and a literature review. The literature review was conducted as a SMS [4], establishing a foundation to answer the RQs, recall Section 1.2. An overview of the complete research process is presented in Figure 3.1. The chosen path for the process is marked in green.

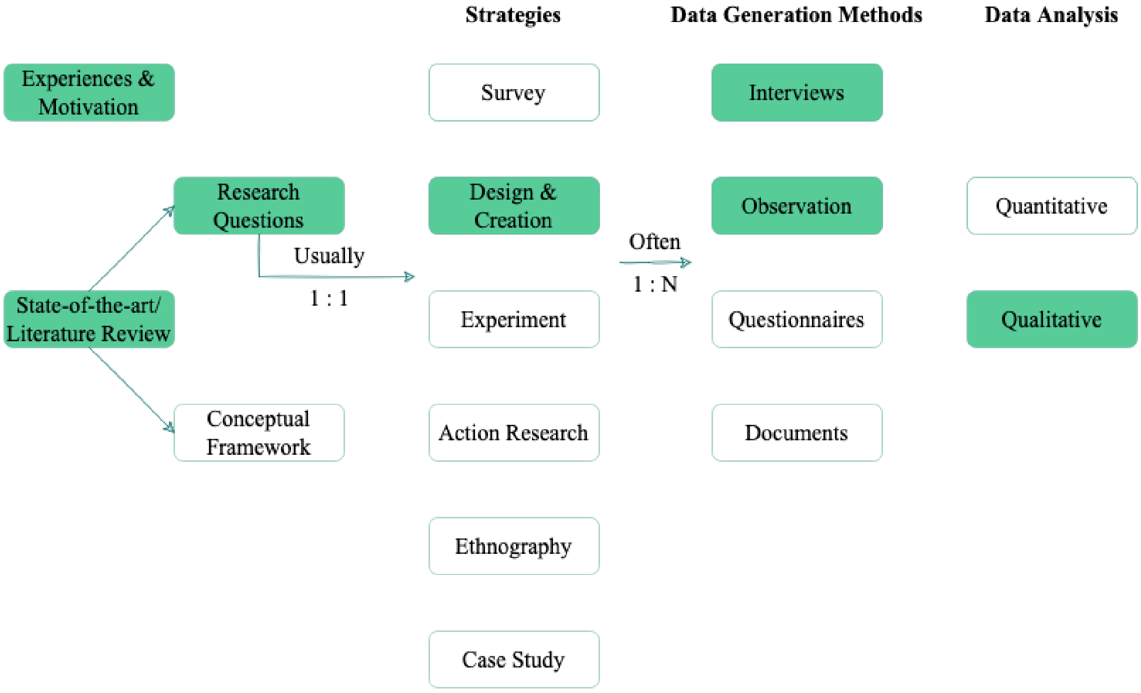


Figure 3.1: Research process diagram. Adapted from Oates [19].

3.1.1 Systematic Mapping Study

This section presents the method used in the SMS, however the findings are presented in Chapter 4. The guidelines of Kitchenham [20], alongside the work of Budgen et al. [21], Petersen et al. [22], and Berg et al. [23], were used as inspiration for the literature review.

The SMS aimed to gain meaningful insight and gather existing research on the research topic. The relationship between DLT, such as the IOTA Tangle, and health data management was the specific research topic for this SMS. Thus, two RQs were established for the SMS:

- **RQ1:** How can the IOTA Tangle provide reliable and secure health data management?
- **RQ2:** What are the advantages and disadvantages of using the IOTA Tangle compared to other potential Distributed Ledger Technologies?

A search strategy, including search strings, selection criteria, quality assessment, and data analysis, was conducted to gather relevant research related to the RQs. The search strings correspond to each RQ and were applied to four different online databases; Scopus, IEEE, Springer Link, and Science Direct. A summary of the number of hits each search string generated is presented in Table 3.1. The total number of hits was 1190.

Related RQ	Online Database	Search string	Number of Hits
RQ1	Scopus, IEEE, Springer Link and Science Direct	"TITLE-ABS-KEY ((iota) AND (health*) AND (data OR priva* OR secur*)) AND PUBYEAR > 2009"	416
RQ2	Scopus, IEEE, Springer Link and Science Direct	"TITLE-ABS-KEY (distributed ledger technology OR DLT) AND (blockchain) AND (DAG OR tangle OR iota) AND (compar* OR review)) AND PUBYEAR > 2009 "	774
		Total number of hits	**1190**

Table 3.1: Search strings applied to four different online databases, Rydningen and Åsberg [4].

After applying the selection criteria and quality assessment to the 1190 articles retrieved from the initial search, the number of relevant papers decreased to 17 primary studies, as illustrated in Figure 3.2. Scopus covered eight of the primary studies, IEEE and Science Direct covered four each, and Springer Link covered one.

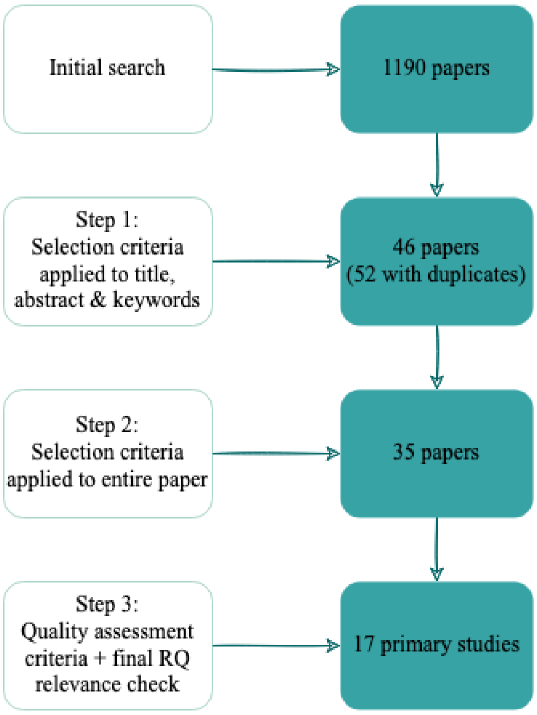

Initial search
1190 papers
Step 1: Selection criteria applied to title, abstract & keywords
46 papers (52 with duplicates)
Step 2: Selection criteria applied to entire paper
35 papers
Step 3: Quality assessment criteria + final RQ relevance check
17 primary studies

Figure 3.2: The selection process of relevant articles, Rydningen and Åsberg [4].

The data extraction from the 17 remaining articles included author, year of publication, type of publication channel (journal, conference, etc.), related RQ, methodology (qualitative, quantitative, or mixed), data analysis, and the main findings.

3.1.2 Design and Creation

The design and creation strategy was a proper fit for this thesis in order to answer the RQs. Oates describes design and creation as a strategy that "focuses on developing new IT products, or artefacts. Often the new IT product is a computer-based system, but it can also be some element of the development process such as a new construct, model or method" [19]. This definition is compatible with what was accomplished in this research project; developing a health data management prototype.

A typical design and creation approach, adapted from Vaishnavi and Kuechler [24], is an iterative process using five steps, illustrated in Figure 3.3. These steps form a cycle with repeating steps. The results and knowledge gathered from one iteration will be helpful in the next iteration.

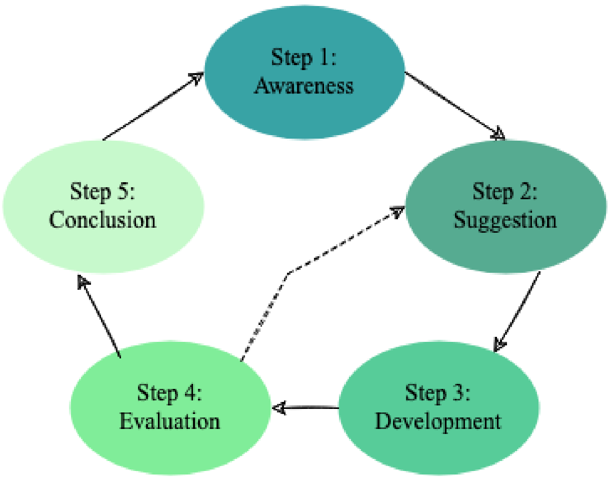


Figure 3.3: Five steps used in iterative process in design and creation strategy. Adapted from Vaishnavi and Kuechler [24].

To explain Figure 3.3, *Step 1: Awareness* is about recognizing and stating the problem. Further, *Step 2: Suggestion* is the step where an idea on how the problem can be addressed is figured out. In *Step 3: Development*, implementation of a tentative prototype design is conducted, followed by *Step 4: Evaluation*, which collects and examines the results of the developed prototype. Lastly, *Step 5: Conclusion* contributes with the knowledge gained from the process. Step 1 and step 5 are often used once during a design and creation process, as the initial and ending phase of the entire process. After step 4, the information and results gathered are brought back to step 2 for another round of suggestion.

The aim was to iterate as many times as possible, but due to the limited amount of time, it was only possible to conduct two iterations. The first iteration consisted of developing and evaluating a design prototype in Figma, see Section 6.1. This iteration was evaluated through usability testing and individual interviews. The outcome of the first iteration formed a basis for the second iteration, planned to be the development and evaluation of a mobile application prototype. Adjustments had to be made in terms of the development of this prototype. Although the plan was to perform similar evaluation as in the first iteration, functional testing was considered sufficient since the prototype was primarily developed to demonstrate that health data management is possible with the IOTA Tangle.

3.1.3 Data Generation Methods

The chosen strategy, design and creation, was supported by two different data generation methods; interviews and observation. Two different types of individual interviews were conducted. The first type was the expert interviews, the second was a follow-up interview after the observation.

Using two, or more, data generation methods is referred to as method triangulation. Method triangulation is used to "corroborate findings and enhance their validity" [19], explore several perspectives, and generate more data to improve the quality of research. This section provides an overview of the data generation methods used in this project, with a focus on how they were conducted and what purposes they served.

Expert Interviews

The expert interviews belongs to step 1 and 2 of the five step iteration process in Figure 3.3. It worked as an extension of the SMS and the aim of the expert interviews was gain valuable knowledge on the research topic ahead of developing the prototype. It was essential to run these at the beginning of the project and get an overview, as it is a complex research topic to investigate.

The interviews were semi-structured. The aim of semi-structured interviews is for the interviewee to be able to speak more in detail regarding the issues raised, and bring up issues they find relevant [19]. A set of general questions was created, but they were written as open-ended as possible to allow the participants to answer as freely as possible. It was desired to have the ability to ask follow-up questions, which semi-structured interviews facilitate.

Two expert interviews were conducted and they lasted between 30 to 45 minutes. They were both performed online over Zoom, and the calls were recorded with a built-in recorder. The interviews were then transcribed ahead of being analyzed. The findings from the interviews are summarized and presented in Chapter 5.

Observation

Usability testing was used as the observational methodology and mirrors the fourth step, Evaluation, of Vaishnavi and Kuechler's five steps of an iterative process, recall Figure 3.3. In order to collect feedback on the prototype, participants were observed as they executed various tasks related to the functionality, design, and usability of the prototypes. Oates states that it is helpful to observe people's actions rather than what they claim they do to gather relevant feedback and discover the weaknesses of a prototype [19]. Usability testing is defined in an article by the Nielsen Norman Group as a widely used observation method to discover issues and opportunities in the design [25]. The aim was to identify issues with the prototype, discover potential design improvements, and gain insight in the end user's behaviors and preferences. The researchers facilitated the user through tasks while observing every move, decision, hesitation and thought throughout the process.

An article by Nielsen explains how only five participants are needed for an usability test [26]. He describes, based on an experiment, a formula with n participants: $N(1-(1-L)^n)$, N being the total number of usability design issues and L being the proportion of issues discovered by participants. It was discovered that the most common value for L was 31%, given this information the results in Figure 3.4 prove that after five participants the curve flattens out significantly. On could argue that 15 participants would discover all design issues and be the best solution, but the time effort is not worth it. Nielsen states that after the fifth user one is simply wasting time "observing the same findings repeatedly but not learning much new". Accordingly, five participants were chosen to conduct the usability testing.

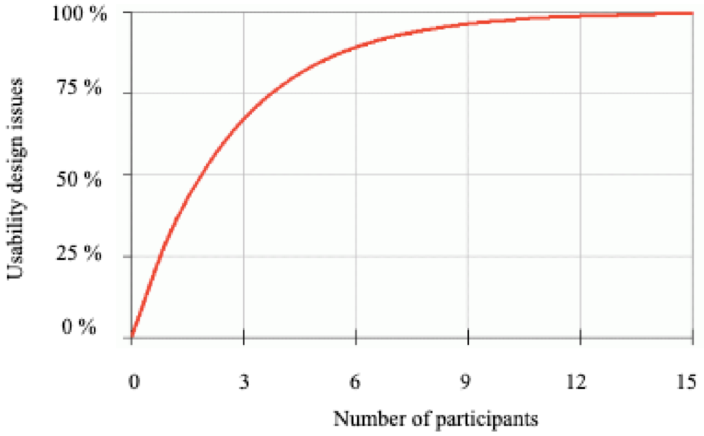


Figure 3.4: Graph showing how many usability design issues each participant in an usability test discovers. Adapted from Nielsen [26].

Individual Interviews

After each observation, in order to collect feedback, a short semi-structured individual interview with some follow-up questions was conducted, five in total. It consisted of four open-ended questions asking about the positive and negative aspects of the prototype's design, functionality, and usability. It allowed the researchers to dig deeper into the observations and the participants to reflect on the tasks in retrospect. Section 6.2.2 explains more in-detail how the usability testing for the prototype was performed.

Considered Data Generation Methods

Questionnaire was considered, but not used. This was considered at the beginning of the project instead of the expert interviews. Nevertheless, it was decided to conduct expert interviews, even though they are more time-consuming than questionnaires. Interviews gathers high-quality, relevant, and detailed data, which was worth spending extra time on. Secondly, a questionnaire was also considered used after the observations. Questionnaires are anonymous and can make it easier for people to be more honest, but it provides little room for reflection. Conducting usability tests is a proper observation method to get inside the participants' heads, understand their thoughts and give them space for reflection. Having an individual interview after this, instead of a questionnaire, made it possible for the participants to express their thoughts and reflections more freely.

3.1.4 Data Analysis

The data analysis also fell under step 4 of the design and creation strategy adapted from Vaishnavi and Kuechler [24]. It was decided to conduct a qualitative analysis. A qualitative analysis is defined by Oates [19] as a method that abstracts the verbal, aural, and visual patterns and themes important to the research topic. In order to prepare the data for analysis the data collected from the interviews and observation were transcribed and translated to English. Ahead of analyzing, the transcribed documents were read in order to get a general impression of the data.

The focus initially was to divide the data into three themes:

- Relevant to the RQs
- General informative descriptions needed to provide context
- Not relevant to the RQs

With these themes in mind it was easy to separate the relevant information from the irrelevant.

The second theme in the list represents information such as work title of the interviewee and education etc. Further, the relevant information was divided into categories, matching similar responses and comparing disagreements. Below, the specific data analysis approach for each method is presented.

Expert interviews

The expert interviews were analyzed according to the general data analysis approach described above. As only two interviews were conducted it was considered unnecessary to spend extra time to learn and use data analysis tools. The researchers had no experience with data analysis tools prior to the research project, and it was easy to compare, analyze and summarize the information of only two interviews manually.

Observation & Individual Interviews

A similar approach was executed for the observation and individual interviews. An overview of the usability test tasks was created to summarize how the observations went. The focus was to extract the most relevant misunderstandings made during observation, but also present the things that were intuitive. Further, the individual interviews were also summarized based on the questions. The focus of the interview analysis was to see connections and differences in the answers and try to interpret the overall impression of the participants. The summarized and analyzed data can be seen in Chapter 7.

3.2 Participants

Involving several participants was necessary to ensure high-quality research. For the expert interviews two participants were recruited by email, and for the usability testing people with different backgrounds and experiences were recruited through the researcher's personal network.

In order to get the most out of the expert interviews, the experts were specifically hand-picked based on their expert knowledge within the main research topics of health data management and the IOTA Tangle technology. Their knowledge, experience, and insight gained from their work provide an essential contribution to our project.

3.2.1 Experts

Expert 1 works as Head of Legal and Compliance within a company that deals with health data management issues and develops innovative solutions related to this. The expert possesses thorough knowledge on the topic of health data, as it has been the expert's primary focus for the last three years.

Expert 2 works as a doctor by trade and has since 2016 been a member of the IOTA Foundation. In this role, the expert primarily oversees engineering. Concurrently with a role in the IOTA Foundation, the expert still works as a consultant in radiology full-time at the University College London Hospital.

3.2.2 Observation & Individual Interviews Participants

The participants were not limited by any specific characteristics. Thus, the participants were selected with intention to recruit people with diverse technical experience, age, and gender so that they would represent a variety of potential users for the prototype. The recruitment of participants was done through the personal contacts of researchers.

3.3 Ethics

An Norwegian Center for Research Data (NSD) application was sent and approved during the early phase of the research, this is attached in Appendix B. The application includes various ethical aspects such as consent forms, data gathering, data storage, data sharing, and data anonymization. The approved NSD application covers both the ethical aspects related to the expert interviews, usability testing, and individual interviews.

3.3.1 Consent Forms for Participants

The NSD application included a consent form for each participant group, one for the expert interviews and one for the usability tests with the individual interviews. This form was mandatory for the participants to sign before participating in the project.

For the expert interviews, the consent form allowed the participants to agree to be anonymized or recognizable in the master thesis. It was decided to offer such an option, as it could be a significant benefit in adding credibility to the paper if someone chose to be recognizable. The usability test consent form, on the other hand, stated that all participants would be anonymized. Both consent forms are added in Appendix C.

3.3.2 Participants Rights

The Norwegian National Research Ethics Committee has established some ground rules regarding research ethics [27]. These rules will be fulfilled in this research through a well-formulated consent form the participants had to sign before participation, open and continuous dialogue with the participants throughout the project, and transparency regarding the research itself. In addition, the committee also mentioned that even if transparency is essential in research, some details need to be protected and anonymized. Personal privacy is critical, and personal information must be treated with sensitivity.

In order to handle the participants' rights properly, guidelines were established. Firstly, it was voluntary to participate and sign the consent form. Secondly, the personal information gathered was limited. This information will be stored securely and privately. The following section presents how data collection and storing was handled. Thirdly, the participants had the right to access all data collected about them at any time. Participants also had the right to withdraw their consent at any time, without any negative consequences. All this information was presented to the participants in the consent form. Besides, an oral repetition of their rights was presented on the day of their participation to make sure they understood their rights. The participants were given the opportunity to conduct a quote check and approve the content prior to the delivery of this paper.

3.4 Collecting & Storing Data

The collected data was only accessible for the researchers and their supervisors. It was stored in a private folder in Microsoft OneDrive with strict access rights. The data will be stored until the end of 2022 and then deleted. The data includes the transcribed interviews and a summary of the usability tests with transcribed interviews. Minimal personal information was collected, only the most necessary for the project. In order to anonymize the participants names were substituted with "Expert 1", "Participant 1", etc.

For the expert interviews, some information about their background, such as work experience and education, was collected and stored. Even though this is personal information, it was decided to generalize it so that the participants could not be linked to the data. One of the experts desired to be anonymized, while the other chose to be recognizable. The only difference in storing data between the two was that the name and background information was stored for the non-anonymized participant. However, both experts were anonymized in this thesis due to recommendation from the researchers supervisor. For the usability tests and individual interviews the personal data collected was their age in a range of five years so as to be less specific, and their education/occupation to provide an impression of their technical experience.

Chapter 4

Systematic Mapping Study

The SMS was conducted during the fall of 2021 as a preparatory project [4]. Recall Section 3.1.1 for a description of the method used. The aim was to gatherer insight on the existing literature of the research topic. Two RQs were established, and together with a search strategy including search strings, selection criteria, and quality assessment a selection of 17 primary studies were extracted and analyzed. The data analysis, together with background information collected ahead of the SMS, were discussed and concluded upon. The findings are summarized and presented in this chapter.

4.1 General Findings

The general findings presents the quantitative data extracted from the primary studies such as year of publication, type of paper (journal or conference), which RQ they relate to, and type of research methodology. It also presents the findings related to this data. It is mentioned in the preparatory project that the amount of primary studies retrieved was not sufficient, as a mapping study should contain broad coverage. Further, it is mentioned that this is due to the novelty of the research topic and that it can be accepted as the "studies retrieved are highly relevant, rich in content, and make up a good foundation for the discussion" [4, p. 28].

In order to provide an overview of the general results, diagrams were created. In figure 4.1, the primary studies are represented in a graph according to which year they were published. Even though the search string allowed for articles all the way back to 2009 to be included in the search results, none appeared relevant until 2018. It was assumed in the preparatory project that this was due to the novelty of the research topic.

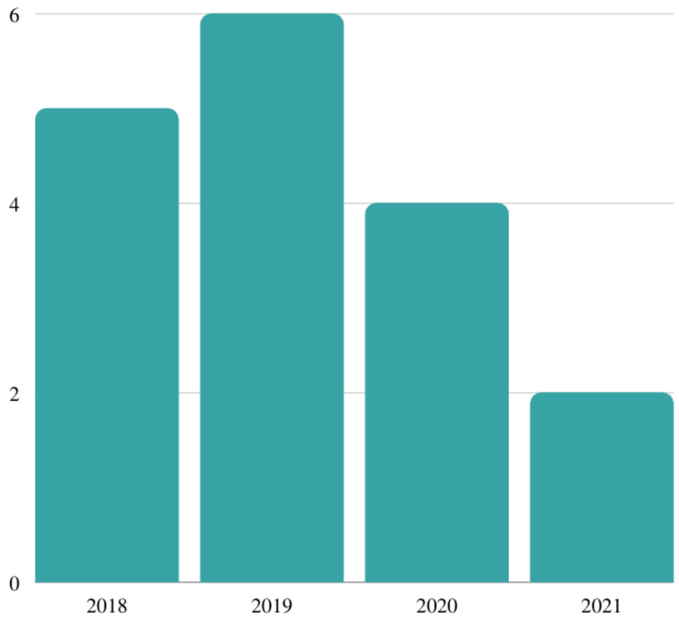


Figure 4.1: Distribution of primary studies based on year of publication, Rydningen and Åsberg [4].

Further, Figure 4.2 presents the distribution of how many studies had a qualitative and/or quantitative approach. Every study had a qualitative approach, and no one had a quantitative approach only. It shows that the qualitative method is the clearly preferred methodology for the research topic.

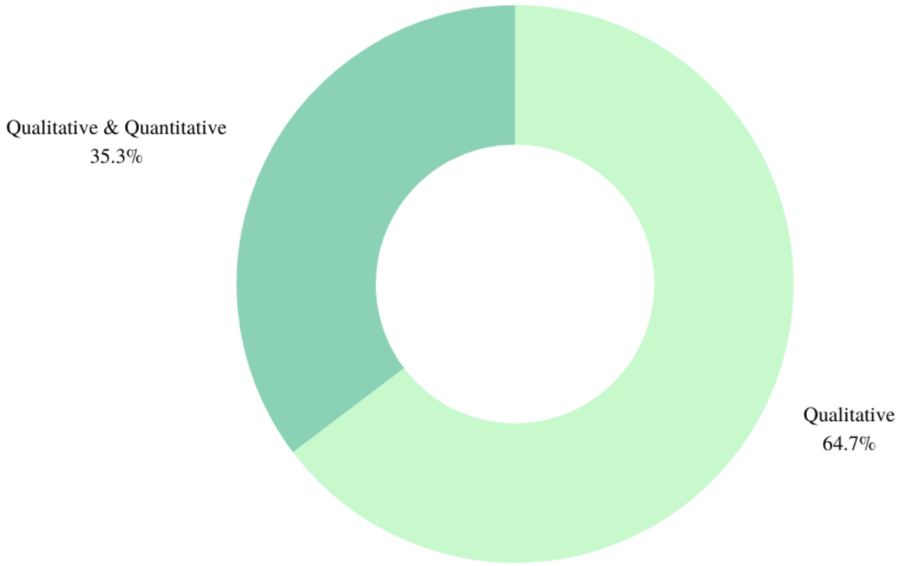


Figure 4.2: Distribution of primary studies based on methodology, Rydningen and Åsberg [4].

Figure 4.3 illustrates a distribution of which primary studies corresponds with which RQ. The distribution is quite even, RQ1 corresponds with 10 studies, and RQ2 corresponds with 7.

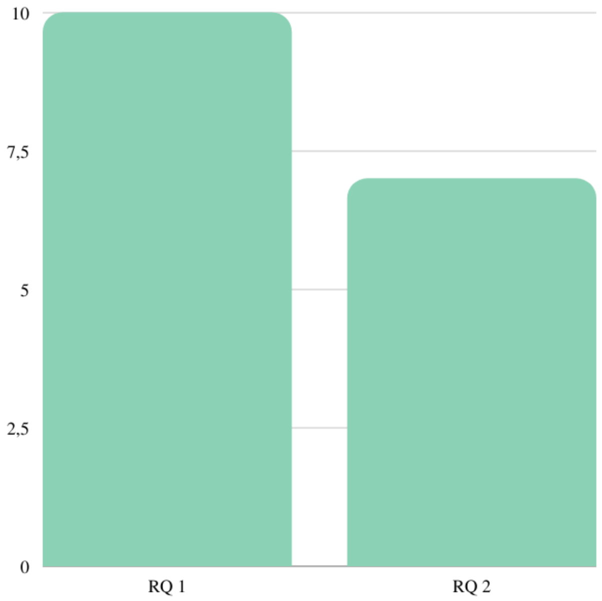


Figure 4.3: Distribution of primary studies based on RQ, Rydningen and Åsberg [4].

Lastly, Figure 4.4 provides a representation of all the journals and conferences in which the primary studies are published. The distribution covers high quality publication providers, emphasising the quality and recognition of the studies.

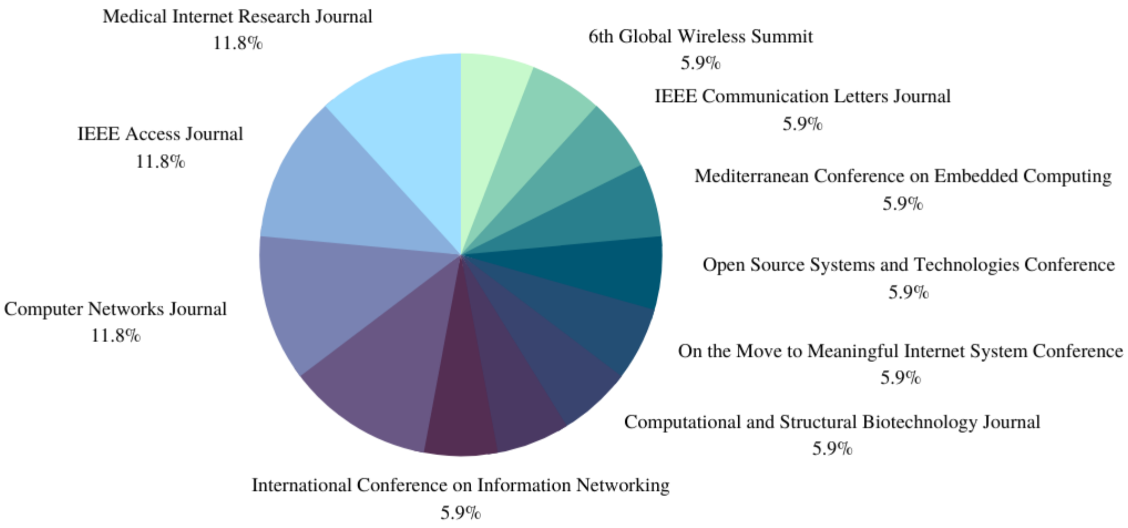


Figure 4.4: Distribution of primary studies based on journal or conference, Rydningen and Åsberg [4].

4.2 RQ1: How can the IOTA Tangle provide reliable and secure health data management?

The two following sections represents the qualitative data extraction and corresponding findings of the SMS.

A total of 10 primary studies [2, 3, 11, 28–34] were selected to answer the first RQ, see Figure 4.3. The focus of these studies was health data management. The results were distributed into three topic areas combined with health data management; blockchain, the IOTA Tangle, and IoT with the IOTA Tangle. The discussion divided the results into four main topic areas, based on four ethical priorities to consider while developing a health data management system, listed by Jamshed et al. [6], recall background Section 2.1. These priorities were privacy, security, system implementation, and data inaccuracies.

Privacy

Ensuring privacy in a health data management system is all about authentication and authorization. Health data is sensitive and confidential, thus it is crucial to share authenticated data between authorized parties to assure privacy.

According to Sengupta et al. [28] the use of blockchain technology in the health care sector has shown great improvement in terms of security. Nevertheless, this integration in health care systems lack some important features in regards to privacy. The limitations are presented in the work of Yaqoob et al. [29], Farahani et al. [2], and Houtan et al. [30], and the two main limitations are low scalability and low interoperability. These, on the other hand, are features the IOTA Tangle handles well. The three articles all conclude that the privacy issue blockchain is facing in health care systems could be solved by the IOTA Tangle due to their different data structure. The blockchain data structure, a block of chains, is more prone to attacks and privacy abuse than the IOTA Tangle's Directed Acyclic Graph (DAG), which uses a communication tool called MAM in order to share authenticated data between authorized parts. As mentioned in the background, Section 2.4.5, IOTA Streams is the new version of MAM. Recall Section 2.4.5 for a comparison of the data structures.

Another three studies, Hawig et al. [3], Zheng et al. [32] and Brogan et al. [34], emphasize the privacy aspect in their research, and they successfully combine health data sharing with MAM and IoMT to manage health data. They demonstrate authenticated, encrypted, immutable, and granularly controllable health data management with the IOTA Tangle.

Security

Ensuring security in a health data management system is equivalent to protecting the system from intruders and attackers and prevent security breaches. Saweros and Song [11] presents a study implementing the IOTA Tangle in a health data management system with improved security. The advantages lies in the decentralization of the IOTA Tangle, which means that no single point of failure nor any single points vulnerable to attack end up affecting the entire network, recall Section 2.4. Reliability and integrity is ensured through validations each node receives from thousands of other nodes, with the use of hash algorithms, to verify transactions. Another advantage of the decentralized approach is data can be stored "directly, locally, and encrypted, instead of passing through an intermediate connector, making the system reliable, secure, and tamper-proof, as well as ensuring data integrity". This was also supported by systems demonstrated in the work of Silvano et al. [33], Zheng et al. [32], and Florea et al. [31], where the IOTA Tangle, IoT/IoMT, and MAM were used to develop decentralized systems.

System Implementation

System implementation of health data management systems includes data transfer, and data storage possibilities in terms of efficiency and performance.

Brogan et al. [34] presented a solution with the IOTA Tangle, IoMT, and MAM providing interoperability in a large and diverse health care ecosystem. High interoperability increases efficiency and performance as the data flow and interaction between stakeholders is improved. The study by Saweros and Song [11] demonstrated a system with the same technologies as Brogan et al. where the patient could control and be responsible for their own health data in correspondence with health personnel. This provided increased efficiency through providing remote patient monitoring, which saves time. Further, the study reduced data fragmentation considerably, this is linked to the fact that the IOTA Tangle is interoperable thanks to MAM.

Lastly, the IOTA Tangle is proven highly scalable in several of the primary studies [2, 28, 29, 32], due to its ability to process parallel transactions, as pointed out in Section 2.4.5.

Data Inaccuracies

In a health data management system data inaccuracies may occur due to two actions. Either people using the system committing errors because they misunderstand the user interface, or unforeseen technical problems.

There is little the IOTA Tangle can do in terms of the human error aspect of data inaccuracies, since it is not a user interface framework. The technical aspect on the other hand is something the IOTA Tangle can improve as it transfers data securely, immutably and tamper-proof [31–33]. Thus, the chance of data inaccuracies to occur are reduced.

4.3 RQ2: What are the advantages and disadvantages of using the IOTA Tangle compared to other Distributed Ledger Technologies?

For RQ2, 7 primary studies were selected [35–41]. The studies compared various DLT technologies in terms of design, architecture, performance, energy expenditure and cost. Some focus on the common concepts used in various DLTs, such as Blockchain, Tangle and Hashgraph structures, while others compared specific DLT designs and their properties. The following section summarized the findings from the literature comparing the IOTA Tangle with other DLTs.

DLT Concepts

A DLT concept is an abstract description of the architecture and organization of transactions of a distributed ledger.

In the paper by El Ioni and Pahl [39] four variants of DLT concepts, as seen in 4.5, are first described and then compared using a set of quality criteria. In addition, a SWOT analysis compared their strengths, weaknesses, opportunities and threats.

The paper highlights the unique features for each type. The main advantages of the IOTA Tangle according to El Ioni and Pahl [39] are scalability, an encryption algorithm robust against quantum computation attacks as well as no transaction fees.

Another study by Zivic et al. [40] compared the suitability of blockchain, the IOTA Tangle and hashgraph for Machine-to-Machine (M2M) communication in the IoT. They examined aspects such as level of decentralization, accessibility, transaction costs, consensus mechanism, stability and speed. Zivic et al. [40] concluded that the IOTA Tangle is the most suited for use in IoT due to it zero fee transactions.

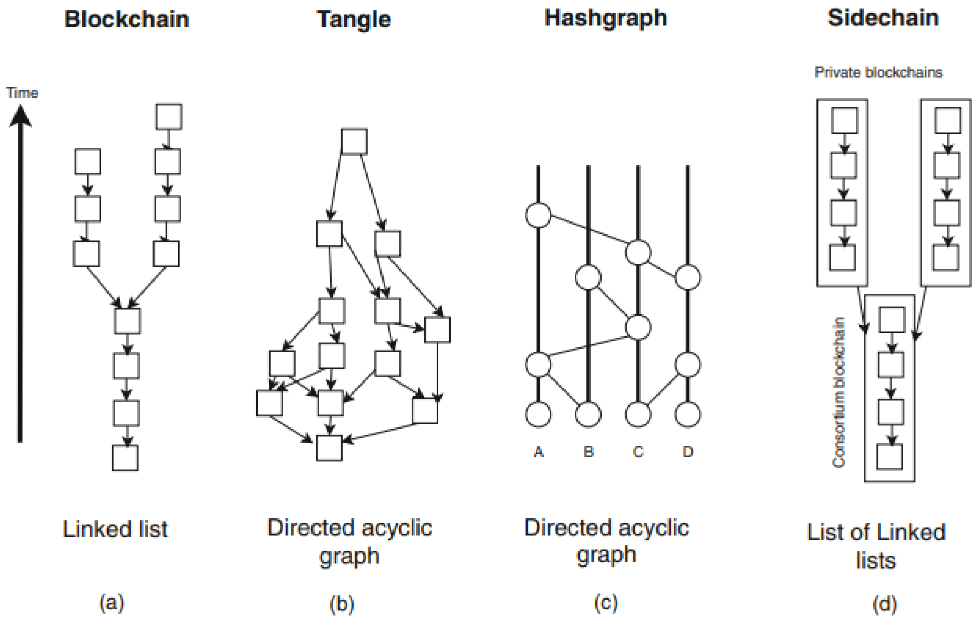


Figure 4.5: Four common DLT concepts, El Ioni and Pahl [39]

DLT Designs

Each DLT concept has a variety of implementations called DLT designs. Two well-known examples of implementations of the blockchain concept are Bitcoin and Ethereum, recall Section 2.4.4.

The paper by Brotsis et al. covers 32 DLT designs and quantitatively evaluates each technology and gives them a score in metrics such as security and scalability [37]. The IOTA Tangle is rated third highest in terms of security, has high scalability, can handle many transactions per second, and has a low block confirmation time due to its DAG data structure.

Another study by Chowdhury et al. examines 11 DLT designs and attempts to evaluate the domain each design is most suited for [38]. The evaluation criteria are upgradability, trust level, scalability, transaction cost and energy use. The IOTA Tangle stand out as having no fees, low energy expenditure and that it is well suited for IoT data transfers.

DAG based DLTs

The study by Pervez et al. performs a comparative analysis of DAG based DLT designs including Nxt, IOTA, DagCoin, Byteball, XDAG, Orumesh and Nano [41]. They claim that the DAG data structure has revolutionized DLT due to its efficient validation mechanisms, scalability and support for the IoT.

In a direct comparison of confirmation time of transactions, Orumesh and Nano with 1-10 seconds spent were on average faster than the IOTA Tangle with a confirmation time between 1-60 seconds.

The IOTA Tangle has a disadvantage compared to the other DLTs in that it has a Coordinator and can not be considered fully decentralized. The Coordinator acts as a reference point for transactions in the network and is run by the IOTA Foundation. The network in its current form can in essence be shut down by the foundation, which is why Pervez et al. state that the IOTA Tangle an not be considered fully decentralized.

The paper also compares key features of each DLT and that the IOTA Tangle is regarded as unique in supporting data transfer, cryptographic messaging, its suitability for IoT and efficient M2M communication.

4.4 Conclusion

This SMS was conducted to analyse the existing literature on the topic of health data management and distributed ledger technologies, with a focus on the IOTA Tangle. The aim of this study was to gain insight and to determine if the IOTA Tangle is a good choice for the development of a health data management prototype.

The IOTA Tangle has several advantages and improvements to the issues faced by health data management systems today. The results from the SMS show that the IOTA Tangle has high scalability, tamper resistance, and security. Combined with the MAM communication tool the IOTA Tangle can provide reliable and secure health data management. In summary, the SMS indicates that the IOTA Tangle is a suitable technology for the development of a prototype.

Chapter 5

Expert Interviews

This chapter presents a summary of the findings from the expert interviews, which serves as a basis for discussion in Chapter 8. The participants are presented initially, followed by the accumulated knowledge categorized into suitable topics. The expert interviews were conducted in order to gain a deeper understanding of the research topic ahead of prototyping. It was decided to perform two interviews since planning, executing, transcribing, and analyzing interviews is time-consuming.

5.1 Expert 1

Expert 1 works as Head of Legal and Compliance position within a company that deals with health data management issues and develops innovative solutions related to this. The expert possesses thorough knowledge on the topic of health data, as it has been the expert's primary focus for the last three years. The knowledge within the topic of health data management is specified towards the regulatory, security and privacy aspects of it. The company aims is to improve patients' and caregivers' quality of life and make it easier for patients to live at home as long as possible. This focus is realized through providing services and products that improve the interaction and communication between patient and caregiver. Full access to own data, privacy, security, and flexibility are some of the company's primary focus areas.

5.2 Expert 2

Expert 2 is a doctor by trade and has since 2016 been a member of the IOTA Foundation. The expert started as a physician in 2000, and later became more interested in the data aspect of medicine. Further, expert 2 developed medical technology working with UCL Computer Sciences, an educational institution in London. Looking into the interoperability of data between hospitals, he became interested in the Ethereum blockchain. However, the expert noticed issues with its consensus mechanism and its limitations on the number of transactions per second the network could handle. The expert was introduced to the IOTA Tangle and joined the IOTA Foundation shortly after. This is where the expert worked on the eHealth-focused activities, and researched using the IOTA Tangle for remote patient monitoring to maintain GDPR compliance when using a public distributed ledger. Later transitioning to overseeing the engineering aspect of development. Concurrently with the role in the IOTA Foundation, Expert 2 still works as a consultant in radiology full-time at the University College London Hospital.

5.3 Development of Health Data Management Products

Health data management products needs to follow strict regulations, live up to certain standards, and answer to customer requirements in order to be accepted on the market. This section provides a summary of the information provided by expert 1 on this topic.

Regulations

It was stated early in the interview that developing a product within the health sector comes with strict regulations. A product could be anything from a software, service, system, to a platform. In the Medical Device Regulations, one must look up the definition of a medical device, and if the product falls within this definition, it can be Conformité Européenne (CE) marked. The CE marking implies that the manufacturer or importer affirms the conformity with European health, safety, and environmental protection standards. For example, expert 1 mentioned that their company is "considered a 'software as a medical device' on the same level as a blood glucose meter or any medical device".

A quality management system must also be implemented for the product in accordance with the requirements of the most suited Organization for Standardization (ISO) standards. It was emphasized that "to us it is ISO 13485 that applies to the production and design of medical equipment. Of course, ISO 27021 is also important as it is the information security standard". Further, in the health sector especially, the system should be following the norms of personal privacy. The product has to ensure information security and privacy in order to fulfill the general health industry standards. These are not regulatory rules, but they are just as important to include due to the sensitivity of health data.

Customer Requirements

The customer requirements cover what is expected and required from the customer. Publicly, one can only deliver products that answer a requirement specification, presented through a customer requirement list with rules and standards to which the product must adhere. This aspect is emphasized by expert 1 stating that "when you sell products to the market as we do, it is the public tender that applies, and then one is only allowed to deliver products that answer to a requirement specification", indicating that the customer has the power in this matter.

Customer requirements also cover usability standards, referred to as universal design. These standards are important to consider when developing a health data management product, as people have diverse experiences and basis for using such a product. Expert 1 explains that it is imperative to them "because we provide a service that is used by chronically ill people who may be disabled or have a hearing or sight or something disability, and also older people who are not very used to technical gadgets and such". It is important to remember all various types of people who might use the product to ensure inclusion for all.

5.4 Issues in Today's Health Data Management Solutions

There are two issues in particular the IOTA Tangle is well suited to tackle, the interoperability and immutability of health data. In this section expert 2 first explains what interoperability means, followed by answers regarding issues in existing health data management solutions.

5.4.1 Interoperability

There are several ways to view interoperability between systems. Expert 2 points out that "there's very basic interoperability, where two things can exchange messages with each other. I think IOTA can help a bit with that". The basic level of interoperability is when you enable the exchange of data between systems, the IOTA Tangle enables this because it allows the transmission of arbitrary data packets. True interoperability, is when two systems can exchange data and the other system understands the data as well. This is interoperability on the semantic level and goes beyond the scope of what IOTA can provide on its own. For example, if the data is a measurement of a patient's temperature, it is not enough to present the temperature on its own. One also need the correct denomination, if the measure is in Celsius or Fahrenheit, where and with what type of device the measurement was taken. In other words, for semantic interoperability between systems, you need the data, correct labeling, and an information model that enables the analysis and interpretation of the data in a meaningful way.

Lack of Incentive for Interoperability for System Vendors

According to expert 2, some vendors don't want interoperability "because, it's either too hard for them to build it, or in the bigger vendors cases it stops them from having vendor lock-in." Large vendors desire vendor lock-in, which is when a customer becomes dependent on a specific vendor for products and services, unable to change to another vendor without substantial switching costs. Vendors of health data management systems currently stand to gain little from openly sharing their collected data. In addition, interoperable systems are challenging to build.

5.4.2 Immutability in Traditional Data Systems

Traditional firewalls are implemented to protect data within a system, for example, a hospital with its patient records. Expert 2 explains that this works for smaller institutions, but as you want to incorporate several hospitals and institutions within your firewall, in order to enable data sharing between them, the firewall would also need to grow accordingly. As a result, "you end up just making firewall bigger and bigger, and with that comes increased risk of holes in the firewall." Suppose the system includes home monitoring of patients. In this case, the problem grows, and the risk of man-in-the-middle attacks increases, which is when an attacker secretly relays and alters the communications between two parties. This example is within an area where IOTA can play a crucial role in enabling the immutable and incorruptible transmission of data between institutions.

5.5 Improving Health Data Management

The experts were asked if they had any suggestions on what could improve health data management today. They expressed their suggestions for improvement in general, as well as solutions that they are working on in in their respective positions. Some of the solutions are to be implemented in the future, and some of the solutions have already been implemented in their companies work. Proactive patient care, ownership of data and automated decision making was the most important suggestions, and the answers are presented in this section.

5.5.1 Proactive Patient Care

In order to achieve proactive patient care, expert 1 says that the mission of their workplace is to make it possible for patients to stay at home longer by receiving follow-up without having to travel to the hospital as often. In addition, "what we work on a lot, and the system is designed to do, is to detect errors faster so that you may also avoid complications and hospitalizations.

So, it is really to improve the quality of life of patients". To bring up an example, the expert explains that if a patient needs medication support, which implies that the home care service visits the patient's house up to three times a day to provide medication, this time could be reduced by providing a medical dispenser instead. Thus, more flexibility for the patient and time saved for the home care service.

Consequently, health professionals responsible for the follow-up of the patients' health measurements also save time using this system. They get patients to send health data via an application instead of providing follow-up visitations. It seems like a common denominator amongst healthcare professionals that they spend much time on work that could be more efficient. Expert 1 emphasizes this by saying that "we very often experience talking to doctors and people who work in the home care service that they spend a lot of time on things that could have been done very easily digitally". To summarize, proactive patient care aims to improve patients' quality of life and save some time for the healthcare workers to work more efficiently and spend time on those who need it.

5.5.2 Ownership of Data

According to expert 2, IOTA will be useful when exchanging data from many devices everywhere. A significant contribution is providing a framework for the identity of devices and people in a decentralized way. Then you would not necessarily be monitored by a third party.

IOTA can enable individual ownership of data. Expert 2 says that with IOTA "we can collect data ourselves with our own decentralized identity and provide that for analysis in a pseudonymized way". Pseudonymization is similar to anonymization. However, an individual can still be identified through additional information. The data could be distributed by IOTA Streams, which can monitor access control to the data. It presents a new model where instead of dumping your data to Google or Apple and having them controlling and curating it, you control and curate your own data. When a data company gathers a large amount of data from their users, one will basically never see the raw data one is generating. One might get some representation of the data in graphs, but the company will own it and monetize it.

This aspect is supported by expert 1, who states that their solution gives the patients access to their own data. Further, elaborating that "the patient has access to all historical measurements and can see graphs of their own measurements. The idea is that the patient should become a larger part of their own health team and be able to detect deterioration and even know what they should do if they see this and that".

5.5.3 Automated Decision Making in Healthcare

Why is the accuracy and immutability of data so important in healthcare? One could argue that if a single point of data gets corrupted, it may not make a significant difference. However, expert 2 argues that as decision-making about healthcare is becoming more and more automated, the cumulative effect of data points being corrupted is that the algorithm may start making incorrect decisions about what medicines and treatments to give to the patient. One may get another medicine than one should, a different dosage, or a new medicine that one does not need. Take, for example, allergies, if you "corrupt the data that says you have an allergy and say you don't have an allergy to something and I give you a medicine that you're allergic to it, then you're dead. So that's the soft way to kill someone". An attacker could also introduce bias to the data, leading to worse results for the patients in the long term.

5.6 The Future of Health Data Management

The experts agree that improved interoperability between healthcare institutions, both public and private, is a crucial issue to focus on for the future of health data management. Today's biggest challenge is the various systems different healthcare institutions use that are incompatible, and due to lack of incentives for interoperability, it might take time to see substantial change in health data management. Expert 1 mentions that "what I hope will happen, and I hope that this happens before that time, is to improve data flow across companies, both between hospitals, or specialists and primary health providers. This is the biggest challenge you see today. That they have used different systems, and no one has access to data from the others. It is really interoperability, as one manages to achieve cross-functional integration that work and that enable better data flow." As the IOTA technology matures Expert 2 believes that it may provide the essential tools for companies and institutions to more securely exchange sensitive health data.

Chapter 6

Prototype Development Process

This chapter outlines the process of developing a health data management application with the IOTA Tangle. The development of the prototype was motivated by the findings of the SMS, summarized in Chapter 4, and the expert interviews, presented in Chapter 5. The RQs, see Section 1.2, ask how the IOTA Tangle can provide reliable and secure health data management and how such an application should be implemented.

The prototype development process was inspired by the work by Preece et al. [42]. It mentions essential activities to perform when developing an application prototype. These activities corresponds with the five steps in iterative processes by Vaishnavi and Kuechler [24], recall Section 3.1.2. In this chapter the two iterations of prototype development are presented. Figure 6.1 illustrates the focused steps with descriptions for each iteration.

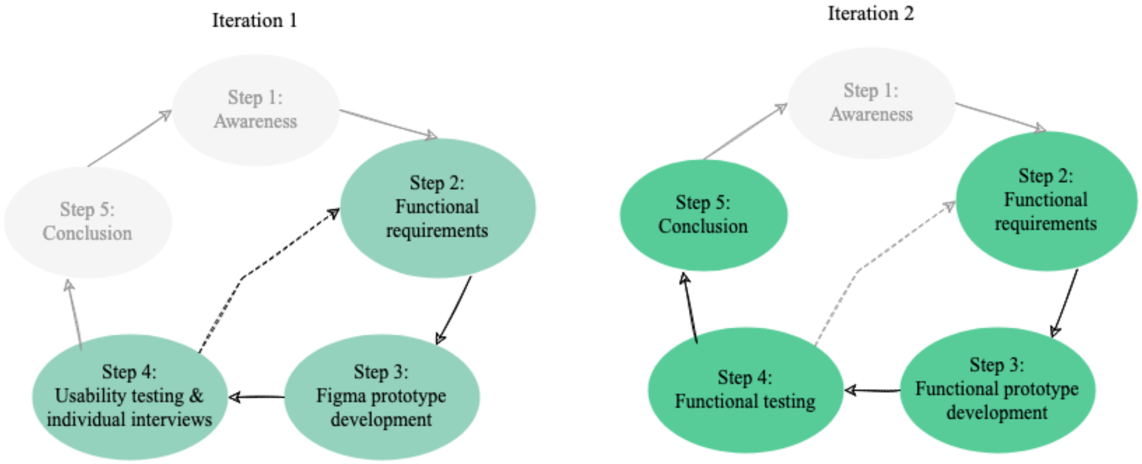

Iteration 1
Step 1: Awareness
Step 2: Functional requirements
Step 3: Figma prototype development
Step 4: Usability testing & individual interviews
Step 5: Conclusion
Iteration 2
Step 1: Awareness
Step 2: Functional requirements
Step 3: Functional prototype development
Step 4: Functional testing
Step 5: Conclusion

Figure 6.1: Illustration of iteration 1 and 2 of the design and creation process. Adapted from Vaishnavi and Kuechler [24].

The first iteration, Figma development process, is presented in section 6.2. The second iteration, functional prototype development process, is presented in sections 6.3.

6.1 Development Tools

A variety of development tools were used to carry out the project. This included technical tools (like Git, GitHub, and Figma), organizational tools (such as Gannt and Trello), and a place to store the data (in this case Microsoft OneDrive). Their purpose is presented below.

Git & GitHub

Git and GitHub was the preferred sharing platform for the code. It was a natural choice as both the researchers had plenty of experience with Git and GitHub ahead of the project. It facilitates creating a repository (project) and sharing code amongst several people. Link to the prototype repository at GitHub: github/tanglehealth.

Figma

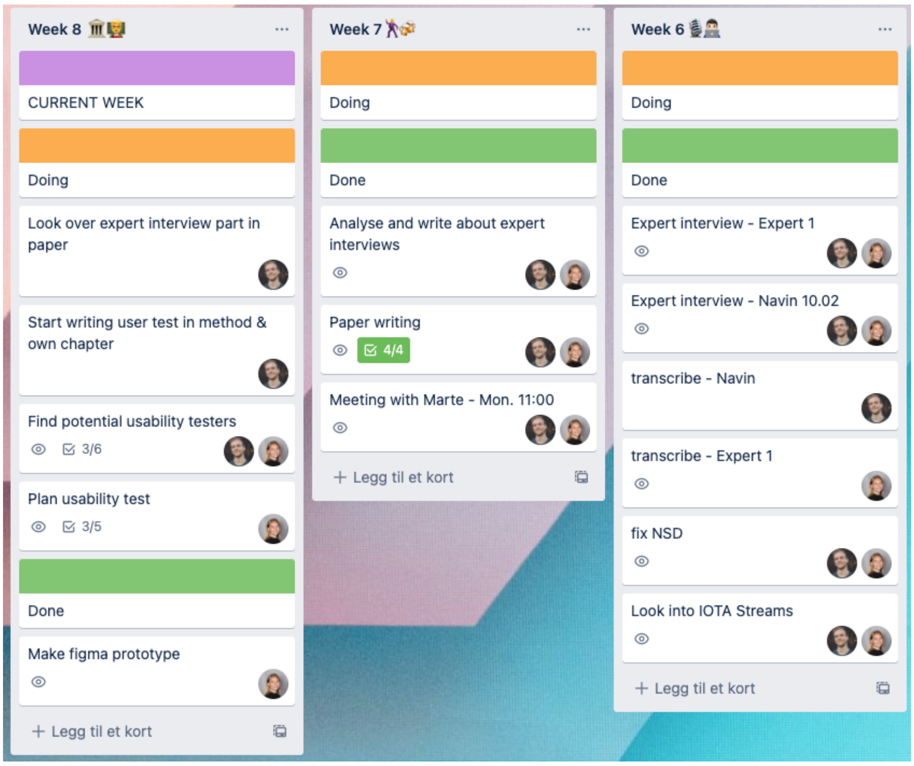
The first prototyping sketches were made on paper, but using paper for usability testing can be challenging and inefficient. Thus, Figma was used to develop the first prototype version to be tested, a link to the Figma prototype is presented in Appendix D. Figma offers several functionalities for developing desktop and application prototypes. It also facilitates for linking between screens which makes the user experience more realistic. Figma facilitates online testing, and even tough all the tests were performed physically it was nice to have the possibility to do it online due to Covid-19 related challenges.

Gannt Chart

This research project started by planning and establishing time estimates for the research period. A semester plan was produced in form of a Gannt chart. It served as a reference point throughout the project regarding task start and end times, and whether the progress was behind, ahead or on schedule. The Gannt chart is illustrated in Appendix A.

Trello

Even though the Gannt chart served as an overall plan for the research it was necessary to do in-detail weekly planning. Trello facilitated for an agile development process. The agile approach was convenient in terms of flexibility. Another advantage with the agile approach was the feeling of success throughout the project, as it was motivating when the weekly goals where met. The focus was to take one week at a time, and in return stress and future concerns were avoided. As illustrated in Figure 6.2 color codes were practiced, the purple tag indicated the current week, the yellow tag was the tasks in progress and the green tag represented the finished tasked. The pictures on each task showed who was responsible for each task. Even though a lot of time was spent physically together, there were times during the project the researchers spent several weeks apart. This made Trello a great tool for keeping track on each other's progress.



Week 8

CURRENT WEEK

Doing

Look over expert interview part in paper

Start writing user test in method & own chapter

Find potential usability testers
☑ 3/6

Plan usability test
☑ 3/5

Done

Make figma prototype

+ Legg til et kort

Week 7

Doing

Done

Analyse and write about expert interviews

Paper writing
☑ 4/4

Meeting with Marte - Mon. 11:00

+ Legg til et kort

Week 6

Doing

Done

Expert interview - Expert 1

Expert interview - Navin 10.02

transcribe - Navin

transcribe - Expert 1

fix NSD

Look into IOTA Streams

+ Legg til et kort

Figure 6.2: Screenshot of Trello board.

Microsoft OneDrive

This platform was provided by NTNU for storing and saving the collected data. It was important to be able to store data securely, especially the data collected from the interviews and usability tests. It was also easy to create private folders for the sensitive data.

6.1.1 Technology Stack

Table 6.1 presents an initial overview of the technologies ahead of developing. Changes were made throughout the project due to unforeseen circumstances and limited time. The changes and adjustments are elaborated in Section 6.3.4.

Technology	Description	Purpose
IOTA Streams	Organizational tool for structuring and navigating secure data through the Tangle [43].	Secure and private health data sharing in prototype.
Rust	A statically-typed programming language designed for safety and performance [44].	One of the few, and most documented, compatible languages to use with IOTA Streams.
Kotlin	Modern statically-typed programming language used by most professional Android developers [45].	Developing the Android application of the prototype.
Wear OS	Google's operating system for wearables.	Connect the smartwatch with the prototype application in order to collect and share health data.

Table 6.1: Technology stack.

6.2 First iteration: Developing Figma Prototype

The first step was to design a prototype in Figma that could be used to test the planned features and user interface of the health data management application. The prototype was designed to be interactive so that users could test the functionalities and usability of the application. Applications like Garmin Connect and Health & Fitness Tracker were used as inspiration.

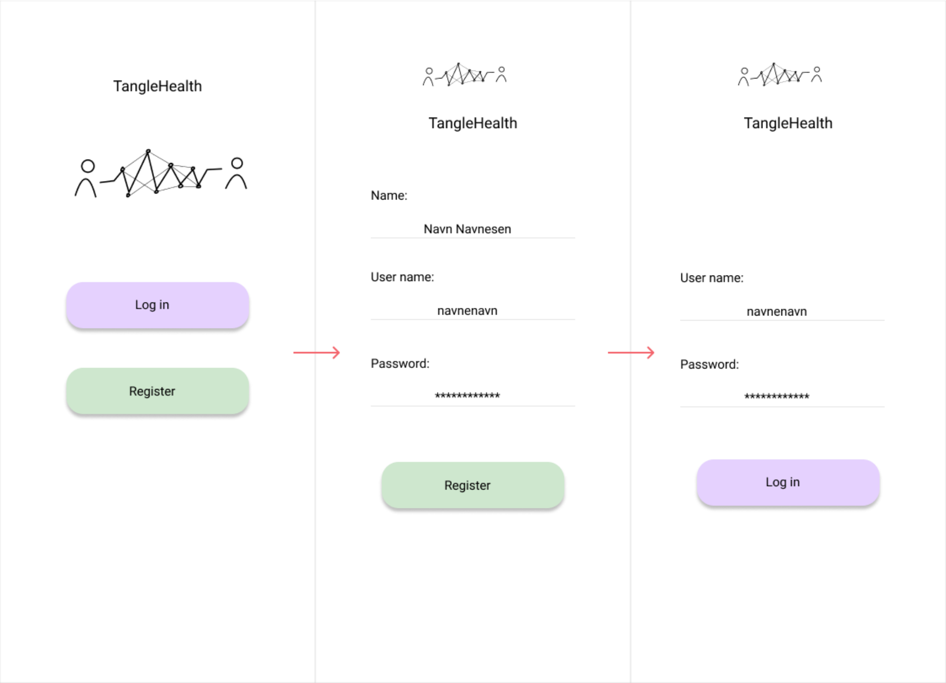
First, the functional requirements were established. As mentioned initially, these requirements were made with inspiration from the SMS, expert interviews, and with the RQs in mind. The requirements were considered necessary to realize a health data management application where users could exchange health data with other authorized users, and they were:

1. Register and log in
2. Pair with a smartwatch and synchronize health data
3. Set up health data sharing groups
4. Subscribe to health data sharing groups
5. Visualize the health data
6. Customize the user profile

After they had been established it was time to develop the design of the application, along with the interaction flow. Step 1, 5 and 6, illustrated in Figures 6.3, 6.7, and 6.8, were easy to design and implement as they were standard functionalities found in many applications. Step 2, illustrated in Figure 6.4, pairing and synchronizing the smartwatch to the application, was challenging to design due to the novelty of combining Wear OS with the IOTA Streams tool together with the Kotlin application. It was difficult to know if there would be any issues with this connection and combination of technologies in terms of synchronizing the data, but the solution ended up being simple and intuitive. The plan was to change the interface if necessary, and not spend too much time dwelling on possible solutions. The unique characteristics of the IOTA Tangle was necessary to take into consideration when designing the user interface, as it affected steps 3 and 4, illustrated in Figures 6.5 and 6.6. The IOTA Tangle requires three-way-handshake when it comes to creating and subscribing to a channel due to IOTA Streams, recall Section 2.4.5. In this case channels were used to create health data sharing groups. Struggling to find an intuitive solution to this issue, it was decided to provide notifications continuously to make sure the user always would know what the status of the sharing groups were.

Below is a representation of a selection of screens from the Figma prototype with corresponding functional requirements. The actual prototype is linked in Appendix D.

1. Register and log in



Name: Navn Navnesen

User name: navnenavn

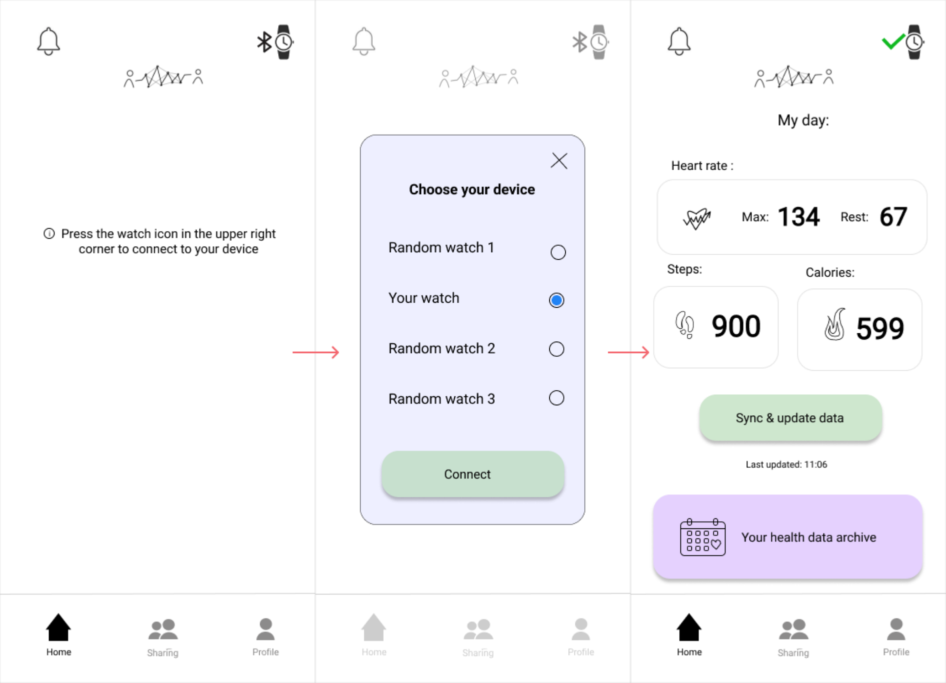
Password: ************

User name: navnenavn

Password: ************

Figure 6.3: Presentation of step 1 in the Figma prototype.

2. Pair with a smartwatch and synchronize health data



ⓘ Press the watch icon in the upper right corner to connect to your device

Random watch 1 ○

Your watch ●

Random watch 2 ○

Random watch 3 ○

Heart rate : Max: 134 Rest: 67

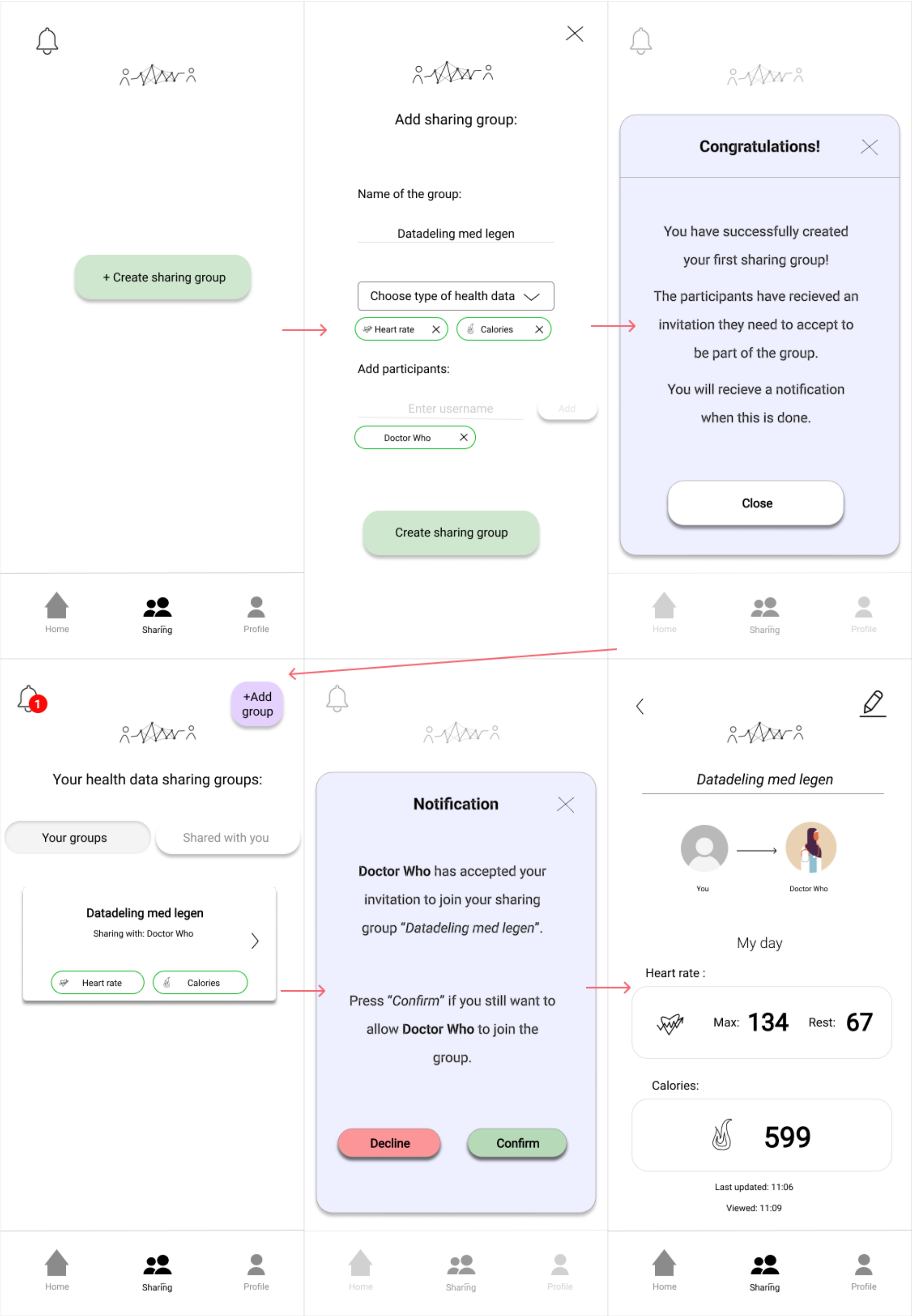
Steps: 900

Calories: 599

Last updated: 11:06

Figure 6.4: Presentation of step 2 in the Figma prototype.

3. Set up health data sharing groups



Add sharing group:

Name of the group: Datadeling med legen

Choose type of health data: Heart rate, Calories

Add participants: Enter username | Add

Doctor Who

Congratulations!

You have successfully created your first sharing group!

The participants have recieved an invitation they need to accept to be part of the group.

You will recieve a notification when this is done.

Your health data sharing groups:

Datadeling med legen

Sharing with: Doctor Who

Notification

Doctor Who has accepted your invitation to join your sharing group "*Datadeling med legen*".

Press "*Confirm*" if you still want to allow **Doctor Who** to join the group.

Datadeling med legen

My day

Heart rate : Max: 134 Rest: 67

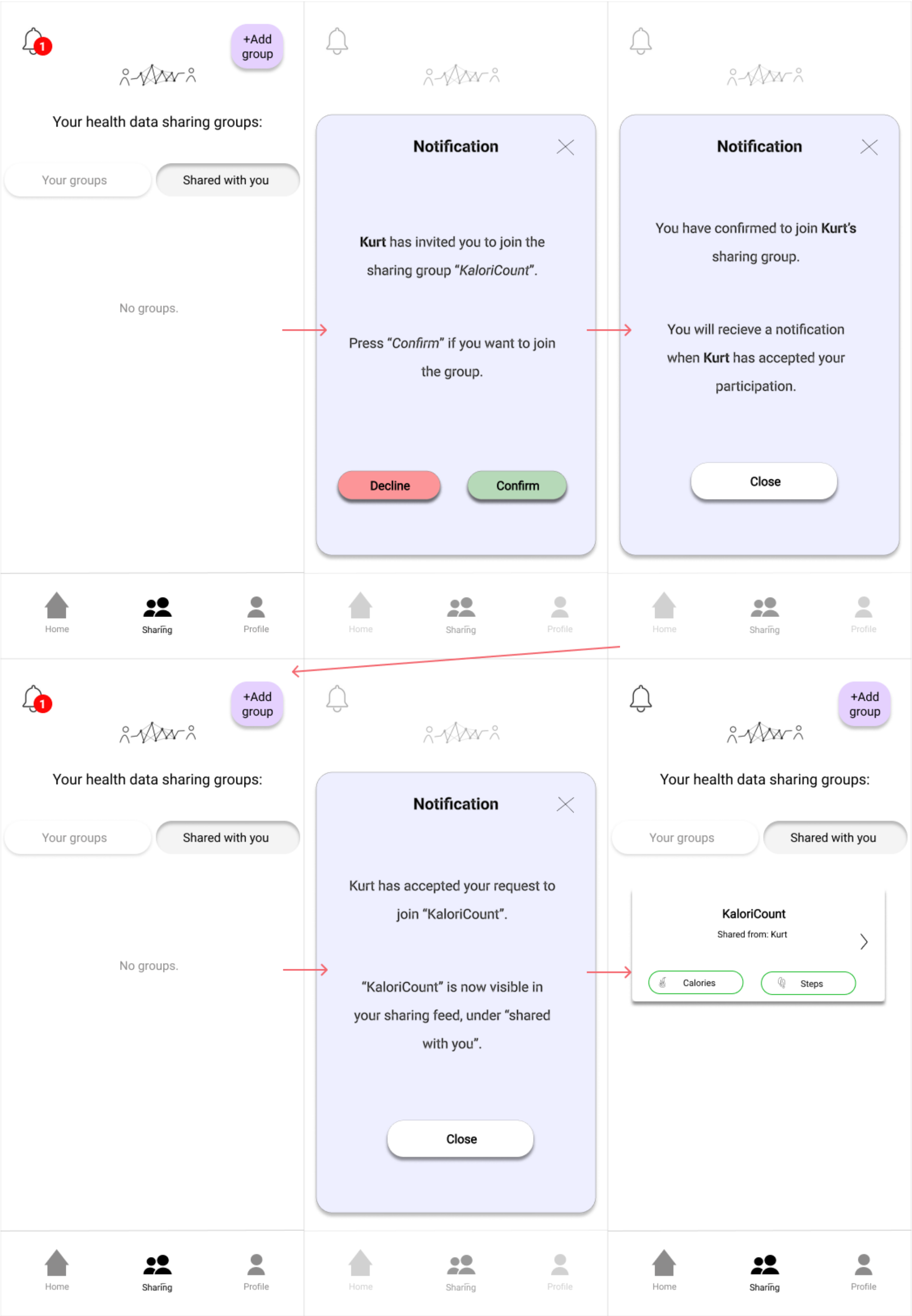
Calories: 599

Last updated: 11:06

Viewed: 11:09

Figure 6.5: Presentation of step 3 in the Figma prototype.

4. Subscribe to health data sharing groups



Kurt has invited you to join the sharing group "*KaloriCount*".

Press "*Confirm*" if you want to join the group.

You have confirmed to join **Kurt's** sharing group.

You will recieve a notification when **Kurt** has accepted your participation.

Kurt has accepted your request to join "KaloriCount".

"KaloriCount" is now visible in your sharing feed, under "shared with you".

Figure 6.6: Presentation of step 4 in the Figma prototype.

5. Visualize the health data

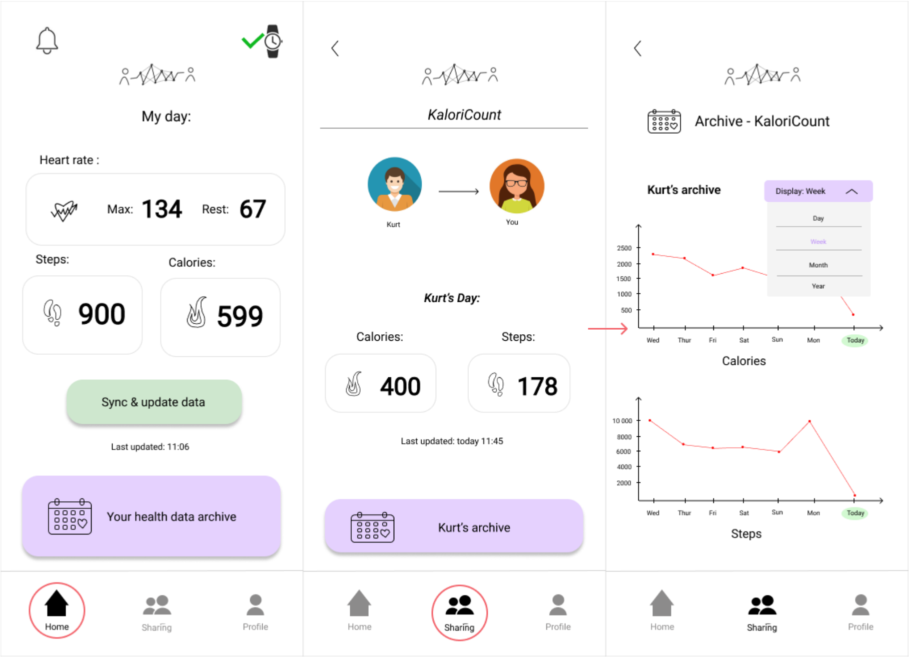
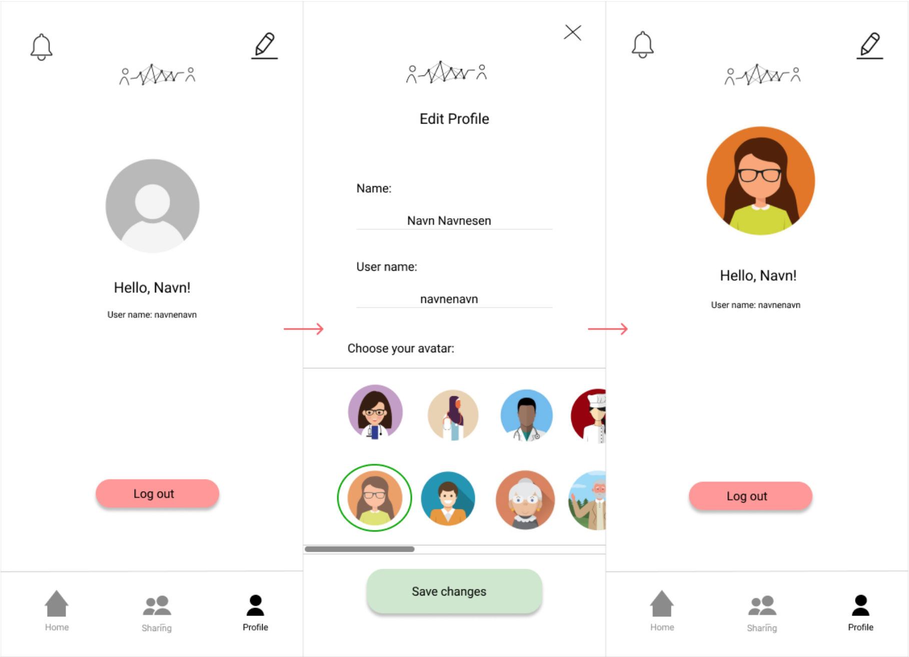


Figure 6.7: Presentation of step 5 in the Figma prototype.

6. Customize the user profile



Name: Navn Navnesen

User name: navnenavn

Figure 6.8: Presentation of step 6 in the Figma prototype.

6.2.1 Design Principles

It was desired to implement the prototype to best meet the functional requirements. Thus, looking into what Preece et al. [42] had to say about this was helpful. An important statement mentioned was to ensure the usability of a product in order to know if it is effective, efficient and satisfying to the users. Ensuring usability is done through following the Don Norman design principles. An overview of these principles can be seen in Table 6.2.

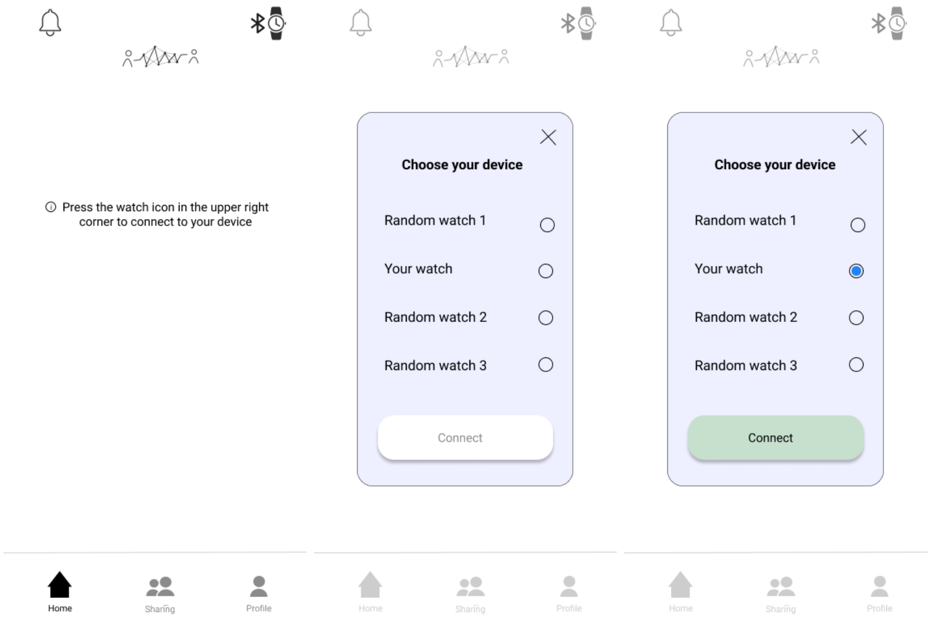
Principle	**Description**	**General example**
Affordance	What action does the product invite you to take?	Button - "Click me"
Constraints	Restrictions leading you to take the "right" actions.	Button - grayed out
Feedback	An action will lead to feedback or consequence.	Submit button - "Successfully submitted"
Mapping	Correlation between actions and results.	Button arrow up - increases volume
Visibility	You have overview of the product's state and possible interactions.	Progress bar, Menu
Consistency	Similar tasks have similar actions and feedback. The design is consistent.	All submit buttons are green.

Table 6.2: Don Norman principles with examples. Adapted from Preece et al. [42].

To summarize how the Don Norman design principles were addressed in the Figma prototype it can be helpful to look at some examples for each design principle.

Affordance was approached such that all important icons and buttons had descriptive text, bright colors and were placed in focus. If a possibility for misunderstanding occurred, a descriptive text was placed in focus to guide the user in the right direction. For example, in the left screen of Figure 6.9 it is explained how one can connect the smartwatch to the app, since the connection icon in the upper right corner could be overseen.

Moving on the *Constraints*, the same figure shows in the middle screen that the "Connect" button is not active until a smartwatch is chosen. This is one example of how the Figma prototype handled constraints, and only invites the user to click the button when the right action has been made.



ⓘ Press the watch icon in the upper right corner to connect to your device

Choose your device

Random watch 1 ○
Your watch ○
Random watch 2 ○
Random watch 3 ○

Choose your device

Random watch 1 ○
Your watch ●
Random watch 2 ○
Random watch 3 ○

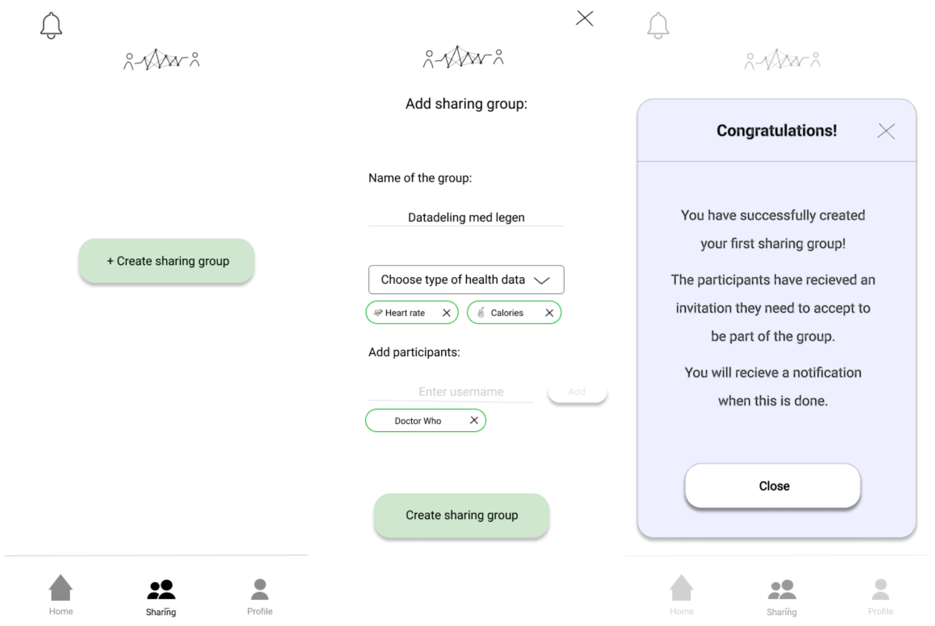
Figure 6.9: Presentation of *Affordance* and *Constraints* in the Figma prototype.

Feedback is the next design principle, illustrated as an example in Figure 6.10. The user is asked to click the "+ Create sharing group" button, fill in the form, and then feedback in form of a notification confirms that it was successful. Using notifications is a direct type of feedback in the app, a more discreet type of feedback is for example the tags with green outlines in the middle screen telling the user what they have chosen. Adding this makes the user more confident in knowing which choices has been made, and where they are in the process of an action.

Mapping is something one learns when using applications in general. An example in the Figma prototype application is the bell with the red circle and the number 1 inside, in the upper left corner of the left screen in Figure 6.11. This is a standard notification icon saying that the user has one new notification. Mapping can often be metaphors to real life actions, in this case it is a bell ringing.

Another example of mapping is the cross in the upper right corner of the middle and right screens in Figure 6.11. Even tough the "Decline" and "Close" buttons at the bottom of the screens communicate that the notification can be closed using one of these, it is also an option to use the cross. Cross equals closing or exiting the current state of the application, similar to when something is crossed out on a piece of paper and is indented to be forgotten.

Visibility is very important for the user in order to know where they are and to not get lost using the application. Figure 6.12 shows how the user can navigate their way through the different screens by using the menu at the bottom of the screen. A menu is a great way to ensure good visibility, and in this case it was important to have as few icons in the menu as



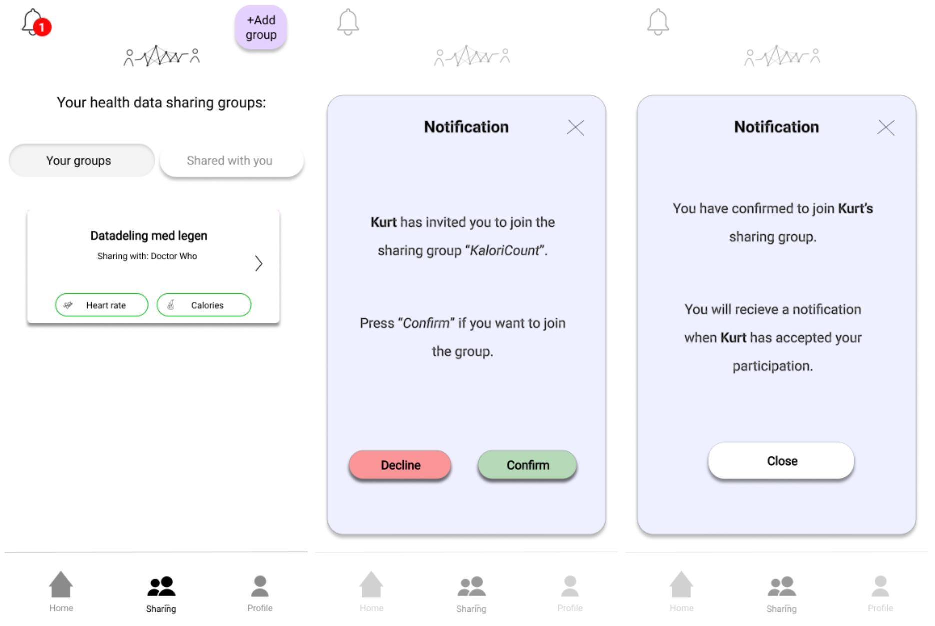
Datadeling med legen

You have successfully created your first sharing group!

The participants have recieved an invitation they need to accept to be part of the group.

You will recieve a notification when this is done.

Figure 6.10: Presentation of *Feedback* in the Figma prototype.



Kurt has invited you to join the sharing group "*KaloriCount*".

Press "*Confirm*" if you want to join the group.

You have confirmed to join **Kurt's** sharing group.

You will recieve a notification when **Kurt** has accepted your participation.

Figure 6.11: Presentation of *Mapping* in the Figma prototype.

possible to make it easier to navigate. The left and middle screen represents how to click in on and out of a data sharing group by using the arrows. The user can use the menu to navigate to the right screen and see the profile. It was desired to add as few elements as possible to each screen throughout the entire application to enhance visibility.

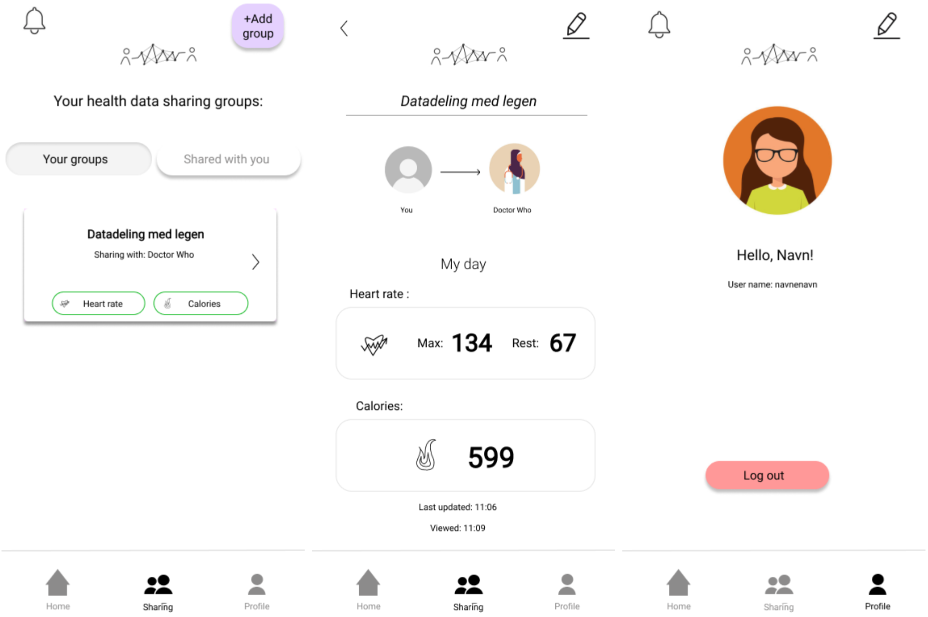


Figure 6.12: Presentation of *Visibility* in the Figma prototype.

The last principle is *Consistency* which can be seen on all the figures above. Consistency is seen in the use of colors, shapes, icons etc. In the Figma prototype all buttons with the same purpose have the same color and descriptive text. The notifications have the same background color to let the user recognize that it is a notification. Icons are consistent, the notification icon will always display notifications anywhere in the application, and crosses will always exit the current state of the application. Theses principles all together ensure the users ability to recognize actions and understand the interaction flow of the application.

6.2.2 First Evaluation: Figma Prototype

In order to assess the usability of the prototype a usability test was created. Five participants of varying age (20-55 years), gender and technical experience were chosen so that the selection, although small, would cover a wider group of potential users, recall Section 3.1.3. The test consisted of a set of tasks that the users were instructed to complete, and an interview to collect feedback, as described in Section 3.1.3. Observing the users gave valuable insight into what was intuitive or not in the interface design.

The tasks were created with the functional requirements in mind. It was desired to make the tasks as realistic as possible, as mentioned in Section 6.1. The tasks with the corresponding requirements is shown in Table 6.3 below.

Requirement	Task
1. Register and log in	You have just installed the new app TangleHealth, you want to register a user and log in to use the app.
2. Pair with smartwatch and synchronize health data	You have a watch called "Your watch" that you have been wearing all day, and thus you would like to connect this to the app to check your heart rate, number of steps and calories burned.
3. Set up health data sharing groups	Yesterday you visited your doctor "Doctor Who", and she told you that she would like you to share your heart rate and calories burnt with her, so you create a sharing group with Doctor Who where you share this data
4. Subscribe to health data sharing groups	Your friend Kurt calls you and says he wants you to see how many calories he burns in a day, you check the app if you have received his invitation. You want to accept this invitation.
5. Visualize the health data	You want to see how many calories Kurt burned in total in January.
6. Customize the user profile	When you enter the group "Data sharing with the doctor", you see that you have forgotten to add a profile picture and want to do this. You're wearing a green sweater and you're a girl.

Table 6.3: Overview of usability test tasks connected with the initial Figma prototype requirements.

The tasks covered all of the proposed features of the Figma prototype. In order to collect as much information as possible during the usability test the participants were told to think out loud and say when they believed a task was completed. This continuous feedback throughout the observation provided valuable insight. In addition, the following questions were asked after the participants had completed the tasks:

Interview Questions

- What was good about the app?
- What was intuitive/easy to understand?
- What was difficult to understand?
- What could have been better?
- Do you feel anything is missing in the app?
- Anything else you would like to add?

These follow up questions provided additional feedback from each participant. Combined with the results from the observations it provided a solid foundation for the second iteration of prototyping.

6.3 Second iteration: Functional Prototype

The development process of the prototype, including the planning, explanation of the technical choices made, and how the development was carried out is presented in this section.

6.3.1 Planning

The system architecture had already been sketched and discussed briefly during the preparatory project [4]. Furthermore, a diagram was created, see Figure 6.13.

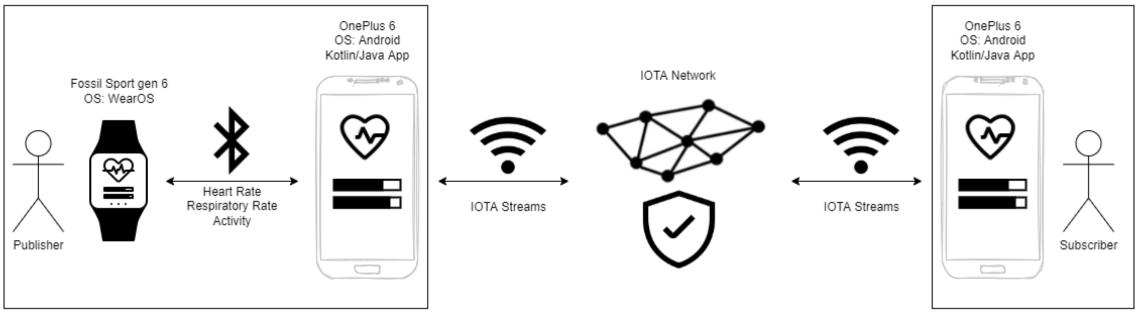


Figure 6.13: Overview of the system architecture of the prototype.

The left side of the figure represents the publisher side, where the publisher monitors their health data through a smartwatch that is connected to a handheld device with an application installed. The application receives the publisher's health data through Bluetooth connection. Further, the health data is sent over the IOTA Tangle network, with IOTA Streams, to a subscriber with another handheld device with the same application installed. The publisher has now collected and shared personal health data with the subscriber, securely and private over the IOTA Tangle network.

An example of how this could be used in the daily life is the publisher being a patient needing to share sensitive health data with their physician, which is the subscriber. Another example could be the publisher being a person who wants to exercise and/or lose weight, where the subscriber is a physical trainer and/or nutritionist helping to supervise. The bottom line is that the application can be used by many people in different life situations.

After the architecture was sketched out it was time to start the development. The Figma prototype was used as a reference on where to begin. The complex visualization of the architecture combined with the detailed Figma sketches made it necessary to divide and conquer the problem into smaller problems. Thus, two lists of functional requirements were constructed. The first list consisting of requirements related to the Android application and smartwatch. These are presented in Section 6.3.3, and initially in Section 6.3.4.

1. Develop a simple version of the application in Kotlin, with input field, a button and an output field
2. Send data from smartwatch to Android application using Wear OS

The second list consisted of requirements related to the IOTA Streams. The implementation of these are elaborated later in Section 6.3.4.

1. Author creates a health data sharing channel
2. Subscriber receives announcement link from Author
3. Subscriber creates a subscribe message that is linked to the channel announcement message
4. Author receives subscribe message link
5. Author uses public key of Subscriber to grant access to the channel
6. Author starts streaming a pre-defined dataset
7. Subscriber retrieves data messages that are then displayed in the health data stream

6.3.2 Technical aspect

How to approach the prototype development was simmering in the back of our heads since the beginning of fall 2021. The IOTA Streams library was always considered relevant to the research topic. The preparatory project confirmed the relevance of the library, due to its extensive use for prototyping in the literature, thus chosen as main technology to use in our solution for this research. This section provides a descriptive justification as to why the specified smartwatch with wear OS, Android Studios and Kotlin was chosen.

IOTA Streams & Rust

After some initial investigation it became clear that the IOTA Streams library was available in the programming languages Rust, WebAssembly and C. The investigation gave the impression that the combination with Rust was the best documented option, both online and in the IOTA Discord, and the most used in GitHub projects. Neither of the authors had any experience with Rust, but being the only high-level programming language of the three made the choice easier. In addition, it is a relatively modern language which made it motivating to learn.

Smartwatch & Wear OS

Contacts at NTNU assisted in selecting a proper smartwatch and compatible OS for health data collection. Smartwatch Fossil Sport Gen 6 with Wear OS was selected. The selection of Wear OS as software for smartwatches lead to an inspection of numerous tech websites ranking the best smartwatches for developers using Wear OS [46–49]. After looking into several guides only two smartwatches remained; Ticwatch E3 and Fossil Sport Gen 6. The latter had better reviews overall and was therefore chosen.

Android Studios & Kotlin

Android Studio was the best Integrated Development Environment (IDE) for this project. It supports running Android applications in both handheld and wearable emulators. Kotlin was the selected language for application development. This was a programming language neither of the researchers had any experience with, but the impression was that it was quite similar to Java, which both researchers had experience with. Kotlin is also a quite popular and modern language making it motivating to learn.

One of the authors had worked in Android Studios ahead of the research project, thus making it painless to get started, set up and run the emulators.

6.3.3 First round of development

With high ambitions, new and exciting technologies, the development started swiftly. Approximately one week was spent on basic setups and installations, the first item in the backlog. Shortly after, the second backlog item, creating an Android application with some basic features was implemented and visible in the emulator.

After two weeks, the implementation of the IOTA Streams Rust library was up an running in the application. In order to execute functions from the IOTA Streams Rust library in the Android application, a binding between Rust and Kotlin was required. For this the Java Native Interface (JNI) was used. Next thing on the list was to create a data sharing channel. This task came with some complications as executing Rust functions that were asynchronous caused the Android application to crash without an error message. A week was spent looking into this issue. During the same week, in order to be productive, the smartwatch was set up. The setup went well, but connecting the watch to the application became a bigger problem than anticipated.

After three weeks, the struggles mentioned above lead to a point in the development were it was time to sit down and evaluate if it was productive to continue in that direction.

6.3.4 Second round of development

Due to the stagnation in the first round of development, it was necessary to remove the Android application and smartwatch from the prototype. Thus, the functional requirements list related to these were removed, recall the first list in Section 6.3.1. The focus now was to create a prototype that demonstrated the core functionality of the IOTA Streams library, namely the creation of a data sharing channel and exchanging health data. Besides, to make the development more productive it was decided to write the application in pure Rust. This made the creation of the sharing channel possible since the error related to running asynchronous Rust functions in the Android application was avoided.

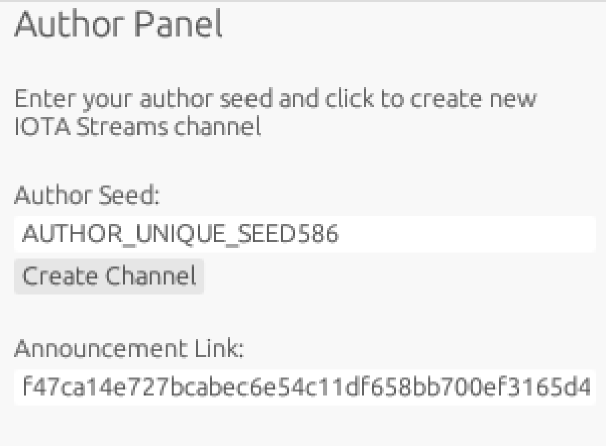
The drawback of creating the prototype in pure Rust was that Rust does not have the best support for making applications with a user interface, thus some time was spent on finding a Rust Graphical User Interface (GUI) framework. After some investigation the Egui framework was chosen, as it was supposed to be one of the easiest Rust GUI frameworks to work with. When developing applications with the Egui framework, Eframe is suggested as the best option, thus used in this project.

GTK is a multiplatform GUI toolkit that was considered for the Rust application's user interface development. It required tons of downloads, and a lot of errors and complications were encountered along the way. It was decided that it was too much effort to use this toolkit.

IUI was another GUI considered used for the user interface of the Rust application. It was simple to set up, but had its issues. Firstly, it was not updated since 2018 making it outdated and full of possible future complications.

Functional Prototype Implementation

Since the prototype was intended to demonstrate the sharing of health data, it was decided that the application would feature a page to create a sharing channel as an Author, see Figure 6.14, where a user can enter their personal unique seed, which is then used to generate the announcement link for the created data sharing channel. The application also needs to support the functionality to subscribe to the generated sharing channel, therefore, a page for a user to insert their unique seed, the announcement link, and to then click subscribe was created, see Figure 6.15. After that the Author processes the subscription, effectively granting access to decrypt the health data using the keyload link, see Figure 6.16. Lastly, after the Author has created the sharing channel and the Subscriber has subscribed to it, and the keyload has been sent, the health data stream is displayed as it is transmitted over the IOTA network, see Figure 6.17. The following figures are snapshots taken during the testing and evaluation of the finished prototype, see section 7.2 for the evaluation of the results.



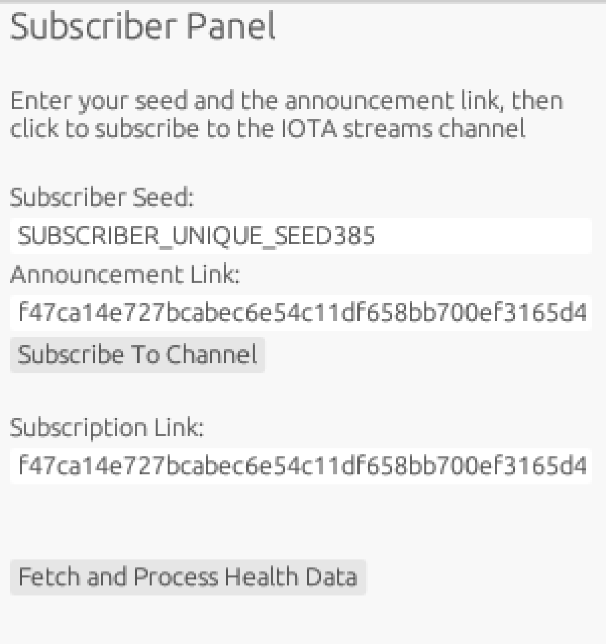
Author Panel

Enter your author seed and click to create new IOTA Streams channel

Author Seed:
AUTHOR_UNIQUE_SEED586

Announcement Link:
f47ca14e727bcabec6e54c11df658bb700ef3165d4

Figure 6.14: Panel for an Author to create a data sharing channel.



Subscriber Panel

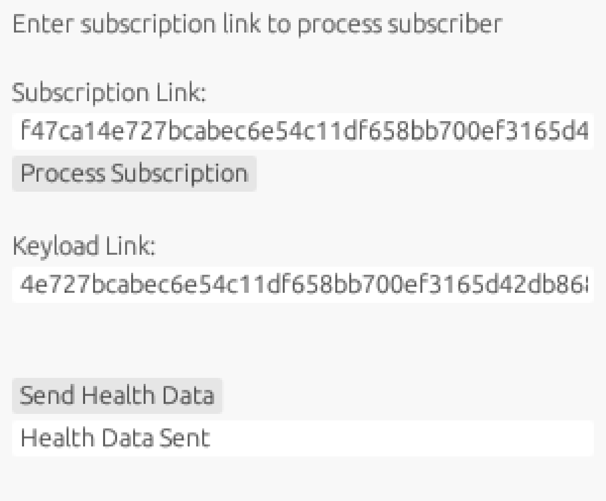
Enter your seed and the announcement link, then click to subscribe to the IOTA streams channel

Subscriber Seed: SUBSCRIBER_UNIQUE_SEED385

Announcement Link: f47ca14e727bcabec6e54c11df658bb700ef3165d4

Subscription Link: f47ca14e727bcabec6e54c11df658bb700ef3165d4

Figure 6.15: Panel for a Subscriber to subscribe to a data sharing channel.



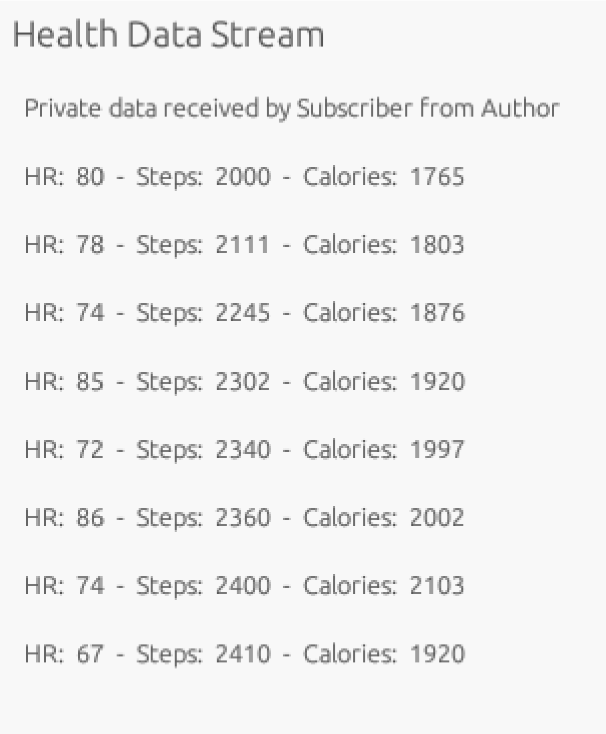
Enter subscription link to process subscriber

Subscription Link: f47ca14e727bcabec6e54c11df658bb700ef3165d4

Keyload Link: 4e727bcabec6e54c11df658bb700ef3165d42db86

Health Data Sent

Figure 6.16: Author processes subscription link.



Health Data Stream

Private data received by Subscriber from Author

HR: 80 - Steps: 2000 - Calories: 1765

HR: 78 - Steps: 2111 - Calories: 1803

HR: 74 - Steps: 2245 - Calories: 1876

HR: 85 - Steps: 2302 - Calories: 1920

HR: 72 - Steps: 2340 - Calories: 1997

HR: 86 - Steps: 2360 - Calories: 2002

HR: 74 - Steps: 2400 - Calories: 2103

HR: 67 - Steps: 2410 - Calories: 1920

Figure 6.17: Panel showing the private health data stream from Author to Subscriber.

Prototype Code

This section presents the most important functions for sharing and receiving health data over the IOTA Tangle using the IOTA Streams library. Each subsection corresponds with one or several functional requirements related to the IOTA Streams listed in Section 6.3.1. The first subsection addresses the first functional requirement. The second subsection addresses both the second and third requirement, similarly the third subsection addresses the fourth and fifth. Moreover the fourth and fifth subsections corresponds to the sixth and seventh requirement.

1. Creates Author and Streams channel

The following code creates a new Author instance and sends the announcement message for the newly created channel to the IOTA network, as seen in Figure 6.14. The code first defines the development network node that will be used, creates a client instance from the node url and then uses the author seed and client to create a new Author instance. The function also takes in a parameter that defines whether the new channel will support single branch or multiple branch communication. After the announcement message is sent the function return the unique announcement link to the created channel. The `.await?` signifies that the function is an asynchronous function that will wait for a response from the IOTA network before continuing.

Code listing 6.1: Creates Author instance from unique seed

```
    let node = "https://api.lb-0.h.chrysalis-devnet.iota.cafe/";

    let client = Client::new_from_url(node);

    let mut author = Author::new(&seed, ChannelType::SingleBranch, client.clone());

    let ann_link = author.send_announce().await?;
```

2. Creates Subscriber and sends subscription

After the Author instance and the new data sharing channel is created, the next step is to create a Subscriber instance that can subscribe to the data shared by the Author, which can be seen in Figure 6.15. The code first creates the Subscriber, followed by receiving the announcement from the announcement link generated by the Author. The subscriber is now listening to activity in the channel, but then needs to send a subscription message and be approved by the Author before it can decrypt the private data stream. The last function returns the address of the subscriber, which the Author can then process in the next step.

Code listing 6.2: Creates Subscriber instance from unique seed

```
let mut subscriber = Subscriber::new("SubscriberA433", client);

subscriber.receive_announcement(&ann_link).await?;

let sub_address = subscriber.send_subscribe(&ann_link).await?;
```

3. Author processes subscription

After the subscriber is created and has sent the subscription message, it can be processed by the Author using the generated subscription address, see Figure 6.16. Then the Author sends out a keyload message with all registered subscribers, which enables the subscribers to decrypt the private data stream.

Code listing 6.3: Author processes the subscription and sends keyload

```
author.receive_subscribe(&sub_address).await?;

let (keyload_link, _seq) = author.send_keyload_for_everyone(&ann_link).await?;
```

4. Author sends health data

In this prototype the health data is simply a predefined vector of strings that represents what a health dataset could look like. In a finished product the health data would be generated in real-time by sensors worn by the user. The for-loop iterates over the messages and sends each message as a signed packet to the IOTA network. This section of code is run when the Author clicks "Send Health Data", see Figure 6.16

Code listing 6.4: Author sends health data as a vector of strings

```
let msg_inputs = vec![
    "HR: 80, Steps: 2000, Calories: 1765", "HR: 78, Steps: 2111, Calories: 1803",
    "HR: 74, Steps: 2245, Calories: 1876", "HR: 85, Steps: 2302, Calories: 1920",
];

let mut prev_msg_link = keyload_link;

for input in &msg_inputs {
    let (msg_link, _seq_link) = author.send_signed_packet(
        &prev_msg_link,
        &Bytes::default(),
        &Bytes(input.as_bytes().to_vec()),
    ).await?;
    println!("Sent msg: {}, tangle index: {:#}", msg_link, msg_link.to_msg_index());
    prev_msg_link = msg_link;
}
```

5. Subscriber processes data

The following code first fetches the messages sent by the Author and then processes each message. The code executes when the Subscriber clicks "Fetch and Process Health Data", as seen in Figure 6.15. The process decrypts and converts the data back to a vector of strings, which is then visualized as seen in Figure 6.17.

Code listing 6.5: Subscriber fetches and processes health data sent by the Author

```
let retrieved_msgs = subscriber.fetch_next_msgs().await;

let messages = retrieved_msgs.unwrap_or_default();

let processed_msgs = messages
    .iter()
    .map(|msg| {
        let content = &msg.body;
        match content {
            MessageContent::SignedPacket {
                pk: _,
                public_payload: _,
                masked_payload,
            } => String::from_utf8(masked_payload.0.to_vec()).unwrap(),
            _ => String::default(),
        }
    })
    .filter(|s| s != &String::default())
    .collect::<Vec<String>>();

for msg in processed_msgs {
    println!("{}", msg);
}
```

6.3.5 Second Evaluation: Functional Prototype

In this section, the process of testing the prototype is described. The results of the tests will be presented in Chapter 7.

The plan was to perform a usability test with five participants for the prototype, similar to the one performed on the Figma prototype, but the time constraints made it difficult to pursue. However, the prototype needed to be tested and it was decided to perform a functional test of successful exchange of private health data. Functional testing focuses on verifying the outcome of an action [50]. The evaluation is inspired by the paper by Brogan et al. [34], that researched the ability of MAM to broadcast and receive authenticated, encrypted activity data from a wearable device.

The functional test consisted of the execution of the steps listed below. These are the same as the functional requirements listed in the second list of Section 6.3.1.

Evaluation Steps

1. Author creates a health data sharing channel
2. Subscriber receives announcement link from Author
3. Subscriber creates a subscribe message that is linked to the channel announcement message
4. Author receives subscribe message link
5. Author uses public key of Subscriber to grant access to the channel
6. Author starts streaming a pre-defined dataset
7. Subscriber retrieves data messages that are then displayed in the health data stream

If all steps are completed correctly the prototype will have demonstrated that it is possible to share health data in a decentralized way over the IOTA network.

Chapter 7

Results

This chapter outlines the results from the development and testing of two iterations of health data management prototyping. Section 7.1 presents the results from evaluating the Figma prototype developed in the first iteration, both from the usability test and post-observation individual interviews. Finally, Section 7.2 summarizes the results from the evaluation of the functional prototype developed in the second iteration.

7.1 Figma Prototype

This section summarizes the results from the usability testing of the first prototype and the feedback from individual interviews. Table 7.1 lists the participants in the testing of the Figma prototype.

Participant	Gender	Age Range	Technical Experience
1	Male	20 - 25	Informatics Master's Student.
2	Female	25 - 30	Informatics Master's Student.
3	Male	30 - 35	Professional Software Engineer.
4	Male	40 - 45	Owns a Android phone, primarily used for calling and texting.
5	Female	50 - 55	Owns an iPhone and an iPad, has a basic technical understanding.

Table 7.1: Overview of Figma prototype test participants.

7.1.1 Observation Results

The following table summarizes the observations made during each task that the participants performed in the usability test. The tasks listed in Table 7.2 correspond to the tasks described in subsection 6.2.2.

Task	Observations
1	All participants understood and performed the task correctly.
2	Participants 3 and 5 did not understand that they had to click "Sync and update data" to get latest data from the watch, they did, however, correctly connect to the watch as the rest of the participants.
3	Participants 1, 2, 3 and 5 did not understand that they had to click the notification icon to confirm the subscription from "Doctor Who" to complete the task. Participants 3 and 4 clicked the text instead of the checkbox when trying to select the type of data to share.
4	Participants 4 and 5 thought the last notification confirming that Kurt has accepted the subscription was unnecessary, while participant 3 thought it was a duplicate. Participant 5 took some time to understand that the new group could be found on the "Shared with you" page.
5	Participants 1, 3 and 5 struggled to read the small text on the graphs. Participants 1 and 3 mistakenly read the value for steps instead of calories burned. Participant 2 thought that the months were clickable and was confused when it did not work.
6	Participants 2 and 3 were confused at first, but eventually clicked the "Edit profile" icon after first trying to click the profile picture. Participant 5 thought that the "Edit profile" icon meant that they were supposed to draw something, understood that it meant "Edit profile" after approx. 15 seconds.

Table 7.2: Results from usability test observation.

7.1.2 Post-Observation Individual Interview

This is a summary of the feedback from the individual interviews where the participants were asked the questions listed in section 6.2.2.

Positive Aspects

Participant 1 thought the application had a "visually appealing design", that the icons and buttons were easy to understand, and that it was clear when something was active/clickable and when something was not. Both participant 1 and 2 noted that the visual representation of the health data was good. Participant 2 said she "appreciated the simplicity of both the process of connecting to the watch and creating a sharing group", which was also noted by participant 5. participants 1 and 3 both commented that the notifications were useful and made the process easier to understand. Participant 2 said that she appreciated that "the application did not have too many buttons and icons", which can lead to confusion. In regards to the icons used, participant 3, 4, and 5 said that they found them easy to understand.

Potential For Improvement

On the negative, participant 1 said that he wished that "registering also logged you in to the application". Participants 1 and 4 noted that the health data should sync automatically after connecting to a watch. When it comes to the notifications, participant 1 said that they felt that the "notifications all looked similar" and you would have to read every single one to understand the process, participant 1 also wished that there was a log of all notifications. Participant 2, 3, and 4 felt that there were too many notifications, and that it seemed unnecessary to confirm a user's subscription to a sharing group after that person has already been invited by the author. Participant 1 also noted that it looked like the sharing group was created successfully even though the subscriber still needed to be confirmed for the sharing to begin. Participants 3 and 4 felt that choosing a name for the sharing group was difficult and would like that the application gave recommendations for good naming standards. The visual representation of the data as graphs on the archive page was commented by participants 1, 2, and 4; they agreed that the graphs could be improved. Participants 1 and 4 did not like the use of line graphs, and participant 4 said that "a bar chart would be better". Both participants stated that it was confusing that selecting the "month" view showed the full year instead of a single month. They also noted that the text was too small. Participant 2 said that since the current month was highlighted in green it gave the impression that the months were clickable when they were not. When it came to editing the profile, both participants 3 and 5 commented that they expected the profile picture to be clickable, since that is what they are used to from other websites and applications. Participant 3 had some feedback in regards to the smart watch/Bluetooth icon, namely that he said that "the Bluetooth icon was superfluous" and that he would prefer a green or red dot next to the watch to indicate if it is paired.

Desired Features

Participants 1 and 4 wished that they could get a more detailed look at their own and others health data, and participant 1 said that "it would be nice to see whether or not the person you are sharing with has viewed your health data". Participants 2 and 3 wanted more information about how the IOTA Tangle and the application functions, as well as more options for data to share. Participant 5 said that there was "a lack of colour" and that that made it slightly boring to look at.

Additional Comments

Participant 1 felt that the "add group" button should be positioned in the feed itself, that notification should say "understood" instead of "close" on the button, and that a red or green indicator for pairing would make more sense than a Bluetooth icon. Participants 2 and 4 found it hard to find the log out button. Participant 3 did not immediately understand what the numbers for max and min heart rate were supposed to mean, in addition, the participant said that he wished "to move the add group button to the center below you data sharing groups feed".

7.2 Functional Prototype

This section presents the results from the evaluation of the prototype described in subsection 6.3.5. A successful test depends on all seven steps executing correctly.

Evaluation Steps

1. Author creates a health data sharing channel
2. Subscriber receives announcement link from Author
3. Subscriber creates a subscribe message that is linked to the channel announcement message
4. Author receives subscribe message link
5. Author uses public key of Subscriber to grant access to the channel
6. Author starts streaming a pre-made dataset
7. Subscriber retrieves data messages that are then displayed in the health data stream

Each of the seven steps listed above were successfully executed and visualized in the prototype dashboard, see figures under section 6.3.4. The results from the evaluation of the prototype show that the prototype was able to demonstrate private, secure and decentralized sharing of health data over the IOTA Tangle.

Chapter 8

Discussion

This chapter discusses the RQs in accordance to the research conducted in this project. First the two RQs are discussed in separate sections, followed by a review of the limitations and ethical aspects of the research. This will lay the foundation for the conclusion presented in Chapter 9.

8.1 RQ1: How can IOTA Tangle provide reliable and secure health data management?

Health data management moves in the direction of becoming fully digital, even developing countries are replacing paper records with EHRs, as stated by Jamshed et al. [6] in Chapter 2. Digitalization can provide more efficient, flexible and accessible systems, in addition to decreased costs and increased work quality. Automated solutions are suggested in the expert interviews in Chapter 5, for example proactive patient care, where patients use automated systems to receive medical help from home. Another suggestion is ownership of data, where patients gain more control and insight in their health, and lastly automated decision making, where systems and algorithms can learn how to automatically look after patients and provide their medicine. Issues that may arise from digitalization are system vulnerabilities such as security attacks, privacy abuse, data inaccuracies, and system errors. The list is endless, and the consequences high due to the sensitivity of health data. That is why it is important to look into how the IOTA Tangle can solve these vulnerability issues.

Reliable and secure health data management is equivalent to data being exchanged and stored according to its specifications without any interruptions, intruders or errors.

The SMS in Chapter 4 discusses RQ1 and concludes that due to its DAG architecture, decentralized approach and communication tool IOTA Streams (previously MAM), the IOTA Tangle could indeed provide reliable and secure health data management. Although the SMS presented a conclusion in regards to the potential of the IOTA Tangle, it was still desired to keep the RQ for further investigation in this Master's Thesis. The expert interviews was a natural next step to acquire more information. The aim was to research if the expert knowledge would strengthen or challenge the conclusion of the SMS. The expert interviews in Chapter 5 summarizes the issues faced in the health sector today, suggestions for improvement, and future predicaments. This discussion seeks to combine the two perspectives to answer RQ1.

Existing Weaknesses & Limitations

Looking at health data management today the two experts had several limitations and weaknesses to point out, recall Section 5.4. Interoperability between systems is the first weakness mentioned by both as one of the main problems. Interoperability is defined in background Section 2.4.3 as the ability to interact and exchange data between multiple systems. This is one of the special traits DLTs provide, and therefore also the IOTA Tangle. It is stated in the SMS through the work of [29], Farahani et al. [2], and Houtan et al. [30] that low scalability and low interoperability is one of the main reasons Blockchain is not suitable for health data management systems in terms of privacy. They also point out that this issue can be solved by using the IOTA Tangle due to its high scalability achieved through the DAG structure enabling parallel transactions, and its use of IOTA Streams. IOTA Streams, as mentioned in Section 2.4.5, makes it possible to structure and publish encrypted data on the IOTA Tangle in channels known as Streams. It is important to briefly mention that Blockchain is used as a reference point due to its success in the market today, see Section 2.4.4. Blockchain is used in several health care systems [51] and has the same principles as the IOTA Tangle, thus a natural choice for comparison.

Expert 2 adds another perspective to the discussion by mentioning semantic interoperability. The expert supports the conclusions of the three research studies in the previous paragraph [2, 29, 30] by saying that the IOTA Tangle would work for a basic level of interoperability, but explains that on a semantic level the systems need to analyse and interpret the data as well. In Section 5.4.1, it is explained that if temperature data is going to be sent from a system, then the right denomination and information regarding the instrument used has to be included in order for the receiving system to display intuitive information. This is beyond the scope of what the IOTA Tangle can do on its own. This perspective clarifies the importance of evaluating what type of health data is going to be exchanged in a health data management system.

Looking into the security aspect of health systems, expert 2 adds that immutability may cause limitations. Immutability is described in the background, Section 2.4.2 as a transaction that can not be altered or reversed. In other words, the message sent will be the one arriving. Automated decision making, already becoming more used in health care, as pointed out in Section 5.5.3, may pose a significant risk without immutability. Further, if data gets corrupted this could lead to the algorithms making wrong decisions, thus providing wrong medication or amount of medication to patients. This is dangerous as a patient could die from such a deviation. The SMS presents solutions for security issues through the work of Saweros and Song [11], Silvano et al. [33], and Florea et al. [31], additionally this is supported by Hawig et al. [3], Zheng et al. [32], and Brogan et al. [34] emphasizing the security aspects with their demonstrating research prototypes. Highly-scalable, interoperable, tamper-proof, and immutable, were some of the key features mentioned in the these studies to describe important features of the IOTA Tangle.

Further, the expert adds another aspect of security issues by pointing out that larger institutions require large firewalls, but the consequence of increasing the firewall size is that it may lead to security weaknesses. Holes in the wall and man-in-the-middle-attacks, where intruders alters the communication between parties, can potentially threaten the security. The solution the IOTA Tangle offers is immutable and incorruptible transmission of data between institutions. This is something the conclusion from the SMS agrees with. Section 4.2 talks about how data inaccuracies can be prevented with the IOTA Tangle due to its immutable, secure, and tamper-proof data transmission [31–33]. This is also emphasized in terms of the privacy aspect by several of the other primary studies such as [3] and [34]. It is important to remember that many DLTs can handle this security aspect, as pointed out in Section 2.4, meaning that the IOTA Tangle is not unique in this sense.

Possible Improvements & Solutions

Two main solutions were suggested by the experts in terms of how to improve health data management. The first proposal being proactive patient care, which is the combination of EHRs and PHRs, written about in Section 2.1. In Section 5.5.1, Expert 1 supports the suggestion by adding that it is the main goal of their workplace to make it possible for patients to stay at home longer and receive the follow-up they need, without having to travel to the hospital every time. Further, it is emphasized that with this approach the hospitals and patients will save time, and have the opportunity to be more flexible and efficient in their correspondence with each other. However, this approach opens up for several complications. A health data management system supports proactive patient care would need to ensure security and privacy through interoperability, immutability, scalability and efficiency, making the IOTA Tangle a suitable choice. Saweros and Song [11] successfully managed to create such a system where patients could be in control of their own data in correspondence with health personnel.

The proactive patient care is an interesting approach suggesting more accessible, flexible and efficient health data management, but it is easy to forget that there is a non-technical side to this approach. Even though the IOTA Tangle looks promising in terms of privacy and security there is still room for error. Expert 1 mentions that their approach to this is that the patient sends their health data via an application instead of visiting the hospital. This saves time, but the risk of not monitoring and sending all necessary data is still there if something were to happen to the application, phone, or internet connection. There are many external factors that have to align in order for this to work perfectly. Consequently, the physician will not receive all data and is not fully updated on the patient's health status. Another aspect of this is the medicine dispenser, as described in Section 5.5.1, the patient's get as a substitute for health care personnel to show up an give them medicine several times a day. What if there is an error with the dispenser and the patient is unable to take their medicine on time, and forgets to let the hospital know? The main challenge with this approach is the increased responsibility of the patient. Thus, it is important to establish whether or not the patient is fit to take this responsibility.

The other topic discussed by the experts was ownership of data, which is related to decentralization. Decentralization is an important property described in the SMS and Section 2.4.1, explaining it as a secure collaboration between multiple participants as opposed to the control of one single administrator. The essence is that data is spread across the network and there exists no single point of failure. Data is stored directly, locally and encrypted instead of passing through a third party service. Each transaction in the network requires thousands of validations from other nodes ensuring reliability and integrity. Both experts agree that patients should have individual ownership of their own data. Expert 2 emphasizes how decentralization and the IOTA Tangle can use pseudonymization with IOTA Streams in order for people to control and curate their own data, recall Section 5.5.2. Traditionally, this data is kept by the platform provider, for example Google or Apple, and even if a graph of the data is presented to the user, it is now owned by a large company and personal ownership is lost. To support this the SMS points out three studies demonstrating decentralized systems by combining the IOTA Tangle, IoT/IoMT, and MAM [31–33] .

The future of health data management

In the future there is no doubt between the experts that interoperability between all types of health care institutions needs to be prioritized, recall Section 5.6. The issue seems to be the various incompatible systems with little room for change and new integration. According to expert 2 there exists few incentives for big vendors to implement interoperable systems. Big vendors have great power in the health care industry and may refuse to prioritize interoperability since it is hard to implement and since sharing valuable data with other companies and institutions may not be profitable. The expert believes that as the IOTA Tangle matures it will become an essential tool for sharing sensitive health data and that it could make the development of interoperable systems more lucrative. The demonstration of interoperability in a large and diverse health care ecosystem by Brogran et al. [34], a solution based on the IOTA Tangle, IoMT, and MAM, is a potential beginning to changing their perspective.

8.2 RQ2: How should a health data management application built with the IOTA Tangle be implemented?

There are many aspects to proper implementation of health data management systems. It should be implemented in accordance to rules and regulations, it should follow design principles, and technical considerations. The following discussion reflects on the RQ based on the knowledge gained through the conducted expert interviews, and the development and evaluation of the prototypes.

Rules, Regulations & Requirements

First of all, the rules and regulation aspect is important to take into consideration due to the health perspective. Although this section emphasizes the importance of this aspect it has not been assessed in the prototyping. The aim of this research was to develop a prototype to answer the RQs, not launch a fully working health application. The reason why this aspect is included is to visualize the complexity of what further development would need to include. The expert interviews reveals that CE marking and ISO standards are important regulations to show that the product complies with general and specific standards.

Expert 1 also mentions the customer requirements, which are important for the prototype. This is often presented through a customer requirement list and must cover usability standards. The approach to this in this research was to create a list based on the expert interviews and SMS. In retrospect, the ideal situation would have been to create a requirement list together with potential users of the prototype.

User Interface and Design

This section discusses the user interface and design aspect of the prototype in light of the RQ. In order to figure out how the prototype should be implemented it was necessary with a thorough investigation, inspired by Preece et al. [42] and Vaishnavi and Kuechler [24], and then build it from scratch. This section discusses the first iteration in adherence to RQ2.

Developing the Figma prototype based on the requirements, mentioned in the previous section, made it easy to divide the user interface into tasks that could be tested by the users in a usability test, recall Section 6.2.2. Inspired by Preece et al. [42] the prototype adapted the

Don Norman design principles. According to the results from the usability test and individual interviews in Chapter 7, the first principle *Affordance* was achieved to an extent. The participants were pleased with the visually appealing design, an that the icons and buttons were easy to understand. This proves that the effort of choosing bright colors, descriptive text and having important features in focus worked, recall Figure 6.9. The negative feedback regarding affordance included the "sync and update" button to import and update the health data from the smartwatch to the phone. It was anticipated by two of the participants that this should happen automatically. It was later discussed between the researchers that it most likely was due to the different approaches smartwatches on the market today has towards this functionality. The prototype was based on the Garmin Connect app, where there is a button for update and synchronization instead of it happening automatically.

The next principle, *Constraints*, was successfully addressed. The participants mentioned that it was easy to understand when something was clickable or not clickable, active or inactive. The simple user interface with a minimal amount of options was also appreciated by the participants, implying that this principle lead to an intuitive and pleasant overall experience of the app. The *Feedback* principle received mixed feedback from the participants. This was addressed by using notifications, were one participant said it was too many notifications, another one pointed out that they contained to much text and information, and it was also mentioned that it was confusing that they were the same color. The notifications should indeed have different colors to communicate different types of feedback. In addition, the lack of a notification log was criticized. It was, however, not prioritized in the prototype as it is a lot of extra work to implement. The main reason the notifications were criticized originates from poor implementation of the *Visibility* design principle. The goal of this principle is for the user not to get lost in the app, and due to the IOTA Tangle and IOTA Streams there were some architectural aspects that needed to be taken into consideration in the user interface. IOTA Streams, recall Section 2.4.5, requires a three way handshake when creating and subscribing to channels, or in this case the sharing groups, explained in Section 6.2. This lead to many notifications being the solution to the problem in order to always keep the user posted on where in the process of establishing a sharing group they were. It is understandable that reading a lot of text many times feels excessive and unnecessary, thus other possible solutions to this should be investigated. One example could be to explain by text or an introduction how the three-way-handshake works and why it is necessary. Another solution could be to add more descriptive text integrated in the app (not in notifications) saying "pending" or "waiting for response".

The next principle is *Mapping*, which is tricky since it relies on people's previous experience with similar technology and especially mobile applications. This is the main reasons for the variety of technical experience among the participants. Most of the buttons and icons were understandable, but there were some issues in terms of the graphs showing health data from the archive. The graphs were difficult to read due to small text, and one participant mentioned it would be better to replace the line graph with a bar chart. This is agreeable since it is what they use in other health applications such as the Garmin Connect app. This reveals that some essential features were overseen when looking for inspiration, and underlines the importance of looking into already existing solutions and consider all aspects of these. Another aspect of mapping, questioned by the participants, was the watch icon, and how it showed that the connection between app and smartwatch was established or not. The majority pointed this out and suggested to replace the Bluetooth- and Check Mark icon next to the watch with a green and red circle. This may be a more intuitive way to improve the mapping of the functionality. One last confusing feature that made the mapping poor was the profile picture not being clickable. Although this is not an essential feature of the app it is important to mention it due to the expectations people have. The overall impression and experience affects the user and their perception on whether they want to use the application or not. Thus, all features should hold certain standards even though they may not seem very important.

The last principle is *Consistency*. This principle was successfully addressed according to the results. The buttons and icons were consistent, the use of colors were consistent and thus there were no negative feedback in relation to this. There are some minor features listed in the results that have not been referred to in this discussion, yet the overall design principles have been addressed in regards to the most important and relevant statements from the results.

Technical Aspect

The second iteration of development revolved around the implementation of the functional prototype of the health data management system. As mentioned in subsection 6.3.4, after three weeks of development and with several issues encountered, the decision was made to reduce the complexity of the prototype. The following section will discuss the technical aspects of application implementation related to the two iterations of the functional prototype.

The IOTA Streams organizational tool is essential for the realization of decentralized and private health data management, see Section 2.4.5. Without this tool, health data management on the IOTA Tangle would not be possible. Therefore, the method of implementation of the IOTA Streams library is the first consideration that should be made when developing an application that needs to handle private data. It is the entrance point to the IOTA Tangle and both iterations of the functional prototype managed to implement the library in the Android application and the pure Rust version.

One of the major issues, however, when trying to run a library written in Rust on a Kotlin based Android application is the necessity for binding the execution of Kotlin code with the execution of the IOTA Streams functions. This required the use of a secondary framework, namely the Java Native Interface (JNI), as mentioned in subsection 6.3.3. This meant that for every core functionality in IOTA Streams, such as creation of a data channel, a developer would have to write the Rust function for data channel creation, a function using JNI that translates the function to something Kotlin can understand, and finally the Kotlin function that handles interaction with user interface. While the initial implementation binding these functions showed promise, as the creation of a data channel in the application was successful, it became clear, that as the application grew that the amount of work to correctly bind all the required IOTA Streams functions with Kotlin code would take a long time. In addition, as mentioned in subsection 6.3.3, the IOTA Streams library uses several asynchronous function calls, which caused an unknown error when attempting to run the function in the Android application.

The second of development of the functional prototype focused purely on demonstrating that the private, secure and decentralized sharing of health data was possible using the IOTA Tangle. Reducing the complexity of the health data management prototype made the implementation significantly easier, as the chosen GUI framework, mentioned in 6.3.4, was based on pure Rust and therefore did not require any bindings to use the IOTA Streams Rust library. In addition, executing the necessary asynchronous IOTA Streams functions now worked as intended.

An important consideration when implementing a data management application using IOTA Streams is that the after an Author has created a new data sharing channel, the generated announcement link must be sent or made available to the intended Subscribers. This was easy to do in the Rust prototype since the dashboard allowed the user to simply copy and paste the announcement link from the Author panel to the Subscriber panel, see Figure 6.14 and Figure 6.15. Going beyond a prototype, the sharing of the announcement link must be done through a second layer unrelated to the IOTA Tangle, which will have its own security concerns. This would still, however, maintain the privacy of the health data as it is not enough to simply have the channel link to decrypt the data sent, for this the Author must also authorize the Subscribers through the keyload message, as seen in Figure 6.16.

The evaluation of the Rust prototype, see section 7.2, showed that the prototype successfully executed the steps necessary to exchange private health data from an Author to one or several Subscribers. Reducing the number of components from the first iteration of the functional prototype to the second proved critical in order to validate that the IOTA Tangle with IOTA Streams supports decentralized, private, and secure health data management. The IOTA Streams library is well documented and is easy to use, especially if one is familiar with Rust programming, and it takes relatively few lines of code in order to implement private data exchange, see section 6.3.4. One challenge, however, is that there are few real world projects and applications to draw inspiration from, as this technology is still fairly novel.

Since the development of the first iteration of the prototype, that included the smart watch and Android application, halted due to time and complexity, the aspect of real-time monitoring and data exchange using smart sensors could not be explored further. Therefore, it is difficult to discuss if the implementation of IOTA Streams in a IoT or IoMT setting is advisable from the knowledge gained through the development of the prototype. Based on previous research on the feasibility of using the IOTA Tangle in IoT, such as the papers by Brogan et al. [34] and Zheng et al. [32], it is still reasonable to expect that the implementation is possible.

8.3 Limitations

The chosen design and creation approach, with five steps iteration by Vaishnavi and Kuechler [24] as described in Chapter 3, had great potential. However, an increased number of iterations could have been beneficial. Each iteration contributes to deeper insight and understanding of what could be improved with the prototype and what the users want. Due to limited time this was not possible. Despite knowing the time constraints, the project was affected by the lack of experience and resources due to the novel combination of technologies chosen. Although the Gannt chart, recall Section 6.1 and the Trello board, recall Section 6.1 made the planning and execution of tasks easier, the development phase delayed the process by several weeks. It is not clear whether or not the Android prototype, as it was intended to function, could eventually have been realized. Given more time or with developers more experienced with the technology, the prototype as envisioned in subsection 6.3.1 may still be a realistic idea for a health data management system. The ongoing Covid-19 pandemic also made it challenging to get in contact with people outside personal contacts and especially hard to get in contact with patients, who were in the at risk group. The restrictions did not allow unnecessary physical contact or visits with patients during the pandemic [52].

In regard to participants, both the expert interviews and usability testing might benefit from different approaches. The expert interview only included two interviews and it is arguable that the research could benefit from adding at least one or two more. The results from these interviews, in addition to the SMS, was and still is considered sufficient, yet more perspectives could potentially nuance the discussion even further. The same goes for the usability testing and individual interviews participants. Although the graph in Table 3.4 in Chapter 3 shows that after five participants the curve flattens this is only based on one experiment. It does not imply that this is true for all usability tests, as argued in the research by Alroobaea and Mayhew [53].

8.4 Ethical aspects

This section looks the ethical aspects encountered throughout this research. The Norwegian National Research Ethics Committee [27] has established rules for ethics in research. In Section 3.3.2 four requirements are listed, summarizing the rules of ethics, sought to be followed in this research. This was achieved through having the participants sign the consent form, presented in 3.3.1 and added in Appendix C. The consent form specifically declared the purpose of the project and explained the rights of the participant. In addition, it emphasized that participation was voluntary and one could at any time withdraw the consent without giving a reason. It was explained how the data collected were to be stored and processed, and that the participants at any time had the rights to ask to access the collected data. The participants were also given a choice to check off whether they wanted to be anonymized or not, regardless of this it was decided to anonymize both.

The data collected is, as stated in Section 3.4, securely stored in a private folder in the Microsoft Teams with restricted access. It is stored anonymized, and it will all be deleted in December 2022. The audio files from the expert interviews were deleted after they had been transcribed.

Chapter 9

Conclusion

An analysis of the IOTA Tangle in connection with health data management has been presented in this master's thesis. Chapters 2, 4,5, and 6 resulted in the findings of Chapter 7 providing a basis for the discussion in Chapter 8. The discussion sought to reflect on the RQs and their respective conclusions are presented below.

9.1 RQ1: How can the IOTA Tangle provide reliable and secure health data management?

The SMS, Chapter 4, concluded that the IOTA Tangle can provide reliable and secure health data management due to its DAG data structure, decentralized approach, and communication tool IOTA Streams. This research aimed to further research the validity of this conclusion through conducting expert interviews. As pointed out by several of the primary studies, the weaknesses of traditional solutions for health data management, such as lack of interoperability, lack of data ownership, data fragmentation and low scalability, are reiterated by the experts, reinforcing the conclusion from the SMS. At the same time, the primary studies point to the capabilities and properties of the IOTA Tangle as promising for resolving these weaknesses. Similarly, the expert interviews concludes that IOTA Tangle will play a role in the future of health data management, especially in regards to improved interoperability and authenticity of health data. The conclusion is that the findings from the the expert interviews and SMS together support that the IOTA Tangle can provide reliable and secure health data management.

9.2 RQ2: How should a health data management application built with the IOTA Tangle be implemented?

There are three important aspects to consider when implementing a health data management application; regulatory, design, and technical aspects. The regulatory aspect involves adhering to standards and rules in terms of security and privacy in the health care sector. Examples of such regulations are the ISO standards and CE marking. This aspect is critical to consider due to the sensitivity of health data. The design aspect assesses how to create an intuitive, inviting and error reducing user interface. This can be achieved through applying the Don Norman design principles, outlined in Section 6.2.1.

The technical aspect focuses on which programming languages, frameworks, libraries, and general technical tools to use. Central to the realization of private and secure health data management on the IOTA Tangle is the IOTA Streams organizational tool. Thus, any implementation must first consider how this tool can function together with other programming languages, frameworks etc. The prototyping was unsuccessful in terms of implementing IOTA Streams in an Android application, due to issues running the asynchronous Rust functions together with Kotlin code, as described in Section 6.3.3. However, the Android application prototype, as it was envisioned, may still be possible to implement given more time. Reducing the complexity of the prototype made implementation significantly easier since it was written in pure Rust code. This prototype successfully demonstrated sending private health data between two users. Developers must consider the three-way handshake required to establish a private and secure channel on the IOTA Tangle for the exchange of health data. Also, since data sent over the IOTA Tangle can not be altered after being sent, due to the immutability property, data accuracy is essential.

9.3 Limitations

Research limitations were associated with the execution of the research method, specifically the limited number of expert interviews and iterations of prototype development and subsequent testing. In addition, limitations such as the consequences of Covid-19 restrictions, time constraints and the researchers' lack of experience with the technologies affected the research. However, the main limitation of the research was the scope of the prototype, which only covers a basic demonstration of health data management on the IOTA Tangle.

9.4 Contribution

This thesis adds to the limited number of studies exploring the IOTA Tangle from a health perspective. Thus, contributing to researchers and software developers in this field. The research has investigated, through answering RQ1, the opportunities and possibilities for the IOTA Tangle to provide reliable and secure health data management. Additionally, the findings from answering RQ2 may assist software developers to implement solutions with the IOTA Tangle.

9.5 Future Work

The gathered results and findings has established a solid foundation for further work on a full-scale application. Future research could build on the knowledge regarding how to implement a health data management system with the IOTA Tangle, and also how this could potentially improve health care systems. There are still aspects of the IOTA Tangle that needs to be further investigated, and the IOTA Foundation is continuously developing and improving it.

Bibliography

[1] E. H. Lund, L. Jaccheri, J. Li, O. Cico and X. Bai, 'Blockchain and sustainability: A systematic mapping study,' in *2019 IEEE/ACM 2nd International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB)*, IEEE, 2019, pp. 16–23. DOI: `10.1109/WETSEB.2019.00009`.

[2] B. Farahani, F. Firouzi and M. Luecking, 'The convergence of iot and distributed ledger technologies (dlt): Opportunities, challenges, and solutions,' *Journal of Network and Computer Applications*, vol. 177, p. 102 936, 2021. DOI: `10.1016/j.jnca.2020.102936`.

[3] D. Hawig, C. Zhou, S. Fuhrhop, A. S. Fialho, N. Ramachandran *et al.*, 'Designing a distributed ledger technology system for interoperable and general data protection regulation–compliant health data exchange: A use case in blood glucose data,' *Journal of medical Internet research*, vol. 21, no. 6, e13665, 2019. DOI: `10.2196/13665`.

[4] E. Rydningen and E. Åsberg, *Health data management the iota tangle: A systematic mapping study*, Dec. 2021. [Online]. Available: `https://studntnu-my.sharepoint.com/personal/marhh_ntnu_no/_layouts/15/onedrive.aspx?id=%5C%2Fpersonal%5C%2Fmarhh%5C%5Fntnu%5C%5Fno%5C%2FDocuments%5C%2FProjects%5C%2FErika%5C%2DEivind%5C%2Epdf&parent=%5C%2Fpersonal%5C%2Fmarhh%5C%5Fntnu%5C%5Fno%5C%2FDocuments%5C%2FProjects&ga=1`.

[5] T. Heart, O. Ben-Assuli and I. Shabtai, 'A review of phr, emr and ehr integration: A more personalized healthcare and public health policy,' *Health Policy and Technology*, vol. 6, no. 1, pp. 20–25, 2017. DOI: `10.1016/j.hlpt.2016.08.002`.

[6] N. Jamshed, F. Ozair, A. Sharma and P. Aggarwal, 'Ethical issues in electronic health records: A general overview,' *Perspectives in Clinical Research*, vol. 6, no. 2, p. 73, 2015. DOI: `10.4103/2229-3485.153997`.

[7] K. Foote, *A brief history of the internet of things*, 2016. [Online]. Available: `https://www.dataversity.net/brief-history-internet-things/`.

[8] J. Gubbi, R. Buyya, S. Marusic and M. Palaniswami, 'Internet of things (iot): A vision, architectural elements, and future directions,' *Future generation computer systems*, vol. 29, no. 7, pp. 1645–1660, 2013. DOI: `10.1016/j.future.2013.01.010`.

[9] S. Vashi, J. Ram, J. Modi, S. Verma and C. Prakash, ‘Internet of things (iot): A vision, architectural elements, and security issues,’ in *2017 international conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)*, IEEE, 2017, pp. 492–496. DOI: 10.1109/I-SMAC.2017.8058399.

[10] G. J. Joyia, R. M. Liaqat, A. Farooq and S. Rehman, ‘Internet of medical things (iomt): Applications, benefits and future challenges in healthcare domain.,’ *J. Commun.*, vol. 12, no. 4, pp. 240–247, 2017. DOI: 10.12720/jcm.12.4.240-247.

[11] E. Saweros and Y.-T. Song, ‘Connecting personal health records together with ehr using tangle,’ in *2019 20th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD)*, IEEE, 2019, pp. 547–554. DOI: 10.1109/SNPD.2019.8935646.

[12] J. Frankenfield, *Distributed ledger technology*, Nov. 2021. [Online]. Available: https://www.investopedia.com/terms/d/distributed-ledger-technology-dlt.asp.

[13] *Dlt basics*, Feb. 2021. [Online]. Available: https://iota-beginners-guide.com/dlt/.

[14] L. Riley, *Universal dlt interoperability is now a practical reality*, Aug. 2021. [Online]. Available: https://www.hyperledger.org/blog/2021/05/10/universal-dlt-interoperability-is-now-a-practical-reality.

[15] *What is blockchain?* Jul. 2020. [Online]. Available: https://www.r3.com/blockchain-101/.

[16] *Today’s cryptocurrency prices by market cap*. [Online]. Available: https://coinmarketcap.com/.

[17] *Iota*, 2020. [Online]. Available: https://crypto.marketswiki.com/index.php?title=IOTA.

[18] N. Shalom, *Three-way handshake*, Nov. 2020. [Online]. Available: https://www.techopedia.com/definition/10339/three-way-handshake.

[19] B. J. Oates, *Researching information systems and computing*. Sage Publications, 2006.

[20] B. Kitchenham, ‘Procedures for performing systematic reviews,’ *Keele, UK, Keele University*, vol. 33, no. 2004, pp. 1–26, 2004.

[21] D. Budgen, M. Turner, P. Brereton and B. Kitchenham, ‘Using mapping studies in software engineering.,’ *Proceedings of the 20th Annual Workshop of the Psychology of Programming Interest Group (PPIG 2008). Psychology of Programming Interest Group*, pp. 195–204,

[22] K. Petersen, R. Feldt, S. Mujtaba and M. Mattsson, ‘Systematic mapping studies in software engineering,’ *Proceedings of the 12th International Conference on Evaluation and Assessment in Software Engineering (EASE 2008)*, pp. 68–77, 2008. DOI: 10.14236/ewic/ease2008.8.

[23] V. Berg, J. Birkeland, A. Nguyen-Duc, I. O. Pappas and L. Jaccheri, 'Software startup engineering: A systematic mapping study,' *Journal of Systems and Software*, vol. 144, pp. 255–274, 2018. DOI: 10.1016/j.jss.2018.06.043.

[24] V. K. Vaishnavi and W. L. Kuechler, 'Design Science Research in Information Systems,' *Ais*, pp. 1–45, 2004, ISSN: 02767783. DOI: 10.1007/978-1-4419-5653-8. [Online]. Available: http://www.desrist.org/design-research-in-information-systems/.

[25] M. Kate, *Usability testing 101*, 2019. [Online]. Available: https://www.nngroup.com/articles/usability-testing-101/.

[26] J. Nielsen, *Why you only need to test with 5 users*, 2000. [Online]. Available: https://www.nngroup.com/articles/why-you-only-need-to-test-with-5-users/.

[27] *Generelle forskningsetiske retningslinjer*, 2019. [Online]. Available: https://www.forskningsetikk.no/retningslinjer/generelle/.

[28] J. Sengupta, S. Ruj and S. D. Bit, 'A comprehensive survey on attacks, security issues and blockchain solutions for iot and iiot,' *Journal of Network and Computer Applications*, vol. 149, p. 102 481, 2020. DOI: 10.1016/j.jnca.2019.102481.

[29] I. Yaqoob, K. Salah, R. Jayaraman and Y. Al-Hammadi, 'Blockchain for healthcare data management: Opportunities, challenges, and future recommendations,' *Neural Computing and Applications*, 2021. DOI: 10.1007/s00521-020-05519-w.

[30] B. Houtan, A. S. Hafid and D. Makrakis, 'A survey on blockchain-based self-sovereign patient identity in healthcare,' *IEEE Access*, vol. 8, pp. 90 478–90 494, 2020. DOI: 10.1109/access.2020.2994090.

[31] B. C. Florea, 'Blockchain and internet of things data provider for smart applications,' in *2018 7th Mediterranean Conference on Embedded Computing (MECO)*, IEEE, 2018, pp. 1–4. DOI: 10.1109/MECO.2018.8406041.

[32] X. Zheng, S. Sun, R. R. Mukkamala, R. Vatrapu, J. Ordieres-Meré *et al.*, 'Accelerating health data sharing: A solution based on the internet of things and distributed ledger technologies,' *Journal of medical Internet research*, vol. 21, no. 6, e13583, 2019. DOI: 10.2196/13583.

[33] W. F. Silvano and R. Marcelino, 'Iota tangle: A cryptocurrency to communicate internet-of-things data,' *Future Generation Computer Systems*, vol. 112, pp. 307–319, 2020. DOI: 10.1016/j.future.2020.05.047.

[34] J. Brogan, I. Baskaran and N. Ramachandran, 'Authenticating health activity data using distributed ledger technologies,' *Computational and structural biotechnology journal*, vol. 16, pp. 257–266, 2018. DOI: 10.1016/j.csbj.2018.06.004.

[35] A. Rovira-Sugranes and A. Razi, 'Optimizing the age of information for blockchain technology with applications to iot sensors,' *IEEE Communications Letters*, vol. 24, no. 1, pp. 183–187, 2020. DOI: 10.1109/lcomm.2019.2949557.

[36] G. Suciu, C. Nadrag, C. Istrate, A. Vulpe, M.-C. Ditu and O. Subea, 'Comparative analysis of distributed ledger technologies,' *2018 Global Wireless Summit (GWS)*, 2018. DOI: 10.1109/gws.2018.8686563.

[37] S. Brotsis, K. Limniotis, G. Bendiab, N. Kolokotronis and S. Shiaeles, 'On the suitability of blockchain platforms for iot applications: Architectures, security, privacy, and performance,' *Computer Networks*, vol. 191, p. 108 005, 2021. DOI: 10.1016/j.comnet.2021.108005.

[38] M. J. M. Chowdhury, M. S. Ferdous, K. Biswas, N. Chowdhury, A. Kayes, M. Alazab and P. Watters, 'A comparative analysis of distributed ledger technology platforms,' *IEEE Access*, vol. 7, pp. 167 930–167 943, 2019. DOI: 10.1109/ACCESS.2019.2953729.

[39] N. El Ioini and C. Pahl, 'A review of distributed ledger technologies,' in *OTM Confederated International Conferences" On the Move to Meaningful Internet Systems"*, Springer, 2018, pp. 277–288. DOI: 10.1007/978-3-030-02671-4_16.

[40] N. Zivic, C. Ruland and J. Sassmannshausen, 'Distributed ledger technologies for m2m communications,' in *2019 International Conference on Information Networking (ICOIN)*, IEEE, 2019, pp. 301–306. DOI: 10.1109/ICOIN.2019.8718115.

[41] H. Pervez, M. Muneeb, M. U. Irfan and I. U. Haq, 'A comparative analysis of dag-based blockchain architectures,' in *2018 12th International Conference on Open Source Systems and Technologies (ICOSST)*, IEEE, 2018, pp. 27–34. DOI: 10.1109/ICOSST.2018.8632193.

[42] J. Preece, H. Sharp and Y. Rogers, *Interaction design: Beyond human-computer interaction*. Wiley, 2002, ISBN: 978-0471492788.

[43] *Iota streams*, 2021. [Online]. Available: https://www.iota.org/solutions/streams.

[44] *Why is rust programming language so popular?* Mar. 2022. [Online]. Available: https://codilime.com/blog/why-is-rust-programming-language-so-popular/.

[45] *Develop android apps with kotlin*, Nov. 2021. [Online]. Available: https://developer.android.com/kotlin.

[46] J. Raynes, *6 best smartwatches for software developers in 2022*, Jan. 2022. [Online]. Available: https://justwearable.com/best-smartwatches-for-developers/.

[47] C. Allison, *Best wear os smartwatch 2022: The top watches using google's operating system*, Mar. 2022. [Online]. Available: https://www.pocket-lint.com/smartwatches/buyers-guides/134135-best-android-smartwatch-top-android-wear-devices-and-google-smartwatches-to-buy.

[48] J. Peckham, *Beste wear os-klokke 2022*, Mar. 2022. [Online]. Available: https://global.techradar.com/no-no/news/beste-wear-os-klokke.

[49] C. Lynch, *Best wear os watch 2022*, Mar. 2022. [Online]. Available: https://www.androidcentral.com/best-wear-os-watch.

[50] S. Pittet, *The different types of testing in software*. [Online]. Available: `https://www.atlassian.com/continuous-delivery/software-testing/types-of-software-testing`.

[51] S. Partners, *5 blockchain healthcare use cases in digital health*. [Online]. Available: `https://stlpartners.com/articles/digital-health/5-blockchain-healthcare-use-cases/`.

[52] Helsedirektoratet, *Koronavirus – besøk – pasienter og beboere*, Mar. 2022. [Online]. Available: `https://www.helsedirektoratet.no/veiledere/koronavirus/besok-pasienter-og-beboere`.

[53] R. Alroobaea and P. J. Mayhew, 'How many participants are really enough for usability studies?' In *2014 Science and Information Conference*, IEEE, 2014, pp. 48–56. DOI: `10.1109/SAI.2014.6918171`.

Appendix A

Gannt Diagram - Semester plan

Master Project - Gannt Diagram
Start: Mon, 10th of Jan
End: Fri, 10th of June

	January			February				March				April				May					June	
Tasks	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Planning phase																						
Develop semesterplan	■																					
Research technologies/libraries/frameworks		■																				
Write and send NSD		■																				
Fill in overleaf template with notes		■	■																			
General architecture modelling		■	■																			
Expert interviews phase																						
Plan expert interviews			■	■																		
Perform expert interviews					■	■																
Transcribe and write summary of interviews						■	■															
Figma prototype phase																						
Development of figma prototype							■	■														
Look into development with IOTA library							■	■	■	■												
Plan user testing								■														
Perform user tests									■	■												
Write summary of results from user tests										■												
Prototype phase																						
Plan prototype										■												
Develop prototype											■	■	■	EASTER								
Plan user testing													■	EASTER	■							
Perform user tests																■						
Write summary of results from user tests																	■					
Writing phase																						
write about sms from last semester																		■	■			
write research method																		■	■			
write background																			■	■		
write discussion																			■	■		
write conclusion and introduction																				■	■	
proof read and final adjustments																					■	■

Appendix B

NSD application

NSD NORSK SENTER FOR FORSKNINGSDATA

Meldeskjema

Referansenummer

496628

Hvilke personopplysninger skal du behandle?

- Navn (også ved signatur/samtykke)
- E-postadresse, IP-adresse eller annen nettidentifikator
- Bilder eller videoopptak av personer
- Lydopptak av personer
- Bakgrunnsopplysninger som vil kunne identifisere en person
- Helseopplysninger

Beskriv hvilke bakgrunnsopplysninger du skal behandle

Navn, epost, alder, utdanning og arbeidserfaring.

Prosjektinformasjon

Prosjekttittel

E-Helse og IOTA Tangle

Prosjektbeskrivelse

Masteroppgave innen teknologiutvikling som skal gjennomføre ekspertintervjuer og brukertesting av utviklet applikasjon.

Begrunn behovet for å behandle personopplysningene

Epost og navn benyttes kun i rekrutteringsprosessen.

For utvalg 1: for at vi skal kunne definere intervjuobjektet som ekspert innen sitt felt er det relevant å behandle personopplysninger som utdanning og arbeidserfaring. Dette anser vi som nødvendig for å gi resultat fra intervjuet nødvendig tyngde.

For utvalg 2: for brukertesting vil alder, og arbeidserfaring/utdanning være relevant for forskningen å kunne presentere ulike gruppers oppfatning av prototypen som skal utvikles.

Ekstern finansiering

Type prosjekt

Studentprosjekt, masterstudium

Kontaktinformasjon, student

Eivind Solberg Rydningen, eivind.rydningen@gmail.com, tlf: 48092973

Behandlingsansvar

Behandlingsansvarlig institusjon

Norges teknisk-naturvitenskapelige universitet / Fakultet for informasjonsteknologi og elektroteknikk (IE) / Institutt for datateknologi og informatikk

Prosjektansvarlig (vitenskapelig ansatt/veileder eller stipendiat)

Letizia Jaccheri, letizia.jaccheri@ntnu.no, tlf: 91897028

Skal behandlingsansvaret deles med andre institusjoner (felles behandlingsansvarlige)?

Nei

Utvalg 1

Beskriv utvalget

Eksperter innen E-Helse, IOTA og Distributed Ledger Teknologi

Rekruttering eller trekking av utvalget

Rekruttert via e-post i eget nettverk.

Alder

30 - 70

Inngår det voksne (18 år +) i utvalget som ikke kan samtykke selv?

Nei

Personopplysninger for utvalg 1

- Navn (også ved signatur/samtykke)
- E-postadresse, IP-adresse eller annen nettidentifikator
- Bilder eller videoopptak av personer
- Lydopptak av personer
- Bakgrunnsopplysninger som vil kunne identifisere en person

Hvordan samler du inn data fra utvalg 1?

Personlig intervju

Grunnlag for å behandle alminnelige kategorier av personopplysninger

Samtykke (art. 6 nr. 1 bokstav a)

Informasjon for utvalg 1

Informerer du utvalget om behandlingen av opplysningene?

Ja

Hvordan?

Skriftlig informasjon (papir eller elektronisk)

Utvalg 2

Beskriv utvalget

Et representativt utvalg mennesker over 18 år.

Rekruttering eller trekking av utvalget

Rekruttert via e-post i eget nettverk.

Alder

18 - 90

Inngår det voksne (18 år +) i utvalget som ikke kan samtykke selv?

Nei

Personopplysninger for utvalg 2

- Navn (også ved signatur/samtykke)
- E-postadresse, IP-adresse eller annen nettidentifikator
- Lydopptak av personer
- Bakgrunnsopplysninger som vil kunne identifisere en person
- Helseopplysninger

Hvordan samler du inn data fra utvalg 2?

Deltakende observasjon

Grunnlag for å behandle alminnelige kategorier av personopplysninger

Samtykke (art. 6 nr. 1 bokstav a)

Grunnlag for å behandle særlige kategorier av personopplysninger

Uttrykkelig samtykke (art. 9 nr. 2 bokstav a)

Redegjør for valget av behandlingsgrunnlag

Informasjon for utvalg 2

Informerer du utvalget om behandlingen av opplysningene?

Ja

Hvordan?

Skriftlig informasjon (papir eller elektronisk)

Tredjepersoner

Skal du behandle personopplysninger om tredjepersoner?

Nei

Dokumentasjon

Hvordan dokumenteres samtykkene?

- Elektronisk (e-post, e-skjema, digital signatur)

Hvordan kan samtykket trekkes tilbake?

De kan kontakte personvernombud, veileder eller masterstudentene for å trekke tilbake samtykke.

Hvordan kan de registrerte få innsyn, rettet eller slettet opplysninger om seg selv?

De kan kontakte personvernombud, veileder eller masterstudentene for å få innsyn, rettet eller slettet opplysninger om seg selv.

Totalt antall registrerte i prosjektet

1-99

Tillatelser

Skal du innhente følgende godkjenninger eller tillatelser for prosjektet?

Behandling

Hvor behandles opplysningene?

- Ekstern tjeneste eller nettverk (databehandler)

Hvem behandler/har tilgang til opplysningene?

- Student (studentprosjekt)
- Prosjektansvarlig
- Databehandler

Hvilken databehandler har tilgang til opplysningene?

Microsoft Teams

Tilgjengeliggjøres opplysningene utenfor EU/EØS til en tredjestat eller internasjonal organisasjon?

Nei

Sikkerhet

Oppbevares personopplysningene atskilt fra øvrige data (koblingsnøkkel)?

Nei

Begrunn hvorfor personopplysningene oppbevares sammen med de øvrige opplysningene

Vi anser det som forsvarlig å oppbevare personopplysningene sammen ettersom dataen ligger i en adgangsbegrenset mappe i Microsoft Teams.

Hvilke tekniske og fysiske tiltak sikrer personopplysningene?

- Adgangsbegrensning

Varighet

Prosjektperiode

10.01.2022 - 10.12.2022

Skal data med personopplysninger oppbevares utover prosjektperioden?

Nei, alle data slettes innen prosjektslutt

Hvor oppbevares opplysningene?

Eksternt arkiv/datasenter
I en privat mappe i Microsoft Teams.

Vil de registrerte kunne identifiseres (direkte eller indirekte) i oppgave/avhandling/øvrige publikasjoner fra prosjektet?

Nei

Tilleggsopplysninger

Har foretatt endringer etter innsending. Siste endring gjort 09. februar 10:51.

Pulsmålingene som tas av smartklokken og sendes til appen vil ikke på noen måte være koblet til personopplysningene som brukeren som tester prototypen har oppgitt. Målingene lagres heller ikke av prototypen etter gjennomført test.

Appendix C

Consent Forms

Vil du delta i forskningsprosjektet

”E-helse og IOTA Tangle”?

Dette er et spørsmål til deg om å delta i et forskningsprosjekt hvor formålet er å undersøke fordelene og mulighetene ved bruk av IOTA Tangle teknologien for helsedatahåndtering. I dette skrivet gir vi deg informasjon om målene for prosjektet og hva deltakelse vil innebære for deg.

Formål

Dette prosjektet er en masteroppgave. Formålet er å utvikle en prototype som kan demonstrere hvordan helsedatahåndtering kan være pålitelig og sikker ved bruk av IOTA Tangle-teknologien. Det er mangel på forskning som involvere brukere i utvikling og testing av prototyper innenfor dette forskningsområdet. Dette åpner opp spennende muligheter for videre undersøkelser.
Følgende forskningsspørsmål er derfor etablert:
RQ 1: Hvordan kan IOTA Tangle gi pålitelig og sikker helsedatahåndtering?
RQ 2: Hvordan bør en helsedatahåndteringsapplikasjon, bygget med IOTA, utformes for å forbedre folks livskvalitet?

Hvem er ansvarlig for forskningsprosjektet?

NTNU (Norges teknisk-naturvitenskapelige universitet) er ansvarlig institusjon for prosjektet. Professor Letizia Jaccheri er veileder for denne masteroppgaven, og masterstudentene er Eivind Solberg Rydningen og Erika Åsberg.

Hvorfor får du spørsmål om å delta?

Vi skal gjennomføre brukertest av vår forskningsprototype på et representativt utvalg mennesker over 18 år. Vi ønsker et bredt spekter i henhold til alder og teknisk erfaring.

Hva innebærer det for deg å delta?

Hvis du velger å delta i prosjektet, vil du delta i et brukertest der du vil få presentert flere oppgaver som skal gjennomføres på en prototype. Prototypen består av en smartklokke som måler puls som sendes til enn app. Pulsmålingene vil ikke kunne kobles til personopplysninger om deg. Brukertesten vil ta ca. 45 minutter. Svarene dine vil bli tatt opp som lyd og senere transkribert til tekst.

Det er frivillig å delta

Det er frivillig å delta i prosjektet. Hvis du velger å delta, kan du når som helst trekke samtykket tilbake uten å oppgi noen grunn. Alle dine personopplysninger vil da bli slettet. Det vil ikke ha noen negative konsekvenser for deg hvis du ikke vil delta eller senere velger å trekke deg.

Ditt personvern – hvordan vi oppbevarer og bruker dine opplysninger

Vi vil bare bruke opplysningene om deg til formålene vi har fortalt om i dette skrivet. Vi behandler opplysningene konfidensielt og i samsvar med personvernregelverket.

- I tilknytning til NTNU vil forfatterne og deres veileder få tilgang til personopplysningene.
- Dataene vil bli lagret i en privat mappe, kun tilgjengelig for partene nevnt ovenfor, i Microsoft Teams underveis i prosjektet.
- Lydopptaket vil bli transkribert med Microsoft Office Word.

Som deltaker vil du ikke kunne gjenkjennes i publikasjon av denne masteroppgaven. Kun et sammendrag av alle deltakernes utsagn fra brukertesten vil bli publisert.

Hva skjer med opplysningene dine når vi avslutter forskningsprosjektet?
Opplysningene anonymiseres når prosjektet avsluttes/oppgaven er godkjent, noe som etter planen er 10. desember 2022. All informasjon hentet fra intervjuet vil deretter bli slettet, inkludert lydopptak.

Hva gir oss rett til å behandle personopplysninger om deg?
Vi behandler opplysninger om deg basert på din samtykke. På oppdrag fra NTNU har Personverntjenester vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket.

Dine rettigheter
Så lenge du kan identifiseres i datamaterialet, har du rett til:

- innsyn i hvilke opplysninger vi behandler om deg, og å få utlevert en kopi av opplysningene
- å få rettet opplysninger om deg som er feil eller misvisende
- å få slettet personopplysninger om deg
- å sende klage til Datatilsynet om behandlingen av dine personopplysninger

Hvis du har spørsmål til studien, eller ønsker å vite mer om eller benytte deg av dine rettigheter, ta kontakt med:

- Personverntjenester på e-post (personverntjenester@sikt.no) eller på telefon: 53211500
- Veileder Letizia Jaccheri ved NTNU på e-post (letizia.jaccheri@ntnu.no) eller på telefon: 91897028
- Masterstudent Eivind Rydningen ved NTNU på epost (eivind.rydningen@gmail.com)
- Vårt personvernombud Thomas Helgesen ved NTNU på epost (thomas.helgesen@ntnu.no) eller på telefon: 93079038

Med vennlig hilsen

Erika Åsberg (Masterstudent)
Eivind Rydningen (Masterstudent)

Erika Åsberg Eivind Rydningen

Samtykkeerklæring

Jeg har mottatt og forstått informasjon om prosjektet *E-helse og IOTA Tangle*, og har fått anledning til å stille spørsmål. Jeg samtykker til:

- å delta i brukertesten

Jeg samtykker til at mine opplysninger behandles frem til prosjektet er avsluttet

----
(Signert av prosjektdeltaker, dato)

Are you interested in taking part in the research project *”Health data management and the IOTA Tangle”*?

This is an inquiry about participation in a research project where the main purpose is to research the advantages and opportunities of using the IOTA Tangle for health data management. In this letter we will give you information about the purpose of the project and what your participation will involve.

Purpose of the project

This project is a Master’s Thesis. The purpose of this project is to develop a prototype that can demonstrate how health data management can be reliable and secure with the use of the IOTA Tangle technology. There exists a gap in the literature in terms of involving users in the development and testing of prototypes. This observation makes the involvement of users, an interesting avenue for further investigation.

Thus, the following research questions have been established:
RQ 1: How can the IOTA Tangle provide reliable and secure health data management?
RQ 2: How should a health data management application, built with IOTA, be designed to improve people’s quality of life?

Who is responsible for the research project?
NTNU (Norwegian University of Science and Technology) is the institution responsible for the project. Professor Letizia Jaccheri is the supervisor for this Master’s Thesis, and the student authors are Eivind Solberg Rydningen and Erika Åsberg.

Why are you being asked to participate?
The research intends to interview several experts within the field of health data management and distributed ledger technology, such as blockchain or the IOTA Tangle, in order to gain insight and knowledge regarding the topic of the research.

What does participation involve for you?
If you choose to take part in the project, you will be participating in a personal interview online. It will take approx. 45 minutes. The interview includes questions regarding your education and work experience, and your experience and knowledge related to the topics of e-health and distributed ledger technology, such as blockchain or the IOTA Tangle. The interview will be recorded by video. The sound will be extracted from the recording and later transcribed to text. The video will be deleted after the sound is extracted.

Participation is voluntary
Participation in the project is voluntary. If you chose to participate, you can withdraw your consent at any time without giving a reason. All information about you will then be made anonymous. There will be no negative consequences for you if you choose not to participate or later decide to withdraw.

Your personal privacy – how we will store and use your personal data
We will only use your personal data for the purpose(s) specified in this information letter. We will process your personal data confidentially and in accordance with data protection legislation (the General Data Protection Regulation and Personal Data Act).

- In connection with NTNU, the authors and their supervisor will have access to the personal data.
- The data will be stored in a private folder, only accessible to the parties mentioned above, in Microsoft Teams during the project.
- The sound recording will be transcribed using Microsoft Office Word.

The participants will not be identifiable in our final publication. The personal data will be anonymized, unless you as a participant explicitly state that you agree to be identifiable by name in our final publication.

What will happen to your personal data at the end of the research project?
The project is scheduled to end on the 10th of December 2022. The transcribed and anonymized interview will be a part of the final publication, while the digital recordings and other related files will be deleted at the end of the project.

Your rights
So long as you can be identified in the collected data, you have the right to:

- access the personal data that is being processed about you
- request that your personal data is deleted
- request that incorrect personal data about you is corrected/rectified
- receive a copy of your personal data (data portability), and
- send a complaint to the Data Protection Officer or The Norwegian Data Protection Authority regarding the processing of your personal data

What gives us the right to process your personal data?
We will process your personal data based on your consent.

Based on an agreement with the Department of Computer Science at NTNU, Data Protection Services has assessed that the processing of personal data in this project is in accordance with data protection legislation.

Where can I find out more?

If you have questions about the project or want to exercise your rights, contact:

- Department of Computer Science via Professor Letizia Jaccheri, by email: (letizia.jaccheri@ntnu.no).
- Data protection officer: Thomas Helgesen (thomas.helgesen@ntnu.no) or by telephone: +47 93079038.
- Department of Computer Science via Master Student Eivind Rydningen, by email: (eivind.rydningen@gmail.com).
- Data Protection Services, by email: (personverntjenester@sikt.no) or by telephone: +47 53 21 15 00.

Yours sincerely,

Erika Åsberg (Master Student)
Eivind Rydningen (Master Student)

Erika Åsberg   Eivind Rydningen

Consent form

I have received and understood information about the project *Health data management and the IOTA Tangle* and have been given the opportunity to ask questions.

Kindly select the boxes that you consent with:

□ to participate in a personal interview

Choose one:

□ for information about me/myself to be published in a way that is anonymized

□ for information about me/myself to be published in a way that I can be identified

I give consent for my personal data to be processed until the end date of the project, approx. 10th of December 2022.

---

(Signed by participant, date)

Appendix D

Figma Prototype

Click this link to see the Figma prototype.

Eivind Solberg Rydningen, Erika Åsberg

Exploring the IOTA Tangle for Health Data Management

NTNU
Norwegian University of
Science and Technology