Improving the usability of secure information storing within blockchain applications

Natali Ljunggren

DIVISION OF ERGONOMICS AND AEROSOL TECHNOLOGY | DEPARTMENT OF DESIGN SCIENCES | FACULTY OF ENGINEERING LTH | LUND UNIVERSITY | 2019

MASTER THESIS

Improving the usability of secure information storing within blockchain applications

Natali Ljunggren

LUND
UNIVERSITY

Improving the usability of secure information storing within blockchain applications

Published by
Department of Design Sciences
Faculty of Engineering LTH, Lund University
P.O. Box 118, SE-221 00 Lund, Sweden

Subject: Interaction Design (MAMM01), Division: Division of Ergonomics and Aerosol Technology, Department of Design Sciences, Faculty of Engineering, LTH, Lund University

Supervisor: Åsa Ek
Co-supervisor: Johanna Persson
Examiner: Christofer Rydenfalt

Abstract

Today's blockchain applications have been inherently created by and for users who understand the blockchain technology. To improve mass adoption of blockchain solutions, the user experience must improve, and the attention must move to users not familiar with the underlying technology. This dissertation starts with reviewing the main concepts of blockchain technology and examining the UX of different Ethereum wallets with the aim to deliver a more user-friendly wallet based on user feedback. It then delivers a wallet design that enables even the most non-technical users to securely and safely use a cryptocurrency wallet with a decreased risk of content loss. The developed solution is then compared to the existing main stream token wallets.

Keywords: Usability, User Experience, Blockchain Technology, Wallet Security, Decentralized Information Storing

For my mother who gave me wings and,
My brother who teaches me to fly

Acknowledgments

First, I would like to thank my supervisors, Åsa Ek and Johanna Persson, for their expert advice and guidance. They both steered me in the right direction whenever I needed it.

Secondly and more importantly, I would like to acknowledge Peter Kristoffersson as the second reader of this thesis. I am grateful for his valuable insights and input and indebted to him for his mentorship.

Lund, February 2019

Natali Ljunggren

Table of contents

1 Introduction

User Experience and lack of knowledge are a serious barrier to mass adoption and use of blockchain technologies. Countless novice and experienced blockchain users fall victim to both basic negligence and sophisticated exploits due to these barriers. To enable an easier and a more secure use of the technologies for the end user, the usability needs to improve from a non-technical user perspective. This project aims to help with this.

1.1 Why User Experience is vital for further blockchain adaptation

A fundamental concept within blockchain technologies is secure information storage. The information itself is stored within the blockchain but the access to this information and the ability to interact with it is held and controlled by the information's owner who holds the digital access means to it.

This digital access information is usually stored in a so-called wallet that can be implemented as a mobile application, web browser plug-in, a computer software etc. The owner of the information is the person who has access to that wallet. In other words, access equals to holding a sequence of numbers and letters (the access information) and, the person who owns this sequence has access to the wallet and all the information it contains.

People who have lost their sequences have lost everything their wallets have contained [1], [2]. This problem exists not only because the user is expected to know the severity of not writing down the sequence and storing it in a secure place, but also because these type of wallet applications often do not provide the user with any back-up solutions of storing their sequence. Wallet applications have been and still are created by and for people who understand the technology and its requirements. Unfortunately, this means that the blockchain applications are beyond the skills of most non-technical people. Just as with the old computer operating systems or even internet itself, the technology needs to become easier, more self-explanatory. Any wider technology adaptation will therefore require focus change from technical end-users to non-technical users.

1.2 Project goals

The aim of this thesis is to design an easy to use, from a usability perspective, mobile blockchain application prototype that is compatible with an optional hardware component.

- The project is expected to deliver a clickable prototype of the mobile application and a written concept that includes specifications of the hardware component
- The suggested system should protect users from common security and usability problems that are present in today's existing solutions.

1.3 Project limitations

Due to the imposed project limitations, this project will focus on delivering a solution for Ethereum, one of the most widely used token platforms today. However, the insight from it will be applicable to the whole blockchain environment and all tokens. Unfortunately, there is a severe lack of scientific papers about usability in the blockchain environment. This project will therefore have to rely on other sources such as the opinions of recognized designers and well-known design principles but mainly the voice of current and potential users. Also, since no access has been provided to existing hardware wallets, the finished prototype will not include a hardware component. However, a conceptual description of how the component is to collaborate with the prototype will be provided based on research concerning the existing ones.

1.4 Project client

This project and the designs here presented are developed for Cisco Systems as a part of their research into blockchain applications.

1.5 The remain of this dissertation

The rest of this document is structured as follows. Chapter 2: Background, presents the fundamental technical concepts of blockchain technology and its applications and, describes and defines different concepts and principles of the design process. Chapter 3: Project approach, discusses the chosen methodologies for this project. Chapter 4. Data gathering, presents the outcomes of phase one, Chapter 5: Data

analysis, presents the outcomes of phase two and Chapter 6: Prototyping & evaluation, presents the outcomes of phase three. Chapter 7: Discussion, discusses the project methodology, the obtained results from the different phases and presents ideas for future research. Finally, Chapter 8: Conclusions: concludes the project.

2 Background

This section describes essential concepts that are required for a full understanding of the project.

2.1 Blockchain technology

Blockchain technology, despite currently being the latest fad, is not really a new technology in itself. What is new and novel about blockchain is the combination of the underlying technologies into a new data storing and validation paradigm, allowing for seemingly immutable and distributed information. The concept of blockchain, as it is known today, was developed by the creator of bitcoin, Satoshi Nakamoto (who, till this day, remains anonymous), and is the underlying concept for most cryptocurrencies and tokens today.

At its core, blockchain is the combination of three already known and proven technologies; private key cryptography, P2P network and a protocol governing incentivization. The result of this combination is a decentralized system for digital interactions (transactions) based on multiple, independent yet trusted third parties (nodes) keeping a copy of the transactional ledger and independently verifying the validity of the transactions processed through the network. [3].

The transactions or records themselves are stored in a chronologically interconnected chain of data blocks where each block contains a chronologically added set of transactions. Once a new block is created, its contents together with the cryptographic hash of the previous block, and in most cases, a timestamp, are used to create a new cryptographic hash for the block. This makes the hash of each block unique and directly dependent on the hash of the previous block in the chain. Any data tampering within the blocks will result in the chain breaking and the tampering becoming visible to all nodes as the hash chain no longer conforms to the lists held by other nodes. This is done by each node independently verifying all hashes and transaction validity - a valid chain is a chain where more than 50% of nodes come to the same hash of the last block. In other words, no single entity controls the chain. [4], [5]. There are variations to this process, i.e. ripple where the exact mechanism is based on consensus rather than majority, however, for most blockchain applications the following describes the high-level implementation:

1. A transaction can involve cryptocurrencies, records, contracts or any other information. When a transaction is being requested (by a user, e.g. transferring assets from one account to another) it is broadcasted on a P2P network that consist of people running purpose-built computers, commonly called “miners”.
2. For each transaction, previous transactions are checked to make sure that the transaction is eligible to be executed according to the blockchain history.
3. Eligible transactions are then added to the block together with the previous blocks hash
4. Once the block is full, it is closed, and the so-called Proof of Work consensus algorithm takes place (hash creation for the block).
5. The miner who finishes the algorithm first sends the hash of the block to every other node and miner and once more than 50% of all miners and nodes validate the hash, they all add the block to their chain.
6. The winning miner is rewarded with the transaction fee per each transaction that was in the block. [6].

Some current implementations of blockchain (i.e. Ethereum) enable decentralized applications (dApps) and systems for digital interactions to be run on the network. This means that for these implementations the blockchain network is more than just a ledger, it is a computing network with full traceability of all processing taking place. [7]. As this thesis predominantly deals with Ethereum - one of the main blockchain implementations allowing for data storage, crypto currencies, tokens and decentralized apps and systems, the following focuses on Ethereum and its functionality.

2.1.1 Ethereum: Concept of storing information

Storing information is a fundamental concept in blockchain technology that is made possible through tokens in Ethereum.

2.1.1.1 What is a token?

A token is a collectible and tradeable digitized proof of ownership which can represent virtually anything e.g. a representation of an asset such as a currency, a virtual share, a proof of ownership etc. [8]. [9].

2.1.1.2 What is a token account?

To store a token, a token specific account is needed. Each account corresponds to its own private and public key pair. Both the private and public key are sequences of a combination of letters and numbers. The public key acts as the public address to where tokens can be sent to. In other words, if someone wants to send tokens to a specific account, one would need the account's public address which is the public key. Exposing the public key does not jeopardize security. The private key is used

to access an account and to perform transactions. Without the private key of one's account, the account cannot be used. Losing a private key equals to losing access to an account and the tokens stored in it. A private key must therefore never be exposed publicly or lost, as losing it equals to losing the account. [9], [10], [11].

2.1.1.3 What is a token wallet?

A wallet consists of one token account or a collection of token accounts. The wallet software uses a cryptographic function to generate a root seed. A root seed is a sequence combination of numbers and letters. If one creates different token accounts within the same wallet, the wallet software can generate all the private and public keys by only using the seed. This means, instead of remembering the private key to every single account within that wallet, one only needs to remember the seed. The seed should be treated as a private key and never be exposed publicly. [9], [12]. Examples of different wallet applications can be found in Appendix C.

2.1.1.3.1 Hot storage

There are so called hot and cold wallets. A hot wallet stores the seed inside of the wallet software e.g. in an app, computer software, browser. Instead of remembering the seed the user can remember a PIN code or use a different form of identification method to access the wallet and its accounts. However, a user might be prompted to insert the seed when e.g. a device is changed, software is updated/re-installed, which means, the user still must store the seed somewhere else or else, access might be lost. [13].

2.1.1.3.2 Cold storage

A cold wallet is a wallet that does not expose the seed to the internet. This type of wallet is considered being the safest option. A cold wallet can be a software that needs a hardware component. E.g. the seed could be stored on a USB similar looking hardware component which can be connected to either a computer, tablet or Smart-Phone. Once connected, it can communicate the seed it holds to a compatible software. Usually the user must enter a PIN code on the component for the seed to be revealed. This type of hardware eliminates the necessity of storing the seed somewhere else. However, it is still recommended that the user has a backup plan in case the component is lost or damaged or simply if the PIN code is forgotten. [13].

2.1.1.4 Securing wallets and transactional invoking

The simplest protection against unwanted transactional invoking is to use a security PIN-code (for both hot and cold wallets). To add an extra layer of security a two-factor identification can be used (Coinbase Wallet, Kraken). An even more secure way of ensuring security is through multi-signature and Shamir’s Secrete Sharing.

2.1.1.4.1 Multi-Signature storing methods

Transactions that require multiple signatures (private keys), a so-called multi-signature, or more commonly, multi-sig, provide a better security in terms of allowing the user to lose M-N signatures or have M-N of the signatures exposed, where N is the required number of signatures and M is the total number of signatures that are valid. If a two (N) out of three (M) scheme is used, the user can lose one key without losing access to his assets. In the case of three (N) out of five (M), the user can lose two keys without losing access to his assets. Same goes for exposure. The user can in the case of two out of three expose one private key and in the case three out of five expose two private keys to a hacker without the hacker being able to steal the assets.

A multi-signature can be used in different ways. All signatures (private keys) can belong to one single person who simply wishes a better security or, signatures can be divided between different people who jointly decide (or the majority) what happens to the assets. [14], [15].

2.1.1.4.2 Shamir's Secret Sharing

Shamir's secret sharing is a cryptographic algorithm that divides a secret, e.g. seed, private key, into smaller unique parts. Each part can later be shared between different people/devices. For reconstruction of the original secret, only a predefined number of the shared parts are required. Most commonly, the required number of parts is less than the total number of parts that can be shared. Hence, all parts are not needed to reconstruct the secret. A common number is to share five parts and require three for reconstruction, i.e., two parts can be lost without leading to a complete loss of the secret. [16]. Shamir's secret sharing can be used to back up a seed and a private key. However, it requires that those who hold the part can be trusted. [17]. As with multisig, Shamir's secret sharing algorithm can be used to authenticate transactions in which case it works as a simple multi-sign implementation amongst a number of people.

2.2 The design theory

The design process is the approach to break down a design project into smaller more manageable chunks. These chunks are; phases, methodologies and different principles that are appropriate for the project field. The general phases for every type of project include: the data gathering phase - the defining of the problem and the collection of additional data, the data interpretation phase - the analysis of gathered data and development of ideas and, the prototyping and evaluation phase - the testing of ideas and the improvement of them. [18].

2.2.1 **Usability**

The aim of this project is to improve usability of storing information in the field of blockchain technology. To fully understand the meaning of this sentence, the reader is presented with the definition of the term usability. The ISO definition of the quality attribute usability is defined as:

> *The extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency, and satisfaction in a specified context of use [19].*

According to the Nielsen Norman Group, usability is a collection name that consist of five quality components [20], namely the following:

2.2.1.1 Learnability

Learnability assessess how easy it is for the user to learn how to use the system.

2.2.1.2 Memorablility

Memorability assesses how easy the user can re-achieve proficiency when not having used the system for a period of time.

2.2.1.3 Efficiency

Efficiency assesses how quickly the user can perform tasks.

2.2.1.4 Errors

The amount of errors the user can make, how severe these are and how easily it is to recover from them.

2.2.1.5 Satisfaction

Satisfaction assesses how pleasant the use of the system is to the user and the overall attitude the user has towards the system.

There are several definitions of usability such as the commonly used by Preece [21]. The one used in this project is, according to the author, the most appropriate as it is the easiest one to assess in terms of quality attributes. Also, the chosen definition is the most aligned one with the Human centred design approach, described in section 2.2.3.

2.2.2 **User experience**

User experience (UX) is defined as a user's perceptions and responses as a concequence to the use of a system – it emcompasses a lot more than usability. When interpretating usability from the perspecitve of the user's personal goals, usability testing can be performed in order to assess the UX. [19].

2.2.3 **Human-centred design for interactive systems**

The Human-centred design for interactive systems, defined by the ISO-standard 9241-210 (2010), is an iterative design approach that considers the needs and requirements of users, human factors/ergonomics, usability knowledge and techniques, and leads to user satisfaction, accessibility and sustainability and in this case also security. The design process involves and is driven by both stakeholders and end-users. It addresses the whole UX.

The approach is defined by four main activities where each activity is based upon the understanding of users, stakeholders, tasks and environments:

1. Understand and specify context of use
2. Specify the user requirements
3. Produce design solutions to meet these requirements
4. Evaluate the designs against requirements.

As a side note, the term user-centred design is sometimes used instead of the term human-centred design. However, the word "human" is preferred since it addresses all stakeholders and not only end-users. [19].

2.2.4 **Data gathering**

2.2.4.1 Interviews

Interviewing is a common technique to gain insights into the opinions, thoughts and ideas of users [22]. To produce both qualitative and quantitative answers, an interview requires both open questions and closed questions. Closed questions are answered with either a "yes" or a "no", or "I don't know" while open questions lead to deeper discussions. A quantitative interview also requires, apart from containing closed questions, to be conducted enough times to be able to draw conclusions about the target users. [23]. Interviews can, if not conducted properly, produce false answers due to research bias and respondent bias, described in section 2.2.8, n and should be thoughtfully prepared to avoid these.

A stakeholder interview is often one of the first activities in the research phase of a design process. A client, the stakeholder in this project, is often considered to be an expert in the project field. The client often possesses information that saves the researcher a lot of time. Apart from finding out project goals and product functionality requirements, the client-interview is a way of quickly familiarizing oneself with the topic. [24]

A semi-structured interview has a flexible and fluid structure, meaning; it is organized around topics, themes and/or areas. It is used when the aim is to obtain qualitative answers rather than quantitative and to let unexpected themes emerge. [25].

2.2.4.2 Competitor analysis

A competitor analysis that focuses on the design aspects of competitor solutions provides information regarding how usability problems can be solved, strengths and weaknesses of the competition and provides evidence that can be used as motivation for changes/suggestions [26].

2.2.5 **Data interpretation**

2.2.5.1 User personas

User personas are descriptions of target users. The descriptions are fictional, yet realistic, and based on user research. User personas are created to examined and understand the characteristics, needs and goals of users. When used in the design process, they often contribute to new insights into the user journey and uncover new problems and solutions that haven't been considered previously. [27].

2.2.5.2 Conceptual design

A conceptual design articulates the form and function of something, in the case of this project, the application. The document includes user interactions, user experiences, user processes and is based on all the underlying strategies and conclusions that the determine these. Articulating concepts and ideas is an important step in the design phase as it can later be used to facilitate other phases such as, by serving as input to the creation of a requirements specification. [28].

2.2.5.3 Requirements specification

In general, a requirements specification articulates what a system is supposed to do. The purpose of a requirement specification is to facilitate and optimize upcoming design phases. It serves as input to the prototyping phase but also as a verification tool that is used to verify that the final proposed design considers all predefined requirements. Requirements are most commonly split into two categories: functional and qualitative (a.k.a. non-functional). Functional requirements describe features of the system, how the system records, computes, transforms and transfers data. Quality requirements describe how well the intended functions of the system operate. [29].

2.2.5.4 Card sorting

Before any prototyping takes place, it is a good idea to have an information structure in mind. Not only does this facilitate and make the prototyping phase more efficient, it also ensures a better overall user experience as the structure is based on user needs. [30].

An information structure, or if more complex, an information architecture, is the organization of features and information that will be made visible to the user through the interface of the application, in this case, the functional requirements. A simple

method of organizing requirements is the so-called card sorting method. In card sorting, each requirement can be seen as a card and all different cards are to be organized into groups. Once all groups are created, they are labelled to something that describes the content accordingly. Card sorting is commonly conducted by the user target group.

2.2.6 **Prototyping and evaluation**

2.2.6.1 Prototyping

A high-fidelity prototype is the closest representation of a product in terms of the interface design and its functionalities. Apart from covering the visuals, aesthetics, and the features, the high-fidelity prototype also covers user interaction, user flow and user behaviour, i.e. the user experience. Hence, evaluating a high-fidelity prototype is a way of assessing the overall user experience. [31].

2.2.6.2 Usability testing

The purpose of conducting usability testing is to identify possible problems with the design and to investigate whether the proposed design fulfils usability requirements. The findings from a usability test can later be used as a basis for improvement recommendation. The early elimination and replacement of design choices that, based on usability testing results, worsen the overall user experience early, lowers the cost of support once the product has been implemented and released. Additionally, and most importantly, it also favours customer satisfaction and invigorates the company trademark.

According to the Nielsen Norman Group, elaborate usability testing is a waste of time. The optimal way of testing is to include a maximum of five participants and to run as many small tests as possible. [32].

A common problem in usability testing is the so called “carryover effect”. In simple terms it describes the situation when performing of a specific task results in altered behaviour when performing a subsequent task (which otherwise would have been completed differently). Depending on how comprehensive a usability test is, e.g. how many parts of the system are being tested in a single test, it can be a good idea to let different users test different parts of a system, the so called “Independent Groups Design” approach. This approach requires a higher number of test participants, but limits the risk of the “carryover effect”. Another strategy to tackle the “carryover effect” is the Counterbalancing approach. With Counterbalancing, the participants test all the parts of a system however, the order of the tasks differs from participant to participant. This approach does not require as many participants as the previous, however, it requires a lot of planning.

2.2.7 **Fundamental design principles**

Donald Norman introduced seven design principles that are fundamental when designing interfaces if the aim is to achieve a usable and simple to learn product. These will be used as guidelines in the prototyping phase and are:

2.2.7.1 Visibility

The things you can interact with such as buttons, tabs should be made visible. The more visible they are the more likely they will be discovered and used.

2.2.7.2 Feedback

When an action has been taken e.g. pressing a button, changing tab, the interface should provide the user with some form of feedback. There are various forms of feedback e.g. visual, audio, tactile, etc. The user should never be confused regarding what action was taken and the consequence of that action.

2.2.7.3 Constraints

The concept of constraints is to limit interaction possibilities. This approach clarifies to the user what can be done. Too many interaction possibilities might leave the user confused.

2.2.7.4 Mapping

Mapping is about making the relationship between controls (e.g. buttons) and the consequence of pressing them clear to the user. Hence, making the system more understandable to the user.

2.2.7.5 Consistency

Similar tasks should be achieved by similar operations and represented by similar elements. This leads to a greater memorability of how the system works, hence facilitating learnability.

2.2.7.6 Affordance

Affordance is about giving clues on how the user can use the system. The user should what kind of interactions are possible when looking at the interface. [33]

2.2.8 **Research bias**

In research, bias is defined as any prejudice preventing deeper investigation or being prevented from finding out the truth or facts. [34].

To avoid bias in the research phase, different bias prevention methods will be used. The potentially relevant biases for this project and their different possible prevention methods are the following:

2.2.8.1 Respondent bias

Respondent bias is the tendency of a respondent not always answering questions truthfully. Respondent bias can be further divided into four sub-biases; Acquiescence bias, social desirability bias, habituation bias, sponsor bias. [35].

2.2.8.1.1 Acquiescence bias

Acquiescence bias is a tendency of agreeing with whatever the researcher suggests. One factor that causes acquiescence bias is the perception of seeing the researcher as an expert. It is easier to agree and feels sensible to agree with an expert rather than disagree. Acquiescence can escalate with fatigue caused by repetitive questions. To avoid this, it is suggested to remove questions that facilitate acquiescence, i.e., avoid questions with an agree/disagree choice and leading questions as it takes less effort to agree with a statement rather than to disagree. [36], [37].

2.2.8.1.2 Social desirability bias

Social desirability bias is a sometimes-observed behaviour caused by the psychological need of being perceived as better than one is in the in the eyes of others, a phenomenon that it amplified by the feeling of being observed. [38], [39].

2.2.8.1.3 Habituation bias

Habituation bias is a biological response to provide similar answers to questions that are worded in similar ways, often amplified by fatigue caused by repetitive questions. [40], [41].

2.2.8.1.4 Sponsor bias

Sponsor bias is the tendency of giving responses that are influenced by opinions about the research sponsoring company. To avoid this, the researcher should maintain or at least be perceived as maintaining a neutral stance. [42], [43].

2.2.8.2 Researcher bias

Research bias is a behaviour that influences the research results. This means that the researcher interprets the results in a way to portray a certain outcome or/and influences, un-intentionally, the respondent by e.g. asking questions that are leading. Research bias can be further divided into three sub-biases, namely; confirmation bias, question-order bias, leading question and wording bias. [35].

2.2.8.2.1 Confirmation bias

Confirmation bias is the tendency of interpreting evidence in a way to confirm existing beliefs and expectations by e.g. remembering evidence that supports a hypothesis and forgetting or minimizing evidence that does not conform the hypothesis. Hence, as a researcher it is important to re-evaluate all drawn

conclusions based on the answers of the respondents and to continuously challenge pre-existing hypotheses. [44].

2.2.8.2.2 Question-order bias

A question-order bias occurs when a question affects the answers of a subsequent question. This is common for questions that are somewhat related to each other as the preceding questions set the context for the upcoming ones. Hence, to minimize question-order bias, it is suggested to ask general questions precedingly to specific, unaided prior to aided and positive before negative. [45]

2.2.8.2.3 Leading questions and wording bias

Elaborating on the answer of a respondent and providing respondents leading questions and wording leads to bias, sometimes as a result of bias (see confirmation bias). To prevent this, researches should not use leading questions or wording, neither should they summarize what the respondents say in their own words. [46].

3 Project Approach

This chapter gives an overview of the project approach and its three main phases. The methods selected for each phase are described and motivated.

To enhance efficiency and effectiveness of the design process and to make this project successful, the Human-centred design for interactive systems (defined by the ISO-standard 9241-210 (2010)) was selected as the main development approach (detailed description can be found in 2.2.3). This decision was made as it is the most common design approach and, the author is familiar with it.

To facilitate the planning and execution of the design process, the project will be divided into three phases as illustrated in figure 1. The first phase includes the gathering of data about users, stakeholders and competitors. The second phase analyses the gathered data and creates input such as, user personas, articulated conceptual design and requirements specification, into the last phase. In the last phase, the final prototype is created, evaluated and improved. A more detailed description of these project phases can be found below.

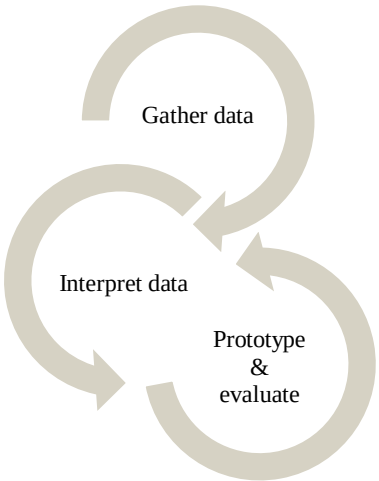


Figure 1. Illustration of the different project phases and how they co-relate

3.1 Data gathering phase

To follow the earlier described design process approach defined by ISO 9241–210 (2010), the data gathering phase aims at specifying the (to be developed) system's context of use. This phase includes:

- An open-ended client (stakeholder) interview with the aim to define a target user and functional requirements
- Conversational interviews with the predefined target user group of today's wallet solutions
- Online research to extract most common user issues of current solutions
- A comparison of today's most commonly used solutions with the aim of defining similarities and differences in terms of design.

Stakeholder interview
An open-ended interview is the most suitable form of a stakeholder interview as the number of participants is small. It would therefore be impossible to obtain quantitative data by conducting a more structured interview. The main goals of the semi-structured stakeholder interview in this project are:

- to identify what problems the system is expected to solve,
- to specify the expected functionality,
- to identify the constraints that might affect the project result and,
- to determine who the produced system is aimed to be used by.

Due to the scope limitations of this project and the fact that the focus of this project is on usability, it has been decided to limit the stakeholder set to the client and end-users only.

A semi-structured stakeholder interview was conducted with the client of the project. The following topics were discussed:

- Functional requirements
- Project constraints
- Stakeholders & end-users
- Common user problems of today's wallets

Notes were taken in between the subjects. Once the interview was completed, a list was created for each topic discussed. The list was sent to the client for a review and once approved, it was set as a basis for further research, see section 4.1.

User interviews
Interviewing is the chosen approach for gaining insights into the needs and requirements of the predetermined user target group of secondary users. This decision was made based on the possibility of attending an engineering conference. The interview structure was kept loose as a more structured and controlled interview requires both more time and space, which was not obtainable. Instead,

conversational alike interviews were conducted with attendees of the conference aimed at investigating:

- to what extent the predefined user target group of today's wallet solutions knows about tokens and blockchain technology,
- what they think of current wallet solutions and their needs.

25 people were randomly selected and interviewed using a predefined set of questions. The interviewees were aged between 23 and 45, all studying some form of engineering program, hence representing the predefined user target group. Each interview took between 5 to 15 minutes. Open questions and closed questions were used to obtain both qualitative and quantitative data and, based on user responses, new questions were asked.

As discussed in 2.2.6.1, interviews can (if not conducted properly) produce false answers due to research bias and respondent bias (defined in 2.2.5). The methods used to avoid the different biases are described below. The definitions of the biases and suggested methods to combat these can be found in section 2.2.8

- Acquiescence bias is avoided by conducting a conversational interview and by presenting oneself, the researcher, as a friend rather than an expert of the subject. Also, questions that facilitate acquiescence are avoided by limiting the amount of closed questions and eliminating any leading questions, hence also minimizing leading questions and wording bias.
- The respondent does not feel observed as the interview feels like a conversation rather than a formal interview, hence preventing social desirability bias.
- The amount of repetitive questions is limited to avoid habituation bias.
- Sponsor bias is avoided by presenting oneself, the researcher, as an objective representant from the University, conducting a background research.
- To prevent question-order bias, related questions are ordered in a way that should not affect the following meaning, general questions are asked prior to specific and aided prior to unaided.
- As to confirmation bias, no hypothesis is defined. However, to ensure that one's own beliefs and expectations are not affecting the conclusions drawn, these conclusions will be re-evaluated before set in stone.

As networking was one of the main activities at the conference, staging a natural occurring conversation did not require much effort. The following questions were included in the interviews:

1. What do you know about blockchain?
2. Do you own any token or cryptocurrency? If yes, Which?
3. Which storing solution do you use?
4. What is your experience with your wallet?

Limiting the number of questions to four simplified the documentation of each interview after each conversation. Once all interviews were conducted, taken notes from the interviews were categorized and summed based on the information content. The summary of the outcomes can be found in section 4.2 while, the in-depth analysis can be found in the discussion.

Online research

To improve the usability of current solutions it is required to research and define common end-user problems and their origin. Some of them have already been identified by the semi-structured stakeholder interview activity (see section 4.1). As the conversational interviews did not provide any useful data regarding end-user problems (see section 4.2), it was decided to search for answers on the web. Different forums were used to read about users, their problems and the cause of these problems. Also, articles defining main user issues and written by different type of designers were studied. The most commonly appearing problems and issues were categorized into three main type of problems, see section 4.3.

Competitor analysis

The main purpose of comparing different solutions is to identify similarities and differences and if possible, map different solutions to a previously defined UX problem, either as a cause or a solution. Another purpose is to identify features that haven't been taken into consideration. Missing a key feature that today's wallets offer, might stop users from changing their wallet.

The first twelve websites, with wallet recommendation content, that appeared after a google search for "best Ethereum wallets" were read. Each website recommended a minimum of 3 wallets and every wallet recommended was written down. A list of a total of twenty wallets was created. The most mentioned competitor solutions that are available today are not necessarily the best ones on the market. However, they are the most used and therefore also the most relevant to analyse in this project. The five most mentioned mobile wallets were compared and analysed.

Each mobile wallet was evaluated against the following questions:

- Where is the seed presented to the user?
- How is the user forced to save the seed?
- What is included in the onboarding process?
- Which potentially unfamiliar terms are used?
- What type of authentication is offered?
- When is the authentication method set up?
- How is the public key retrieved?
- What security options are there?
- Is there any prevention from serious mistakes?
- How is gas fee presented and used?
- What alternative key storing options are available?
- Are there any interesting features?

Questions were inspired by the outcomes of the stakeholder interview and the online research thus, considering all defined problem areas. The different mobile applications were compared based on the answers for each question, section 4.4.

3.2 Data interpretation phase

The data interpretation phase aims to specify user requirements and the application structure (second activity of the ISO 9241–210 (2010) standard) based on the results from the data gathering phase. To aid in this, this phase includes the creation of:

- User personas
- Conceptual design
- Requirements specification
- Application structure

User personas
The user personas in this project are created to be further used as inspiration when articulating the conceptional design. They will also serve as a behavioural basis when defining the application structure. Finally, requirements will be evaluated against user personas to ensure that all the user personas requirements have been considered in the final specification. Three user personas were created with the results from the data gathering phase as inspirational input, two representing primary users, and one representing a secondary user. The previously defined problem areas were used to describe the user persona context and the characteristics of each user persona was based on the predefined user target group, see section 5.1.

Conceptual design
To deliver a user-friendly mobile application it is crucial to solve the usability problems that exist in today's solutions. The first step to achieve this is in this project is to articulate the design on a conceptual level (third activity of the ISO 9241–210 (2010)). Documenting how different usability problems can be solved ensures that they are all taken into consideration in the final design. Each defined usability problem and each user persona has been taken into consideration when defining the conceptual design of the application. The conceptual design, see section 5.2, will further serve as input into the creation of the requirements specification.

Requirements specification
Together with the earlier specified requirements obtained in the data gathering phase (stakeholder interview) and new ones defined in the articulated conceptual design, a more thorough requirements specification was created consisting of both functional and quality requirements. The specification concerns the deliverable of this project and not the application to be implemented in the future. The

requirements specification was created in order to simplify the identification of fundamental features and elements that are vital for the success of the proposed design, see section 5.3.

Application structure
In order to structure features and element effectively, the card sorting method was chosen to obtain an application structure. Since time for this project is limited, it has been decided to conduct the card sorting based on previously defined user personas. Putting oneself in the shoes of each persona and conducting the card sorting, will result in five different structures. The most common appearing groups will later define the final structure. This approach is subjective but less so than if it were not to be based on user personas. [47].

3.3 Prototyping and evaluation phase

The prototyping and evaluating phase of the project implements the requirements in Adobe Experience Design (a software tool, often referred to as XD) based on the obtained application structure in phase two, (fourth activity of the ISO 9241–210 (2010)). This phase consists of usability testing, improvement suggestions and modifications to the system based on the test outcomes, see figure 2.

Figure 2. Illustration of the prototyping and evaluation phase

Prototyping
The information architecture obtained as a result of the card sorting method was used as a basis when designing the structure of the application. The earlier defined requirements specification was used as a feature checklist to ensure that all desired functionalities and elements were included in the prototype. Furthermore, earlier described design principles were used as guidelines and as a quick evaluation tool to ensure that all fundamental principles of design have been taken into consideration, increasing the chances of providing a good user experience. XD was used as the prototyping tool throughout the entire prototyping phase.

Usability testing
The usability testing in this project explored, assessed and validated the design and the overall user experience by gathering both objective and subjective data as well as quantitative and qualitative data. To ensure a consistent performance of the usability testing, a test-plan was created prior to the testing. User personas were used as inspiration when selecting test participants. Seven participants were selected, four representing primary users and three representing secondary. The previously

developed methodology to avoid bias was applied (p. 26). Finally, the testing was carried through.

The following data was gathered during the usability test:

1. *Objective/quantitative data*
    - Task success
    - Task time
    - Errors
    - Whether TL needed to intervene
2. *Objective/qualitative*
    - Description of faults
    - Cues given by researcher
    - Expressions made by the participant
3. *Subjective/quantitative*
    - Questions with a grading of 1-5
4. *Subjective/qualitative*
    - Open questions

The following questions were answered after finalizing the usability testing phase:

A. *Learnability*
    - Can a user make a transaction without any guided help?
    - Is it easy to find the account address?
    - Does the user understand the concept of seed after using the application once?
B. *Efficiency*
    - How quickly can a user set up his own account?
    - How long does it take to make a transaction?
C. *Errors*
    - Does the application prevent the user from making errors?
    - What kind of errors are easily made?
D. *Satisfaction*
    - How does the user feel about the onboarding process?
    - Is the onboarding process too long?
    - Does the security page appeal to the user?
    - Does the security page motivate the user to continue securing the account?

Results were analysed by answering the research questions and, based on the analysis of the outcomes, recommendations for change were documented, see section 6.1. Finally, the prototype was changed according to the documented recommendations (see section 6.2).

4 Data gathering

This chapter contains the obtained results from the methods used in the data gathering phase namely, the stakeholder interview, conversational interviews, online research and competitor analysis.

4.1 Semi-structured client interview

The following results are the outcomes of the conducted interviews, described in 3.1.

4.1.1 **Functional requirements of the solution**

The minimum functional requirements for the expected system to be delivered, as defined by the client interview, are:

R1. Wallet set-up
The wallet should have an onboarding process where the user is asked to write down the wallet seed.
R2. PIN/faceID/Fingerprint authentication
The user should be prompted to set-up an authentication method for quick access.
R3. Send & receive ether
Once the wallet is set-up. The user should be able to send and receive tokens to other addresses.
R4. Export private key
The user should be able to export the seed from the wallet at any time provided that the user is authenticated.

4.1.2 **End-user definition**

The primary end-users are users who are new to the concept of using tokens. They have either read about tokens in the media, stumbled upon something that requires a token or, they have heard about tokens from someone they know. These people are often interested in the financial benefits of trading tokens or, have a technical

agenda meaning, they want to use their token e.g. in a DApp. They are familiar with the token concept to the extent that they understand that a token is a collectible item that can be stored and transacted with the help of a wallet.

Secondary users are current users. These users most likely have a technical or financial background and they use different solutions that expose them to different concepts of blockchain. They are used to: conducting research in order to understand the technical concepts that they are exposed to and, determining the best methodology to achieve their goal. Both primary and secondary users already own ether. Primary users want to move their ether from third party owned account to a wallet while secondary users are those who want to change their wallet. Both primary and secondary users have some form of higher education.

4.1.3 **Common end-user problems in today's wallets**

4.1.3.1 Serious mistakes are easily made

Serious mistakes such as sending tokens to the wrong address and writing down the seed wrong are easily made. Seeds are not displayed in a way that prevents this and the solutions of today do not force the user to write down the seed correctly. The address of someone's account is long and consists of a sequence of meaningless, for the user, numbers and letters. Hence, the risk of making a mistake while typing in someone's address is high.

4.1.3.2 Consistency and learnability

The different wallets of today are inconsistent. Different terms are used to describe the same things e.g. private key, seed, recovery sequence. This means that each time a user tries a new wallet, he or she must re-learn the meaning of different words or learn new words. Some wallets use several terms to describe the same thing.

4.1.3.3 Slow and tiering transactions

To perform a transaction a so-called gas fee must be paid. Depending on how much the user is willing to pay, the fee amount determines the speed of the transaction. A transaction might go on for weeks being unconfirmed without the user being able to revert it if the gas fee is set to a very low amount. This means, the user cannot, after a transaction has been made, choose to pay more for the gas fee in order to speed up the transaction. Most wallets of today do not explain how the gas fee affects the speed of transaction. Instead, the user is left with the option of choosing the amount and is, at some point (if the amount was not high enough), surprised that the transaction is still unconfirmed. This leads to user dissatisfaction and frustration.

4.2 Conversational interviews

The following results are the outcomes of the conversational interviews, described in 3.1.

The following points summarize the obtained responses.

- According to the answers of question 2, none of the conference attendees owned any tokens, cryptocurrencies nor a wallet.
- 23 of 25 had heard about the cryptocurrency Bitcoin.
- 4 had heard of Ethereum.
- None of them knew the concept of private key management and tokens.
- All were familiar with the word cryptocurrency. The main source of information was word of mouth or reading about it in the media.

4.3 Online research

The most common usability problems of today's wallet solutions, according the online research, section 3.1, are presented below.

4.3.1.1 Users are expected to understand the concept of secure private key management

Users are expected to understand and know the concept of secure private key management when using today's self-sovereign token storing solutions. A user who wishes to set-up a token wallet and start collecting and trading tokens, is expected to be aware of the severity of losing the wallet generated seed. Based on the majority of today's token wallets, the user is expected to know the following; not having access to one's seed equals in most cases to losing one's token wallet and all its content as represented in the physical world.

Users that do not understand the concept of the seed don't always realize the importance of saving and storing the seed in a secure and retrievable place. This has led to users losing their tokens and, in some cases, their fortunes. [48], [2], [1], [49]

4.3.1.2 Users are not being helped with keeping their wallets safe

Users are responsible for secure safe keeping of their own keys. As earlier mentioned, a user is responsible for holding and storing the wallet seed. In today's banking apps a user has several options of retrieving access to an account. Different authentication methods are possible and the third party, the bank, can in most cases help a user retrieve access to an account. The latter is only possible since the account is controlled by the bank. In a nutshell, this gives the end-user a feeling of security

and assurance and, allows the user to make mistakes, such as losing access to credentials.

In the world of blockchain, where information is decentralized, third party-controlled wallets are few and unpopular amongst today's users. Non-third party owned wallets are owned by whoever holds the seed making them fully secure as no third party can access them (e.g. a bank taking penalty fees from one's account because they own the account). Hence, wallets seldom offer different ways of storing and retrieving the wallet seed which creates major risks for the unaware user. [50], [51].

4.3.1.3 Alternative key storage methods are too complicated

Current alternative key storage methods are too complicated and, in some cases, can seem impossible to execute for the average user as they require a lot of effort. Most storing solutions today require users to understand different technical concepts which limits the end-user spectrum. These alternative methods are seldomly found in wallets of today, especially in mobile wallets. [52], [53]

4.4 Competitor analysis

The outcomes of the competitor analysis, section 3.1, can be found below. Other data such the Ethereum wallets considered and the websites included in this comparison analysis can be found in Appendix A.1.

4.4.1.1 Most mentioned mobile

The five most mentioned mobile wallets are Guarda, TrustWallet, BRD, Jaxx, and Coinbase.

4.4.1.2 The onboarding process

Guarda does not have an onboarding process. Upon opening the Guarda application for the first time since download, the wallet is created automatically. In Coinbase and Jaxx wallet, the user must accept the terms of use in the beginning of the onboarding process. In Jaxx wallet, the user is asked to set-up different accounts since it not only offers to store ether, but also other currencies. Additionally, the user is also asked to specify the currency in which the total value of the content of the wallet is to be displayed as. Setting up an authentication method is part of the onboarding process in Coinbase, Jaxx (custom onboarding process) and in BRD Wallet. The seed process is included in the onboarding of Coinbase, Jaxx (custom), BRD and TrustWallet.

A slow onboarding process with many steps might demotivate the user to finalize the wallet creation. In order to provide a simple and fairly quick onboarding process all unnecessary steps that do not affect user security should be eliminated. However,

user security must always go ahead of usability. Hence, the user should be forced to set-up an authentication method and write down the seed at some point before any assets are transferred to the wallet. However, any other customization should be offered once the wallet has been created.

Table 1

	Coinbase	Jaxx express	Jaxx custom	BRD	TrustWallet	Guarda
Terms of use	X	X	X			
Authentication	X		X	X		
Seed process	X		X	X	X	
Username set-up	X					
Accounts set-up		X	X			
Currency set-up		X	X			

4.4.1.3 Seed process

The seed is commonly presented in the last step in the onboarding process and under settings tab (Coinbase wallet, Trustwallet and BRD wallet). This is also accurate for Jaxx wallet if custom set-up is chosen. In Guarda, the seed can only be accessed in settings. In most wallets, the seed process is optional (Coinbase, Jaxx, BRD, Guarda) and can be skipped. TrustWallet is the only wallet that forces the user to write down the wallet seed - the wallet is not accessible unless the user solves the seed puzzle. A seed puzzle meaning, the user is asked to order previously presented seed words, is a common way of making sure that the seed is written down by the user (Coinbase, Jaxx (custom -set-up)). BRD Wallet on the other hand, asks the user to type in two words from the seed sequence whereas, Guarda asks the user to provide the whole sequence. Guarda is the only wallet that both checks the order and the spelling of the seed sequence. If the user decides to skip the seed process in BRD and Guarda, the user is notified that this action is important. In Guarda the user is reminded to write down seed before signing out. Also, in Guarda, if the user hasn't visited the Wallet Security tab, where the seed can be accessed, there will be a notification icon next to the tab as long as the tab is not visited. BRD on the other hand, shows a message on the main page.

None of today's wallet solutions force the user to write down the seed words with the right spelling in the right order. Either the seed process is optional, does not exist in the onboarding, or only the order of the words is checked and not the spelling. In conclusion, there is a lot to improve from a security perspective.

Numbering the seed words makes the process effective because, the user can quickly identify (if the numbers have been written down together with the seed) which words have been written down and which are left. It also ensures that the words are

written down in the right order. BRD wallet makes the process of writing down the seed word even more fail proof by showing one numbered word per screen. However, in the unlikely event of writing down a word wrong, the process of going back is unnecessary and breaks the onboarding flow because, one must go back as many pages as there are words. A simple way of solving this would be to provide a button that takes the user back to the first seed word. However, if the user is forced to type in the whole seed sequence, there is no need for making the writing down process fail proof to the extent that it becomes time consuming and requires a lot of static interaction. To make sure that the spelling is correct, words should be typed in by the user and not be provided by the application (compare to seed puzzle). The most effective and user-friendly way without compromising security would be to first, present the user with numbered seed words (perhaps in segments of 3) and second, force the user to type the seed words with the right spelling in the right order on the next page.

4.4.1.4 Authentication method

All wallets offer PIN-code authentication. Coinbase and BRD Wallet also offer biometric identification. Setting up the authentication method is only mandatory in Coinbase. As previously mentioned, the authentication method is either set-up in the onboarding process (Coinbase, BRD Wallet, Jaxx - if custom onboarding set-up is chosen), or under the settings tab, (Guarda, TrustWallet, Jaxx (if express onboarding set-up is chosen).

The temporary authentication gives temporary access to the wallet in the event of losing one's seed. Hence, not forcing the user to set-up a temporary authentication method increases the chances of losing one's assets. Therefore, for security reasons, the user must be forced to set-up an authentication method. Also, the user should be notified that biometric authentication method is the safest option as the chances of losing a PIN-code is more common than biometric identification failing.

Most smartphones today force the user to set-up a second authentication method (PIN-code or pattern) when a biometric authentication method is set-up in case the biometric authentication method fails. The simple reason is that if the biometric authentication fails, it is not the user's fault. System errors must be avoided at any cost. Hence, a similar approach (with a backup authentication method) should be taken in this project.

4.4.1.5 Language

The different terms that are used in today's wallets and that might be unfamiliar to the target user group are; token, crypto, collectible, DApps, recovery phrase, back-up phrase, private key, decentralized app, protocols, public address, public key, protocols, miner, block, mining fee, phrase and pairing code, paper wallet, paper key, blockchain synchronization, bitcoin nodes.

The conclusion that can be drawn is that users of today's wallets are forced to familiarize themselves with technical terms. In addition to this, in some wallets, different terms are used to describe the same concept, e.g. private key, seed, recovery key etc. (see 4.1.3.2). Thus, there is room for improvement in terms of consistency and usability meaning, being consequent with wording and limiting the amount of technical terms.

4.4.1.6 Public address

There are three common functionalities that concern the public address. The address can either be copied, shared or scanned in most cases.

Table 2

	Coinbase	Jaxx	BRD	TrustWallet	Guarda
Copy button	x	x		x	x
Share button	x	x	x		x
Barcode		x	x	x	x

As can be seen in table 2, all applications offer at least two of the mentioned functionalities. Therefore, to satisfy current users of today's wallet solutions, all three functionalities should be offered.

4.4.1.7 What security options are there?

All wallets offer PIN code as authentication method and only two offer faceId/fingerprint authentication (Coinbase, BRD). Coinbase allows the user to change the auto-lock time. The seed can be viewed in settings in all applications. In conclusion, users are not being helped with keeping their wallets safe (see 4.3.1.2) There seems to be room for improvements in terms of offering security options such as implementations of multi-signature and Shamir's secret sharing algorithm.

4.4.1.8 Gas fee

Gas is not explained and is presented as "gas limit", previously defined under 4.1.3.3. Users can enter any amount but no explanation regarding how the gas fee affects the transaction is available (Coinbase, Jaxx, Guarda, TrustWallet). To improve this, the user needs to be made aware of the relation between the transaction speed and the transaction fee.

4.4.1.9 Interesting observations

Both the Coinbase Wallet and TrustWallet includes a DApp explorer that lists all common DApps. TrustWallet enables the possibility to have multiple wallets within one application. Jaxx provides the option of storing addresses in an address book where one can store wallet addresses temporarily (as long as the application is not

re-installed or deleted). However, these addresses are not accessible when making transactions. The only feature the address book has is the ability to copy a saved address. Jaxx also offers crypto in-app purchases. BRD Wallet offers a request amount feature that allows the user to create a custom made QR code that when scanned, fills out both the amount and the address. BRD Wallet also lets the user limit the amount that can be spent with biometric authentication. If the user wants to spend above that limit, PIN-code must be provided. Guarda is the only application that allows the user to remove the wallet from the application. If one wants to delete the wallet from the other applications, the whole application must be un-installed. Guarda also offers exchange possibilities, crypto in-app purchases and in app chat support. No applications offer any key storing options.

In Coinbase and Jaxx, the seed can be screenshotted, in TrustWallet it can be copied. It is debatable whether this is a security risk or not. If the user copies the seed or takes a screenshot of it and stores it on their phone, the access to the wallet will be lost hence, defeating the purpose of the seed process. If the phone is hacked, the seed is exposed. Whether it is or isn't a secure risk depends on how the user uses the function. Hence, it is suggested to eliminate these functions to provide a better security for the un-aware user.

Coinbase offers the option of setting-up a username. Instead of sending tokens to an address, a user can enter a username. Thus, limiting the risk of writing down an address wrong. This feature works for transactions between Coinbase wallets only and, is redundant since there already exist an implementation that works for all Ethereum wallets namely, Ethereum Name Service (ENS) names. As with domain names, the ENS name is connected to a specific address and can be bought and sold as easily as any domain name.

None of the compared wallets offer any method of integrating a hardware component with the application. Hence, to appeal to most users, setting up the wallet with a component should be made optional. Also, to appeal to most users, the application should be compatible with the three most commonly used hardware components.

5 Data analysis

This chapter contains the obtained results from the methods used in the data analysis phase namely, the user personas, conceptual design, requirements specification and the application structure.

5.1 User personas

The following user personas were created according to the described methodology in section 3.2.

5.1.1 **Paul, 30 years old, "I just want keep my Ethereum"**

Paul is an Engineer working at an IT company. Paul does not know anything about blockchain or how tokens work. He first hears about Ethereum at work from his co-workers. Intrigued, he decides to buy some ether using a known broker. After telling his co-workers about his new investment and having discussions about how to keep his investment safe, Paul realizes that he can't let a third party, the broker, hold his ether for him.

Paul is very active on his spare time and barely has any time left for new hobbies. He therefore wants and expects the process of setting up a new wallet to be easy and quick. After some shallow online research, he decides to try the X app – known for its safety and great usability. He downloads the free app and starts the process of onboarding. At first, he is asked to write down a sequence of words (seed). Once written down, Paul is asked to enter the words he just wrote down. The application ensures that Paul has written down the seed words correctly and understood that must do it before depositing any assets. A few steps later, Paul is asked to choose an account method; with or without a hardware component. Paul is concerned about security and decides to read more about the hardware component. Paul wants the most secure option and to his convenience, the component can be ordered directly within the app. The onboarding is put on hold, but the app provides him with information about his order. Once received, Paul is happy to set up his wallet without having to do any research. Unknown and uncommon terms are explained

within the app and the integration between the wallet and the component are explained in a tutorial. Paul connects the hardware component to the application and goes through with the onboarding, moves his ether from the third-party account to his new wallet, signs out from the app, stores the hardware component in his safe and goes back to his activities.

5.1.2 **Anna, 25 years old, "I just want to attend a Hackathon"**

Anna is a newly graduated UX designer and has a boyfriend, Tom. Tom wants Anna to attend an Ethereum Hackathon with him. Tom is a developer and together they will make a great team. Once they've both sent in applications there is an option of staking ether meaning, those who stake have a greater chance of being accepted to the Hackathon. Unfortunately, there is one problem. Anna does not own any ether and neither a wallet. Tom, who works for the company behind X, suggests a simple solution; that Anna downloads the X app and that he will transfer her the amount required. Tom also uses app X. Once Anna has downloaded and set-up her wallet, Tom scans the barcode representing her address with his camera in his wallet app. The app gives him two options; to save the address together with a chosen name or, to create a new transaction to this address. He saves her address in the app and names it "Anna" for future transactions. He makes the transaction and once received, he does the staking transaction for her with her phone. After two weeks Anna receives bad news, her application did not go through. The app notifies her that she has received a refund. She decides to send Tom back the refund. It seemed so easy when Tom did it and so, she is confident to make the transaction on her own. She enters the history of transactions, presses the old transaction from Tom and his address. She saves his address together with his name and starts making a new transaction. When making the new transaction, Anna sees that she can't pay him back everything as she must pay for a transaction fee as well. The fee varies and depends on how quick Anna wants the transaction to be. She has the option of choosing; within minutes, hours or days. The pre-set option is within minutes. Anna decides to choose the cheapest option, within days, since there is no rush and this way, Tom can get more ether back.

5.1.3 **Maria, 60 years old, "I just want to invest in a company"**

Maria is retired. She studied economics in her early life and she has always been investing in stocks. She now wants to invest in a company that only takes ether as payment method. Maria asks her daughter to buy her the amount of ether that she needs. Her daughter who frequently uses ether, lives abroad and is not able to create a wallet for her mother. Maria must set up a wallet

herself and she downloads the X app, as suggested by her daughter. She does not order the hardware component at first. Once the onboarding process is completed, Maria is asked to send her daughter the wallet address. Maria presses the receive button in the app and shares the address from the app to her daughter through a chat app. A few minutes later, Maria receives a notification saying that she has received a payment. Maria enters the website where she wants to invest her ether. At the last step of the investment process, she is given an address to where the investment should be sent. Maria presses the send button in the app, scans the address (a long sequence of numbers and letters), with the camera and confirms the transaction. Once the transaction has gone through Maria is notified and she is also asked to consider to back-up her recovery key (seed). Maria decides to enter the security settings where she is made aware of the level of security she has at the moment. Maria realizes the importance of backing up her key and decides to read more about the different options available in the app.

5.2 Conceptual design

This document presents the articulated conceptual design and its different components.

5.2.1 **The onboarding process**

The application will have an onboarding process where the authentication method is set-up. The authentication method is mandatory for security reasons as discussed in section 4.4.1.4. The offered methods will be faceId/fingerprint or PIN code authentication. Additionally, the user will be forced to set-up a PIN-code authentication as back-up when choosing biometric authentication as main authentication method.

Once the authentication method is set-up the user will be asked to choose a wallet set-up method, either with a hardware component or without. If the user chooses to set-up the wallet with a hardware component, he or she can either continue with the onboarding process (if the component is at hand) or, order the hardware component directly within the application. If the user decides to order the hardware component, he or she can get updates about the delivery in the application, see 5.1.1. Once the component is delivered, the user can continue with the set-up process.

The user can also continue the onboarding process without the component and order it at a later stage as motivated in 4.4.1.9.

5.2.2 **The seed process**

The following wallet set-ups are possible within the application:

- The application stores the seed and the public address.
- The application does not store the seed but stores the public address. The component holds the seed and needs to be connected to the smartphone for any transaction.

To address the problem defined under 4.1.3.1, the seed process will be made mandatory. The user will be forced to go through the process before any funds are at risk meaning, before any deposit can be made. The seed process will look differently depending on which wallet set-up was chosen.

5.2.2.1 With hardware component

The user is asked to connect the hardware component to the mobile application to transfer the public address of the hardware component to the application.

5.2.2.2 Without hardware component

In order to keep the onboarding process as smooth as possible (see 4.4.1.2.) the seed process will be made optional in this phase. However, if the user decides to skip the process in the onboarding, the user will not be able to deposit any funds until he or she goes through the seed process at a later stage. Before any depositing is made, the user will be forced to go through the seed process. If on the other hand, the user did go through the seed process in onboarding, this will not be required.

The seed process is as follows. The user is presented with the seed words and asked to write them down and store them in a secure place. In the next step, the user is asked to type the words in.

To address problem 4.1.3.1 and as suggested in 4.4.1.3., the user will be forced to write down each word in the right order. This process is time-consuming, however, the mistake of not writing the seed down correctly might lead to disastrous consequences. Hence, security is prioritized over usability in this case. To avoid mistakes in the process of writing the seed down, the process is facilitated by presenting the seed words in sections of three. This way the user can easily identify which words have been written down and which have not. For security reasons, the seed should never be shared or sent through the internet or, be saved on a device (outside the application) that is connected to the internet. Also, since the seed process is mandatory, any method that can help the user to skip or cheat this process should be eliminated. Thus, functionalities such as screenshot and copy/share will be restricted when concerning the seed.

5.2.3 **Transactions**

To aid in the prevention of writing down the receiver's address wrong when performing a new transaction, problem 4.1.3.1, an address book feature is suggested (discussed in 4.4.1.9). If the user can store an address which he or she is planning to re-use in the future, the risk of writing the address down wrong the second time is reduced. Unlike in Jaxx wallet, the addresses will be easily accessed when making a transaction.

To further aid in this, a feature that enables the user to request a specific amount to one's wallet is suggested. As seen in BRD wallet (see 4.4.1.9) this is made possible through a custom made QR-code. The wallet generates a custom made QR code with the input of a requested amount. When the QR code is scanned, the address field and the amount field are automatically filled in the app of the sending user. Not only does this method prevent the user from typing in the wrong receiver address, it also ensures that the amount typed in is the requested amount.

In order to compete with commonly used solutions of today, any new wallet application should offer these features as well as fundamental ones such as, copy/share public address/QR-code (see 4.4.1.6).

To partly address problem 4.1.3.2, the gas fee will be named "transaction fee". As seen in the comparison analysis, most wallets do not provide any explanation for the gas fee (see 4.4.1.8). Neither do they provide any information regarding the transaction speed and how it is connected to the gas fee. To reduce the amount of slow and tiering transactions (see problem 4.1.3.3) the user must understand the concept of gas fee. The user must know that the transaction fee will affect the speed of transaction. To avoid too much technical information and to present this information in the most effective and intuitive way, the user will be presented with three options of transaction speed; within one minute, within one hour or within a day. The transaction fee will vary based on the time option chosen and the user will not only understand the connection between the gas fee and the transaction speed but also, be able to decide the speed of transaction without any technical knowledge. With this solution, the decision task changes from deciding the fee to, deciding the transaction speed. Considering that fees usually are static and not changeable, this new solution is more intuitive for a non-technical user when compared to more commonly used solutions.

Additionally, there must also be more information available explaining to who the transaction fee goes to and why the fee for one option might vary different days. This extra information will be accessible whenever the user is asked to choose the transaction speed and wishes to read more about it.

5.2.4 **Security**

The user will be able to access the wallet seed/update the public address with the hardware component at any time in the app. The user will also be able to update authentication method in the app. As seen in 4.4.1.7 most of today's wallet solutions do not offer any security options apart from the option of changing auto-lock time. To address problem found under 4.3.1.2, "Users are not being helped with keeping their wallets safe", providing several storing and retrieving options might not only eliminate the pressure that comes with being one's own secure safe but also give the user a similar level of assurance one would get from trusting a third party. Hence, options such as multi-signature and an implementation of Shamir's secret sharing will be offered as an extra feature within the app. The user will also be able to order a hardware component within the app that could be used as a secondary back-up of the seed, part of the multi-signature or simply as a hardware wallet meaning; the application does not store the seed on the mobile device and thus, the hardware component must be connected to the smartphone when making transactions. The wallet will also be compatible with the most used hardware components of today, discussed in 4.4.2.9.

Apart from offering the above-mentioned storing options, they also need to be simple to use (see problem 4.3.1.3). To give the user an outline of the already taken security measures, an overview of how secure the wallet is will be presented to the user. To make sure that migrating users do not lack any basic features that were available in their previous wallet, changing auto-lock time will be added as a feature.

5.2.5 **Language**

As seen in 4.4.1.5, language can be a barrier when it comes to usability. Different terms that describe the same words will not be present to avoid confusion. Technical terms will be used sparingly. The ones used, will be repeated and explained several times.

5.3 Requirements specification

The final requirements specification consists of both functional and non-functional (quality) requirements.

5.3.1 **Quality requirements**

RQ1. Usability: 4/5 of the users in the usability testing agree with the statement "The application is easy to use"
RQ2. Learnability: 4/5 in the usability testing can perform all tasks in this specification without errors on the second time using the application
RQ3. Integrity: A user shall only be able to access the wallet with the right authentication credentials or seed
RQ4. Security: If the authentication has failed 3 times, the user can only access the wallet with the seed
RQ5. 5/5 users are familiar with all terms used in the application
RQ6. Different terms that describe the same words will not be present
RQ7. 4/5 users know the meaning of the terms used in the application
RQ8. The user understands the importance of writing down the seed
RQ9. The user understands what he can do to add more security layers

5.3.2 **Functional requirements (Product level)**

RF1. The application shall have an onboarding process, specified by task 1.
RF2. Smartphone functionalities such as screenshot & copy will be restricted during the seed process
RF3. User shall not be able to deposit unless the user has gone through the seed process
RF4. The user shall be able to view the account address
RF5. The user shall be able to copy the account address
RF6. The user shall be able to share the account address
RF7. The account address shall be presented as both a sequence of numbers and letters and a QR code
RF8. The user shall be able to create a custom QR code with amount as user input, that when canned fills out the address and amount section automatically
RF9. The application shall hold an address book
RF10. The user shall be able to view a contact
RF11. The user shall be able to delete a contact
RF12. The user shall be able to edit a contact
RF13. The user shall be able to create a new contact
RF14. The application shall support transactions

RF15. The user shall be able to select a recipient by
- Selecting from contact list
- Inputting address sequence
- Scanning address sequence
- Scanning barcode

when making a transaction

RF16. The user shall specify amount to send when making a transaction
RF17. The user shall be able to choose transaction speed when making a transaction
RF18. The user shall be able be presented with an overview of the transaction details before confirming a transaction
RF19. The user shall be notified when a transaction is received.
RF20. The user shall be notified when a transaction has been confirmed
RF21. The gas fee will be presented as transaction fee.
RF22. The application will provide explanation for the transaction fee
RF23. The user will be given three options of transaction speed, within a minute, an hour and a day
RF24. The wallet balance will always be visible
RF25. The balance will be displayed in ether and in dollars
RF26. The wallet will contain a list of transaction history where each transaction can be clicked into
RF27. The application will provide the user with an overview of how secure the wallet is based on which security measures that have been taken by the user
RF28. The user will be able to change authentication method
RF29. The user will be able to change auto lock-time
RF30. The user will be able to back-up seed provided that he or she can authenticate oneself
RF31. The user will be able to set up multisignature
RF32. The user will be able to split and share the seed to contacts (Shamir's secret sharing implementation)
RF33. The user will be able to set a spending limit
RF34. The user shall be notified, once a month, to back-up the wallet seed
RF35. The user shall be able to turn of notifications

Task 1.	*Onboarding process*
Purpose	Create new wallet
Frequency	One-time event
Sub-task 1.	Application generates and presents seed. Seed words are numbered and presented in sections of three words per page.
Sub-task 2.	Optional: User is prompted to enter seed words in the right order with the right spelling
Sub-task 3.	Optional: User is prompted to set-up quick authentication: a) FaceID & PIN-code b) Fingerprint & PIN-code c) PIN-code
Sub-task 4.	User is asked to choose account type a) Without hardware component b) With hardware component
Sub-task 5.	User is informed of different key recovery methods and where they can be found and set-up within the app

5.4 Card Sorting

5.4.1 **Application structure**

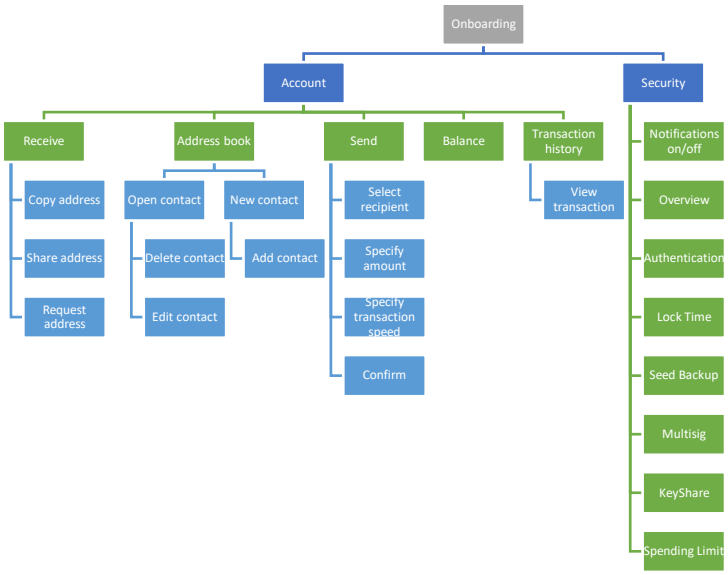


Figure 3. The application structure defined through the card sorting method

6 Prototyping & evaluation

This chapter presents the results from the prototyping and evaluation phase, namely, prototyping and usability testing.

6.1 Resulting prototype

The first prototype created consists of eight pages illustrating the onboarding process, figures 4-12, and twelve pages illustrating the main structure of the application, figures 12-23.

Onboarding

Figure 4. The user can create a new or, restore an old wallet

Figure 5. Feedback – the user knows how many steps are left (3)

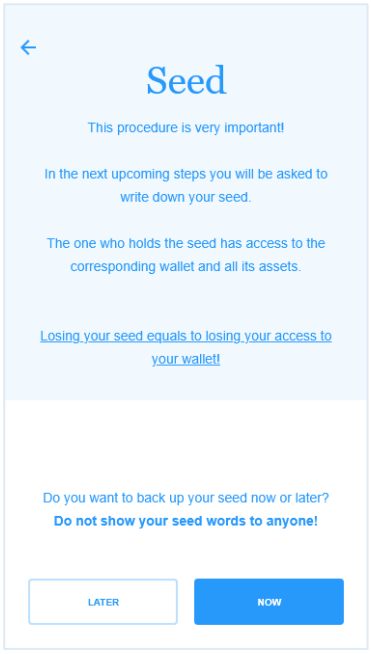


Figure 6. Seed process is optional to provide a quick onboarding process

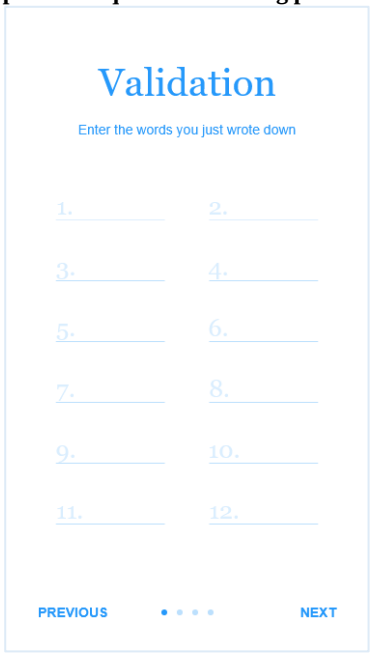


Figure 7. Both the spelling and the order of the seed is checked

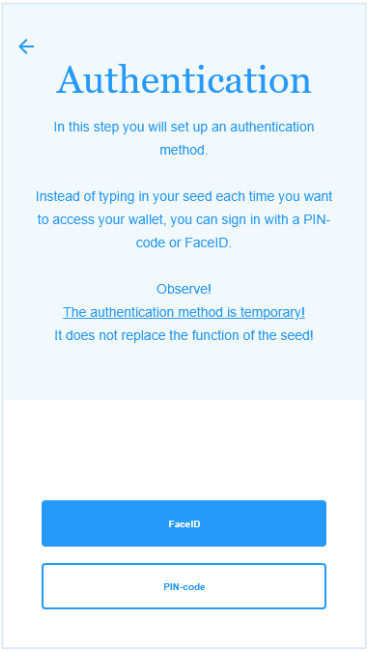


Figure 8. The user is informed that the authentication method is temporary

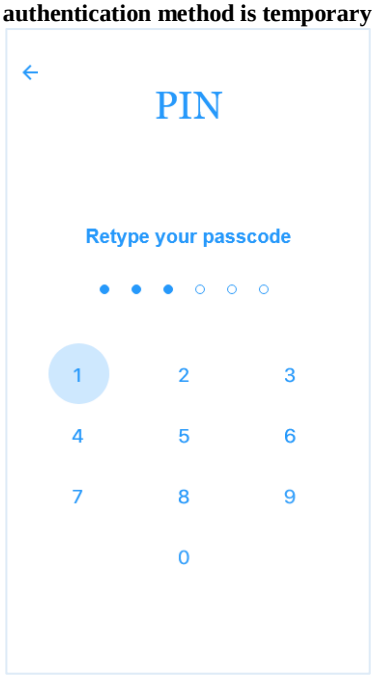


Figure 9. Feedback - The user knows which digit was entered (digit background changes to blue)

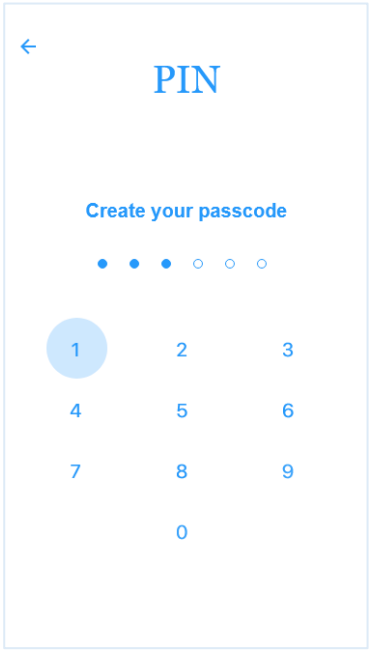


Figure 10. Feedback – the user knows how many digits have been pressed

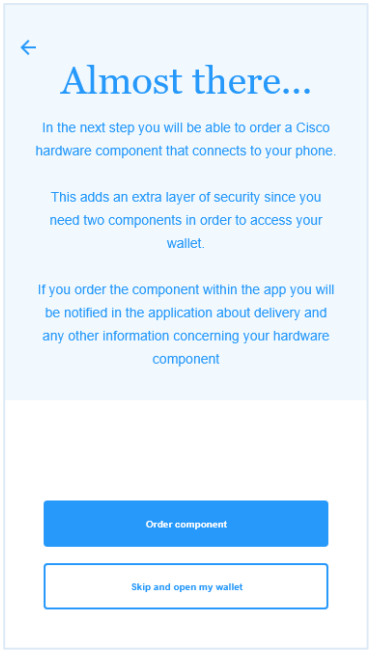


Figure 11. The user is not forced to order a hardware component.

Application

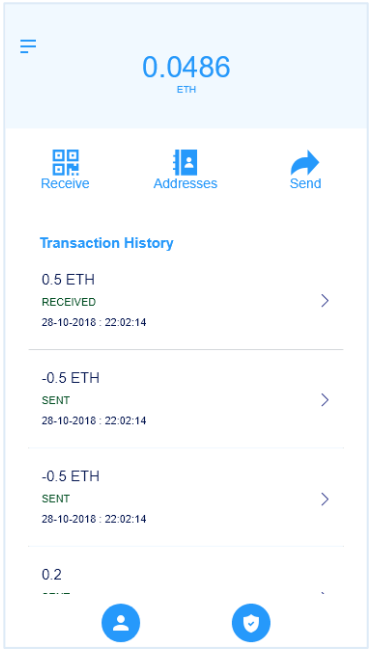


Figure 12. Consistency – Tabs and sub tabs have a consistent design (icons)

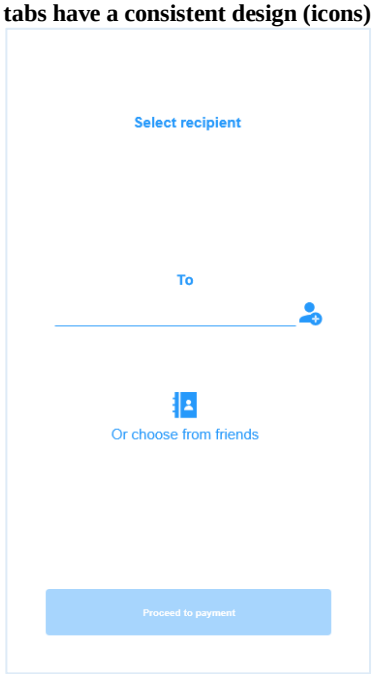


Figure 13. Constraint – user can't proceed without selecting recipient

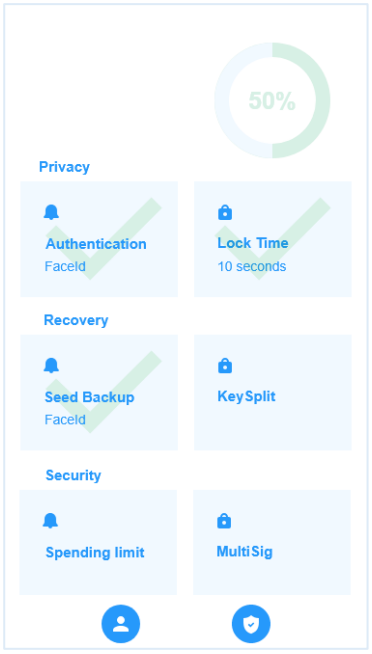


Figure 14. Mapping/feedback – Security and enabled features are marked green

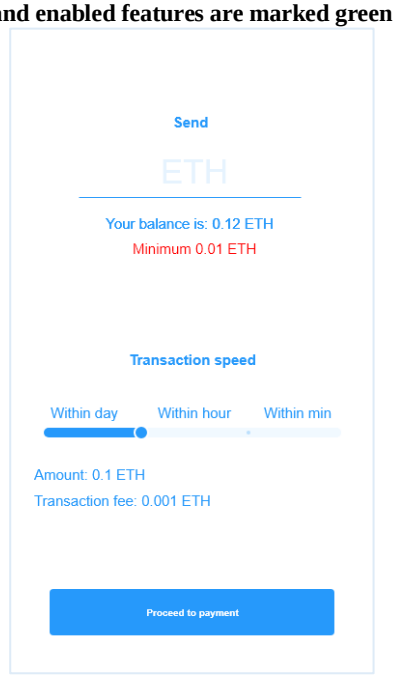


Figure 15. Transaction fee is named transaction speed

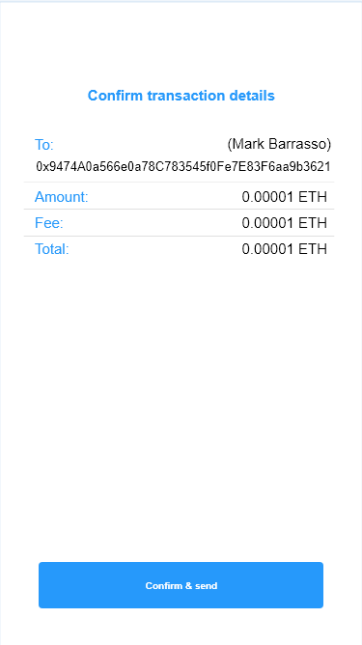


Figure 16.

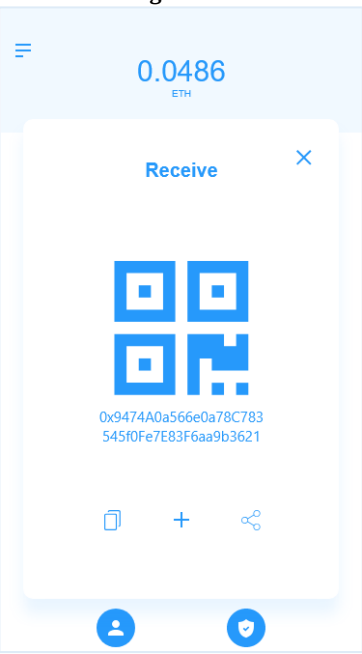


Figure 17

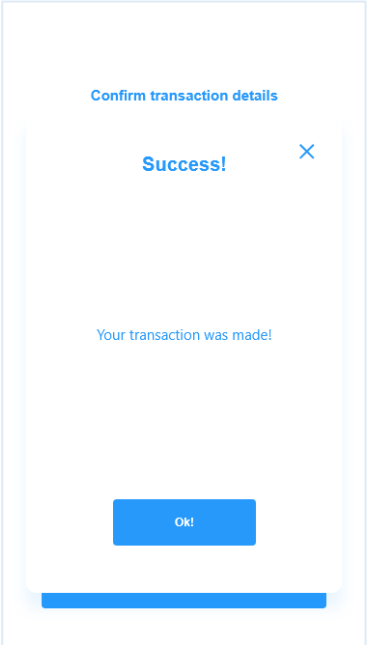


Figure 18. Feedback – user gets confirmation if transaction has been submitted

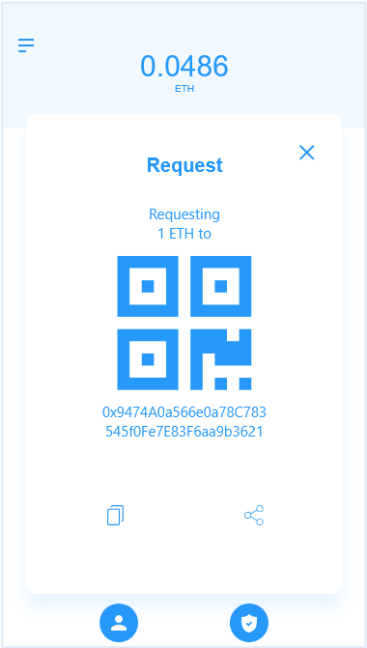


Figure 19

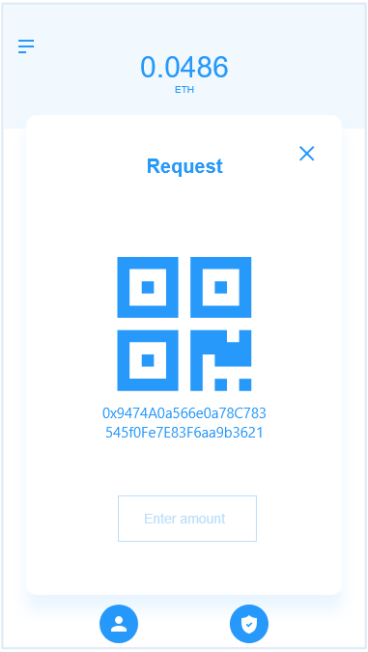


Figure 20. Commonly used icons are used for common purposes (account & security tab)

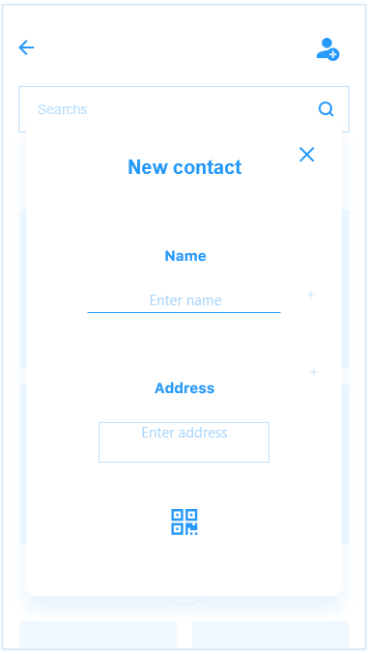


Figure 21

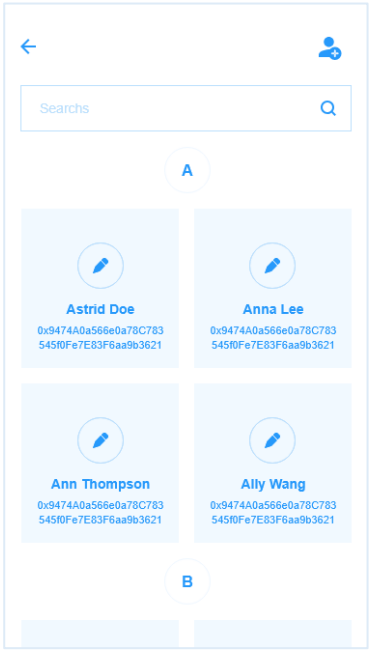


Figure 22

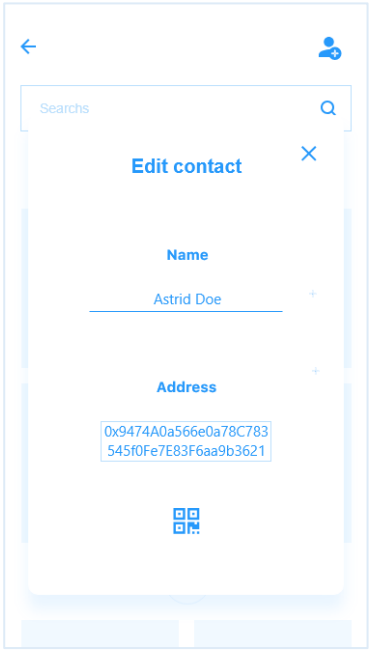


Figure 23

6.2 Usability test results

This section summarises the result analysis of the usability testing. The test material given out to participants can be found in Appendix B. Four of the five components that together define the term usability have been assessed and are:

6.2.1 **Learnability**

- Can a user make a transaction without any guided help?

Yes. All users completed the transaction task without any guided help

- Is it easy to find the account address?

3/7 users could not find the account address immediately. According to them, the icons for receive and send are not easy to understand – they do not match the text "Receive" and "Send", figure 12. One suggestion that came up is to use arrows, one that points up for the send feature and one that points down for the receive feature. The logic here is that receive and send are opposites and should be illustrated by e.g. opposites arrows. See 6.2.6 Task 2.

- Does the user understand the concept of seed after using the application once?

6/7 understood the concept and the importance of storing the seed in a secure place. They explained the importance when responding to question 1, see appendix B. One participant could not grasp the concept technically – not design related.

6.2.2 **Efficiency**

- How quickly can a user set up his own account?

All users were able to set-up the account under five minutes. 4/7 chose to skip the seed process and completed the onboarding under 2 minutes.

- How long does it take to make a transaction?

Three users completed the task under 3 minutes and the rest under 5 minutes. Users spent a lot of time understanding the second transaction screen, figure 15. Three of them complained about the amount of information being presented. When selecting recipient, figure 13, 3/4 users did not understand that they were choosing one out of two options for selecting an address (enter address manually or select from contacts).

6.2.3 **Errors**

- Does the application prevent the user from making errors?

Yes, to some extent, some errors are not prevented, see below

- What kind of errors are easily made?

3/4 users tried to select recipient twice in second transaction screen, figure 13. Two participants wanted to scan the address immediately – no such feature. They both suggested that the feature should be a main feature since it is a feature that will be used frequently.

6.2.4 **Satisfaction**

- How does the user feel about the onboarding process?

Users found the onboarding process intuitive, see 2.6.2 Task 1.

- Is the onboarding process too long?

No, it is under five minutes

- Does the security page appeal to the user?

Yes, all of the participants found the security page appealing

- Does the security page motivate the user to continue securing the account?

Three out of seven thought that the non-implemented features should stand out more and be more alarming by e.g. using the colour red, figure 14.

6.2.5 **Other comments made by participants**

During the usability test, participants found several issues that had not been addressed. One being, a user cannot empty one's account completely. Instead of manually specifying an amount to send the user should be able to send whatever is the maximum (depending on the transaction speed chosen and the current fee for that speed). Users also noticed that a contact can't be deleted and that changes cannot be saved – features that was mistakenly forgotten during the prototype phase. Users also commented on the fact that the consequence of pressing the icon representing "Request' under "Receive" is not clear. Also, users can not reset the value once entered.

Recommendations for change: Add option to delete contact. Re-think the request amount design (amount should be easily reset and icon to request needs a better mapping)

6.2.6 **Average grading question results**

Task1:

How intuitive was the onboarding process?

Average score: 4.2

Task 2:

Was it easy to locate your account address?

Average score: 2.1

Task 3:

How was your understanding of the different steps when making the transaction?

Average score: 3.7

Task 4:

Was it obvious to you which steps have been taken so far and which have not?

Average score: 4.3

6.3 Resulting prototype based on improvement suggestions

6.3.1 **Application structure**

Based on the recommendations from the usability test, section 6.3.2, the application structure was re-designed. The “scan” feature was added as a main feature and hence, as a main tab.

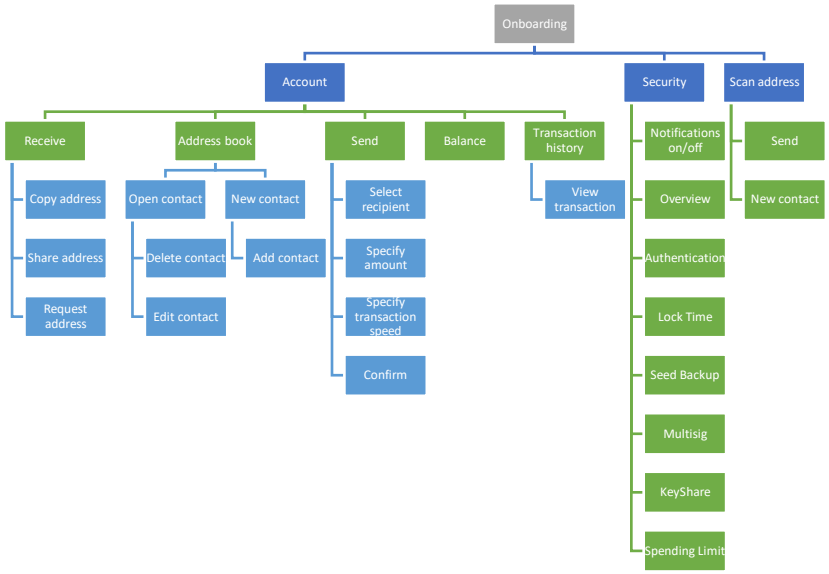


Figure 24. The re-designed application structure based on suggested improvements from the usability testing.

6.3.2 **Prototype (iteration 2)**

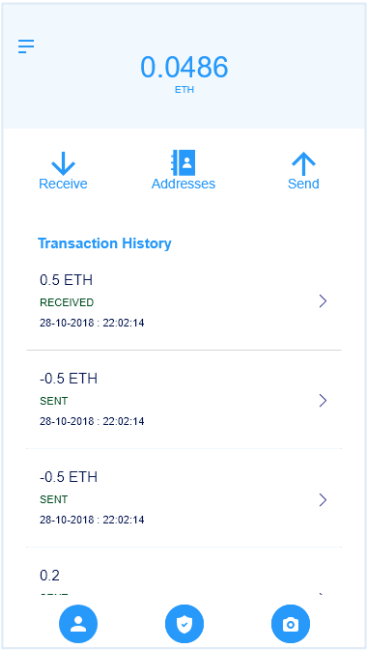


Figure 25. The camera tab icon to the right opens up the phone camera to scan an address

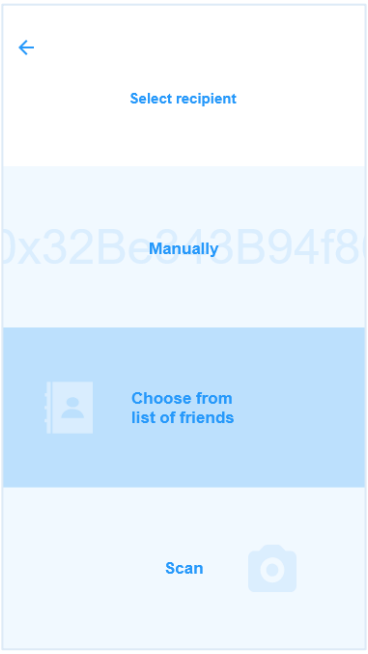


Figure 26. The user has to select one of the methods.

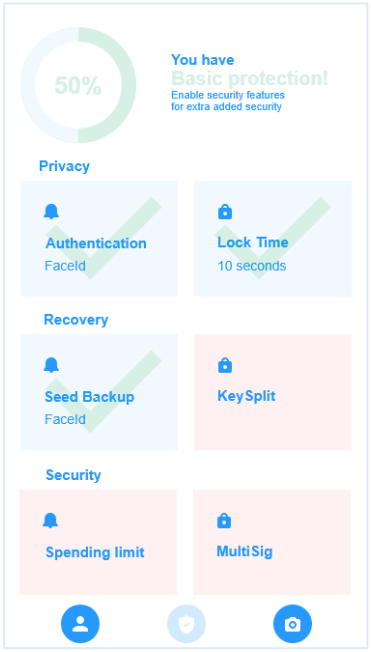


Figure 27. Red background marks which features are not enabled

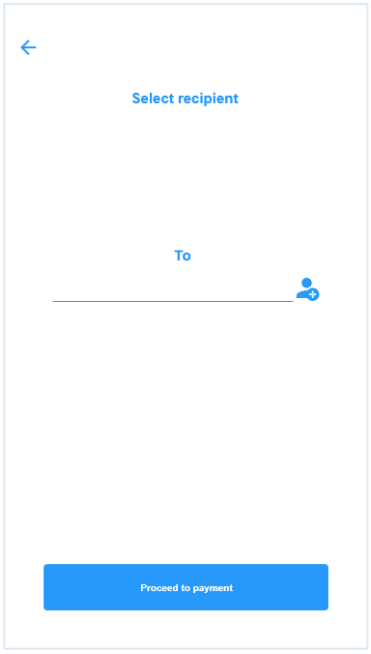


Figure 28. Option to choose from phonebook was removed

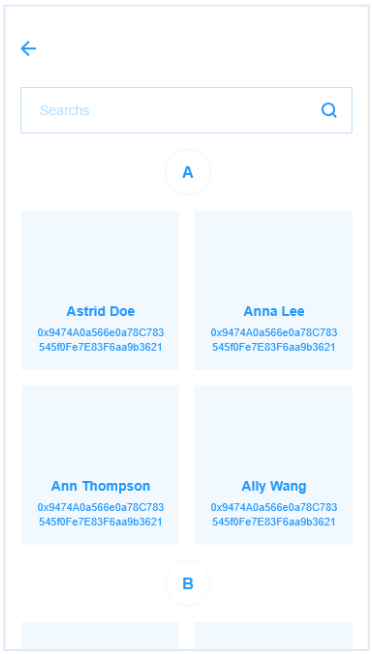


Figure 29

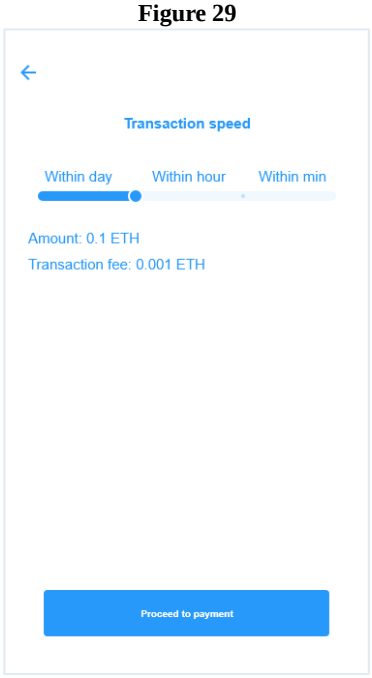


Figure 30. Transaction screen was divided into two screens (nr.1).

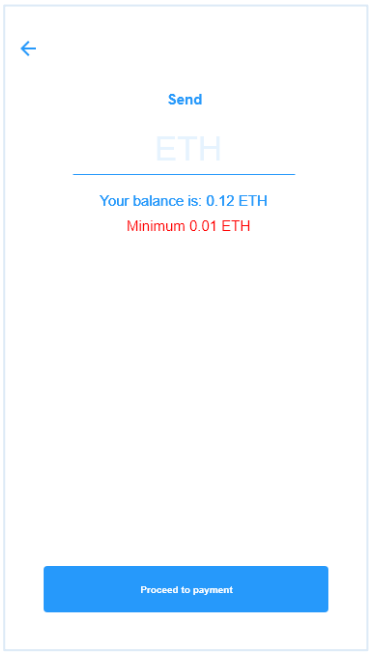


Figure 31. Transaction screen was divided into two screens (nr. 2)

7 Discussion

This chapter discusses the project results and what could have been done differently. It also assesses the decisions made and suggests future avenues that could be explored.

As explained in the introduction, blockchain is not a new technology in itself even though it is new as a combined concept. What's new about blockchain is how the underlying technologies are combined and used today, e.g. tokens and decentralized applications. As this combination is quite young, there is not a lot of research regarding UX and usability within the blockchain field. Also, understanding how blockchain and how the different implementations of blockchain work can seem complex to the average person. Hence, if one does not know the underlying reason behind a problem it can be difficult if not impossible to propose a potential solution. Thus, apart from proposing a user friendly and secure design that aims to solve the most common usability problems of today, this thesis can be used as basis for further research. This is possible as it not only defines existing problems but, also explains them to a degree that is needed for anyone trying to come up with solutions to these.

Furthermore, over the course of delivering this project, a number of different viewpoints have materialized leading to a number of questions and interesting findings. Some of these required a decision to be made while others put a new perspective on the project. These have been grouped accordingly to the project phases and are discussed below.

7.1 Data gathering discussion

Based on the results in section 4.2, randomly choosing participants at a technical convention is not a good method for finding existing users of today's blockchain applications. Instead, one should attend an event specifically related to blockchain such as a hackathon or a blockchain conference. At the convention it became clear that the majority of the user target group (of current solutions) are not familiar with the concept of blockchain technology nor the concept of blockchain tokens. The term cryptocurrency is a known term to the secondary user target group however, the technical knowledge behind it is shallow. The expected target group of users,

the “technologically savvy”, ended up not understanding even the simplest issues. This is surprising considering how much media focus there is on this topic, yet no one seems to understand it. This shows the hurdles that any wider blockchain application will have to tackle. It also leads to the conclusion that the secondary user target group definition is not adequate – not all “tech-savvy” people are current users of today’s wallet solutions.

To resolve this, a lot of time was spent on structuring a secondary research methodology that would result in detailed descriptions of common usability problems, an outcome expected from the user research. This methodology included a well-prepared stake-holder interview, an online research and a competitor analysis. On one hand, these steps might have taken less time and some elements of them might have been excluded if the user research (conversational interviews) would have led to a better outcome. On the other hand, in a situation where primary research approach turned out to not be possible, these steps confirmed the validity of the defined user problems.

The competitor analysis showed the same usability problems as obtained from the stakeholder interview as well as the online research. This in turn ensured that the defined usability problems are real. Unfortunately, this does not change the fact that a lot of time was lost preparing and conducting the conversational interviews.

When conducting the competitor analysis, it was also decided to exclude hardware components due to two reasons, lack of time and not having access to the most common hardware wallets for testing purposes. Instead, the author decided that, if time allowed at the end of the project (which at that point was already strained due to additional research done) more online research would have be done into comparing the different hardware-based solutions and how to integrate them with the proposed solution. In retrospect, there is also a third reason of not including the hardware solution; if the target users are currently oblivious to blockchain technology, introducing a further element would just confuse them even more.

7.2 Data analysis discussion

The creation of user personas turned out to be used far more than expected during the initial phases of this project. Solutions to the defined usability problems (requirements) were inspired by the created user personas. The structuring of the application (the card sorting method) was based on how each user persona would prioritize the predefined requirements. And finally, the created user personas served as inspiration when selecting participants for the usability testing. It is obvious that user personas are a very useful tool when the access to the user target group and time is limited. However, user personas should not be seen as a method to omit real users in a design phase. Even though user personas are based on research, they are still subjective descriptions of the target user group, especially if the users in the

research were scarce. The reader should not think that user personas are always enough to define user needs. In this project fortunately they were as they were confirmed by both the stakeholders and other experts within the field of blockchain applications, allowing the author to be confident in using the user personas to obtain user needs. Without this confirmation, the results would have been questionable. Would such confirmation not have taken place then; a lot more primary user research would have to be conducted.

There are two more reasons that could possibly explain why the created user personas were a success in this project. One being, the fact that the user persona descriptions were low on attributes and focused more on user problems and scenarios rather than the identity of a target user. The second reason is: since the application is aimed to be used by "anyone", perhaps defining specific attributes might harm the resulting design. It is possible that designing for a specific type or types of users would not lead to a widely adopted design. On the other hand, one can argue that there are advantages with defining user attributes as well as methods to do so for a wide user target group. However, to represent a wide target user group by defining user personas with specific identity attributes this, would require considerably more user personas and as a consequence more time. The user personas in this project should maybe instead be seen more as user personas in different scenarios than just descriptions of target users.

Another problem that arose due to the time limitation was realization that the number of features were to many. Upon the creation of the requirement specification it was decided to solve this problem by not taking all features into consideration. Defining the functionality of the implementations of multi-signature, Shamir's secret sharing, and the integration of the hardware component would require a lot of research as there are no guidelines or even examples of how this would be implemented in a mobile wallet. Thus, these were not included in the requirements specification. This however, would make for interesting future work, not only for the blockchain applications but also for any secure solutions using these security approaches.

7.3 Prototyping and evaluation phase

The Donald Norman's design principles turned out to be used less than planned. The reason being: one who has applied these principles many times does not design without them in mind. Hence, they were only used as a validation tool to validate that every principle had been taken into consideration.

A few examples are given to illustrate how Donald Norman's principles are incorporated within the design of prototype 1. Visibility is provided by allowing the

user to start all main tasks, e.g. starting a transaction, under one of the different tabs, see figure 12. To provide feedback, the user is always given some sort of feedback when taking an action, see figures 9, 10, 18. Constraints are used to notify the user that certain information needs to be provided prior to proceeding with an action, see figure 13. To provide a good mapping between buttons and the consequence of pressing them, commonly used buttons have been chosen for common purposes, see figure 20. Also, colours are used to show how one thing affects another, e.g. such as how the amount of enabled security features affect the overall wallet security, see figure 14. Tabs and sub-tabs have a similar design hence, providing overall consistency, see figure 12.

The usability test assessed four of the five quality components; learnability, efficiency, errors, satisfaction (see section 2.2.1.) Based on the results of the usability testing (see section 6.2) changes were made to the prototype. "Receive" and "Send" icons turned out to have a bad mapping with the consequence of pressing them (see section 6.2.1.) To make them more intuitive and make the design easier to learn (learnability), old icons were replaced with new icons that illustrate their oppositeness (as suggested by the participants), see figure 25.

As it turned out, there is room for improvements regarding the efficiency of the design, (see 6.2.2.) The second transaction screen holds too much information for the user to process, figure 15, hence split into two separate screens, see figures 30, 31. Also, when selecting a recipient for a transaction it is unclear whether the user has two options or two decisions to make. To clarify that these are options, the user is constrained by being forced to choose one option first and then select the recipient address in the improved version of the prototype, see figure 26, hence also eliminating the error found in section 6.2.3. As suggested by the test participants, a scan option should be provided by the application to limit the error of writing down someone's address wrong. This was a feature that was initially planned to be included in the design but got somehow lost during the prototyping. The feature was not planned to be a main feature but test participants argued that it would be a frequently used feature if it would exist hence, it was included as a main one, (see figure 24 and figure 25).

Participants were overall satisfied with the design but were not incentivized to enable different security features. According to the participants they would be more incentivized to enable features if the non-enabled ones were annoyingly obvious. As suggested, the non-enabled features were made more obvious by the use of the colour red (an alarming colour), (see figure 27). Additionally, the usability test led to the realization that some basic features were missing, e.g. possibility to delete a contact, not being able to re-set a requested amount and that the request amount icon does not say anything about the consequence of pressing it. These findings are left to improve for future improvements.

Only a few of the quality requirements were assessed during the usability testing, see section 5.3.2. Requirement RQ1. RQ2 would require a second round of usability

testing to be assessed. RQ3 was fulfilled and tested by the author herself as this is not a requirement that needs a target user. RQ4 is a requirement for future implementation as this feature is not possible to implement in XD. RQ5 and RQ7 are fulfilled as no test-participants were asking about any terms during the use of the application. RQ6 is fulfilled and assessed by the author. As seen in 6.2.1., 6/7 users understand the concept of the seed, confirming RQ8. RQ9 is validated by the answers of task 4 in 6.2.6. Only the main features of the application were tested which means that these conclusions might not be correct. For instance, the terms multisig and seedsplit (an implementation of Shamir's secret sharing) are technical terms that might not be understandable, which could affect the assessment of RQ5 and RQ7. As these features were not tested, the quality requirements assessment is not certain from a quality perspective. When it comes to usability, the quality requirements development was not done as thoroughly as the development of the research questions. Thus, the results from the research questions are more reliable to look at when assessing usability. Based on the results from the usability tests (see 5.3), one can see that the suggested changes did not affect the overall structure of the application and nor the different features (see 6.3.1). As the changes were minor, it seems as if the four usability quality components would be highly scored assuming that the implemented changes in fact solve the issues. Therefore, it is not unrealistic to assume that the final prototype is easy to use from a usability perspective. However, to be certain, a second round of usability tests are needed to confirm this statement.

The usability tests were conducted in environments participants were comfortable in, such as at home, school or at work, to simulate a natural situation. The information given out presented the user with different scenarios to make the testing feel more natural to the participant. However, a testing situation and environment is always artificial. Also, test participants are rarely perfect representants for all users. Even the most rigorous usability test cannot result in a 100% accurate verdict. Therefore, to obtain as truthful results as possible, ideally, several iterations of usability testing would have been performed with new groups of users.

With more time, a second iteration of usability testing would have been possible with the aim to validate the design changes for the improved prototype.

As there was no second round of usability tests, it was also not possible to assess the memorability. If time would not have been restricted, the second round of usability testing would have included two groups; one with the same participants as in the first round to assess memorability and a second new group to compare the results between both iterations to tackle the carryover effect, (see section 2.2.6.2)

Furthermore, none of the suggested approaches for tackling the carryover effect were used in this project as only a few parts of the application, the main features, were tested. These parts were not connected to each other and they all had different designs thus, preventing the tester to approach different tasks in the same way.

However, to fully ensure that no learning had taken place, an Independent Groups Design approach could have been used. That would however, require a lot of test participants and more time which was not available. The Within Subjects Design approach could also have been used but would require a comprehensive planning which again was not possible due to the time constrains. Instead the approach of optimizing a usability test was used (the Nielsen Norman Group) which suggests only involving five participants. To ensure that five were present, seven participants were invited. Fortunately, none decided to cancel which resulted in seven tests instead of five.

7.4 User centred approach and its difficulties

The first thought that comes to mind when assessing whether the outcomes of the entire project are realistic or not is the fact that there was only one person conducting all the steps in this project. Based on common sense, the person that assesses and draws conclusions about his or her own work might unconsciously lose objectivity. With this in mind, a lot of time was spent on reading and understanding different biases and how to avoid these prior to entering any of the project phases. One would therefore expect that these have been eliminated to some extent although, one can never be sure.

A question that also arises is whether a blockchain application design process, one that focuses on User Experience and usability, differs from the typical standards of how a design process should be performed. Something that might differentiate any blockchain application project from others is the complex technical knowledge that it required today. The complexity is not because blockchain technology itself is difficult to understand, it's rather the lack of pedagogical information that makes blockchain technology difficult to grasp. This does affect how application is delivered as the normal expectations do not apply. For normal apps users have an idea about what is happening, in blockchain apps new users have really no knowledge of what is happening. It is almost as trying to explain how a modern smartphone works to someone that has only ever seen an old school mobile phone.

The above-mentioned difficulty was also the reason why the development method used was an amalgamation of a number of different approaches to design (as defined in section 2.2.3). The lack of knowledge and understanding of even the most basic concepts of blockchain and cryptocurrencies amongst the target users, created some unexpected difficulties in the form of not being able to get the expected user input. What was supposed to be an iterative user centred design process ended up being somewhat in between an iterative and a waterfall approach. It can be argued that a more traditionally iterative design process, as the one defined by ISO, would lead to more reliable outcomes. Unfortunately, this would require a lot more time, which

was not available. This “learning by doing” approach in this project allowed to complete the project and its goal on time.

Here, a question that arises is whether it is a good idea to focus on users who are not familiar with the concept of blockchain and its implementations. It might seem overkill to create a system for people who are not aware of the technology or not interested in using it. In this project this was solved by designing for a non-technical user who, for some reason wishes to learn more about blockchain or simply needs to set-up a wallet for some reason, a so-called early adopter.

7.5 The end result

The resulting design is based on the different methods used to produce a usable (sometimes referred to as user-friendly) product. However, it would be ill-advised to say that the interface could not have been designed differently. In the end, the design choices made were subjective and based on the author’s own interpretations of different design approaches and principles. This does not necessarily mean that it is a bad thing. A User Experience designer is allowed to make assumptions and interpretations as long as he or she is open to the possibility that these might be wrong which, as in this project, is assessed by the usability testing.

Towards the end of the project, the proposed application was compared to the previously investigated wallets {mostly Ethereum). Interestingly the proposal differs quite a lot compared to other analysed competitor applications. The main differences are:

- The information is structured in a way that is intuitive to the user and based on how frequently certain features are to be used. More frequent features are given more visibility. The choice of limiting the number of tabs to three limits the amount of choices that can be made hence, providing a better learnability and memorability.
- The terms used in the application are non-technical. The few terms and concepts that might be new to the user, such as “seed”, are explained in a non-technical manner.
- Users are provided with information regarding how secure their wallet is and what steps they can take to secure it even further.
- The proposed design will be compatible with the most common hardware components of today, a feature that does not yet exist in current solutions.
- If the application is to be successful amongst its competitors, it needs to provide fundamental functionality that some competitors offer such as friend’s list, scan address feature, request amount feature but also new features such as order hardware component within the application and

new security features such as multisig and a implementation of Shamir's secret sharing algorithm.

Just because these the competitor wallets are the most used ones does not mean that they are the most usable ones available. It seems that these were designed by and for blockchain experts without taking into account normal users – something that is confirmed when reading more about them. For future research it would therefore be interesting to investigate less mentioned wallets and perhaps even wallets that are not related to Ethereum.

The process of buying tokens is known to be a complicated process. To improve the overall user experience of storing tokens, the buying process needs to be improved as well. The buying process directly affects the user experience and whether a wallet will or will not be used. If the buying process is too complicated and the user decides not to buy, no wallet will be installed or even searched for as it won't be needed. Improving the buying process could be entirely solved by providing the option of in app-purchases of ether. Improving the buying process is beyond this project's scope. However, should be considered as a future goal and perhaps a feature.

Also, if a wallet is to be integrated with different hardware components, this in turn will cause a chain reaction problem not considered in this project such as; how does one backup a hardware component?

It is safe to say that this project only touched on one aspect of UX in blockchain applications. There is a lot more to blockchain than just wallets, all the other aspects (i.e.: node software, validation software, chain storage, etc) are just as important but are not discussed in this dissertation. Any future work will also have to focus on those.

8 Conclusions

This chapter summarizes what has been done in this project, the project outcomes, what could have been done differently and future suggestions

The purpose of this dissertation was to examine UX in blockchain environment, more specifically in Ethereum wallets, and to propose a blockchain wallet design that would help onboard users without any prior blockchain exposure. The project itself was done in collaboration with Cisco Systems who acted as the client and requested a design for their own internal needs. During the project a special focus was put safety and security of the wallet meaning ensuring that data access would not get lost easily. The exact project deliverables were:

- The project was expected to deliver a clickable prototype of the mobile application and a written concept that includes specifications of the hardware component
- The suggested system should protect users from common security and usability problems that are present in today's existing solutions.

8.1 Delivery Process

The project was delivered through a three-phase approach (Data gathering, Data Interpretation, Prototyping and Evaluation). Data gathering included blockchain and cryptocurrency research, user and stakeholder research, competitor research and usability testing. The Data Interpretation analysed these from a user perspective while the Prototyping and Evaluation delivered the design. During the course of the project a number of recognized design methods and principles were used to develop the end product, these were:

- Human-centred design for interactive system defined by the ISO standard 9241-210 (210)
- Stakeholder interview
- User interviews
- Competitor analysis
- User personas
- Conceptual design
- Requirements specification

- Card sorting
- Donald Norman's seven design principles
- Prototyping
- Usability testing (Nielsen Norman Group)

The project approach itself has changed over the execution as new information and lack of it became apparent. As a result, a lot more time has been spent on user research and competitor research and less on usability testing. Had time allowed, there would have been a second iteration of usability testing to validate the changes made to the first prototype and, more research done on hardware components.

8.2 The results

The project delivered a wallet design that addresses majority of the challenges faced by new users as well issues with the existing wallets. The background research has also identified some of the most common usability problems of today, the main ones being:

- Users are not being helped with keeping their wallets safe
- Alternative key storage methods are too complicated
- Serious mistakes are easily made (entering the wrong address when making transaction)
- Users are expected to understand the concept of secure private key management
- Consistency and learnability (different terms are used to describe the same concept)
- Slow and tiering transactions without any explanations (what is a transaction fee? how will the user know the consequence of deciding the amount?)

Furthermore, the proposed design also fulfils the client requirements based on the project goals and seems to be superior to the compared alternative wallets. More specifically, when compared to the most widely used Ethereum wallets, the proposed application:

- is more intuitive,
- does not require technical knowledge in order to be used,
- is informative especially concerning access means security,
- considers compatibility with hardware components and,
- is more comprehensive in terms of the amount of features it offers.

8.3 Future work

Although complete in itself, the project also opens the doors to more work. Specifically, further work should be done on defining how to integrate the existing design with hardware wallets, both from a technical and UX perspective witch also raises the question of wallet access and storage when hardware solution is added. It would also be interesting to compare less known wallets to see whether they solve the different usability issues differently and perhaps even wallets that are not strictly Ethereum based.

From a wider perspective, more UX research will also be required into the other elements of blockchain; verification, node management, chain storage to a name a few.

It seems that when it comes to UX in blockchain, the vast majority of work is still in front of us.

References

[1] I. Lesuisse, "Argent — Secure, Simple and Seedless," Medium, 04 09 2018. [Online]. Available: https://medium.com/argenthq/decentralised-and-seedless-wallet-recovery-5fcf7dddd78d. [Accessed 07 02 2019].

[2] CRYPTOSEC, "5 Common Ways On How People Lose Their Bitcoin/Crypto," 30 10 2018. [Online]. Available: https://cryptosec.info/ways-people-lose-their-crypto/. [Accessed 07 02 2019].

[3] N. Bauerle, "What is Blockchain Technology?," Coindesk, [Online]. Available: https://www.coindesk.com/information/what-is-blockchain-technology. [Accessed 31 01 2019].

[4] IBM, "What is blockchain?," [Online]. Available: https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=45015045USEN&. [Accessed 31 01 2019].

[5] M. Lucas, "Blockchain: The complete guide," Computerworld, 29 01 2019. [Online]. Available: https://www.computerworld.com/article/3191077/security/blockchain-the-complete-guide.html. [Accessed 31 01 2019].

[6] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," Bitcoin, 03 2009. [Online]. Available: https://bitcoin.org/bitcoin.pdf. [Accessed 31 01 2019].

[7] A. Kharpal, "CNBC," 18 06 2018. [Online]. Available: https://www.cnbc.com/2018/06/18/blockchain-what-is-it-and-how-does-it-work.html. [Accessed 31 01 2019].

[8] Ethereum, "The coin," [Online]. Available: https://www.ethereum.org/token. [Accessed 31 01 2019].

[9] Ethereum, "Ethereum White Paper," 27 01 2019. [Online]. Available: https://github.com/ethereum/wiki/wiki/White-Paper. [Accessed 2019 01 31].

[10] H. Kenneth, "Ethereum account," Medium, 05 07 2018. [Online]. Available: https://medium.com/coinmonks/ethereum-account-212feb9c4154. [Accessed 31 01 2019].

[11] "Accounts, Addresses, Public And Private Keys, And Tokens," The Ethereum Wiki, 27 04 2017. [Online]. Available:

https://theethereum.wiki/w/index.php/Accounts,_Addresses,_Public_And_Private_Keys,_And_Tokens. [Accessed 31 01 2019].

[12] P. Ryszkiewicz, "Secure Cryptocurrency Seeds," Medium, 03 23 2018. [Online]. Available: https://medium.com/@peterryszkiewicz/secure-cryptocurrency-seeds-fdd99f39df7e. [Accessed 31 01 2019].

[13] COTI, "The difference between hot and cold wallets in the digital currency world," Medium, 11 01 2018. [Online]. Available: https://medium.com/cotinetwork/the-difference-between-hot-and-cold-wallets-in-the-digital-currency-world-1aa6f957ddd1. [Accessed 31 01 2019].

[14] S. Khatwani, "Best Multi-Signature Bitcoin Wallets [2019 Edition]," Coinsutra, 11 06 2018. [Online]. Available: https://coinsutra.com/best-multi-signature-bitcoin-wallets/. [Accessed 31 01 2019].

[15] B. Davenport, "What is Multi-Sig, and What Can It Do?," Coincenter, 01 01 2015. [Online]. Available: https://coincenter.org/entry/what-is-multi-sig-and-what-can-it-do. [Accessed 29 01 2019].

[16] D. Stinson, "An Explication of Secret Sharing Schemes," *Designs, Codes and Cryptography*, no. 2, pp. 357-361, 03 25 1992.

[17] O. Birch, "Secure Multiparty Computation and Shamir's Secret Sharing on Wanchain," Medium, 19 07 2018. [Online]. Available: https://medium.com/wanchain-foundation/secure-multiparty-computation-and-shamirs-secret-sharing-on-wanchain-e502012b80ef. [Accessed 31 01 2019].

[18] Chicago Architecture Foundation (CAF), "DiscoverDesign Handbook," [Online]. Available: https://discoverdesign.org/handbook. [Accessed 18 02 2019].

[19] ISO/TC 159/SC 4 Ergonomics of human-system, "Part 210: Human-centred design for interactive systems," ISO 9241-210:2010. [Online]. Available: https://www.iso.org/standard/52075.html. [Accessed 08 11 2018].

[20] J. Nielsen, "Usability 101: Introduction to Usability," 04 01 2012. [Online]. Available: https://www.nngroup.com/articles/usability-101-introduction-to-usability/. [Accessed 09 11 2018].

[21] H. S. J. P. Yvonne Rogers, Interaction design: Beyond human-computer interaction (3rd edition), John Wiley & Sons, 2011.

[22] S. Baty, "User Research for Personas and Other Audience Models," Ux matters, 27 04 2009. [Online]. Available:

https://www.uxmatters.com/mt/archives/2009/04/user-research-for-personas-and-other-audience-models.php. [Accessed 12 02 2019].

[23] S. Farrell, "nngroup," Nielsen Norman Group, 22 05 2016. [Online]. Available: https://www.nngroup.com/articles/open-ended-questions/. [Accessed 19 02 2019].

[24] Talebook, "How to understand your clients? Guide to Stakeholder Interview.," UX Planet, 30 04 2018. [Online]. Available: https://uxplanet.org/talebook-method-001-stakeholder-interview-63eebe4ca12a. [Accessed 10 11 2018].

[25] J. Mason, "Semistructured Interview," in *The SAGE Encyclopedia of Social Science Research Methods*, Thousand Oaks, SAGE Publications, Inc., 2004, p. 1020.

[26] S. Douglas, "How to do a UX competitor analysis: A step by step guide," Usabilitygeek, 25 09 2017. [Online]. Available: https://usabilitygeek.com/how-to-do-ux-competitor-analysis/. [Accessed 20 02 2019].

[27] A. Harley, "Nielsen Norman Group," 16 02 2015. [Online]. Available: https://www.nngroup.com/articles/persona/. [Accessed 13 11 2018].

[28] "Conceptual Design, Great Products Begin with Great Design," ATA Engineering Inc, [Online]. Available: http://www.ata-e.com/services/design/conceptual-design/. [Accessed 19 02 2019].

[29] S. Lauesen, "Introduction and basic concepts," in *Software requirements - Styles and techniques*, Addison-Wesley Professional, 2002, pp. 1-13.

[30] U.S. Dept. of Health and Human Services. The Research-Based Web Design & Usability Guidelines, Enlarged/Expanded edition. Washington: U.S. Government Printing Office, 2006. [Online]. Available: https://www.usability.gov/what-and-why/information-architecture.html. [Accessed 06 02 2019].

[31] E. Ibragimova, "High-fidelity prototyping: What, When, Why and How?," Medium, 28 12 2016. [Online]. Available: https://blog.prototypr.io/high-fidelity-prototyping-what-when-why-and-how-f5bbde6a7fd4. [Accessed 12 02 2019].

[32] J. Nielsen, "Why You Only Need to Test with 5 Users," NN/g Nielsen Norman Group, 19 03 2000. [Online]. Available: https://www.nngroup.com/articles/why-you-only-need-to-test-with-5-users/. [Accessed 17 02 2019].

[33] D. Norman, "The psychopathology of everyday things," in *The design of everyday things*, New York, Basic Books, 2013, pp. 1-36.

[34] E. G. W. Christopher J. Pannucci, "Identifying and Avoiding Bias in Research," *Plastic and Reconstructive Surgery*, vol. 126, no. 2, pp. 619-625, 2010.

[35] R. Sarniak, "9 types of research bias and how to avoid them," Quirks, 08 2015. [Online]. Available: https://www.quirks.com/articles/9-types-of-research-bias-and-how-to-avoid-them. [Accessed 10 02 2019].

[36] S. Moss, "Acquiescence bias," 2008.

[37] D. Watson, "Correcting for Acquiescent Response Bias in the Absence of a Balanced Scale: An Application to Class Consciousness," *Sociological Methods & Research*, vol. 21, no. 1, p. 52–88, 1992.

[38] D. Dodou and J. C. F. de Winter, "Social desirability is the same in offline, online and paper surveys: A meta-analysis," *Computers in Human Behavior*, pp. 36, 487–495, 2014.

[39] O. Kaminska and T. Foulsham, "Understanding Sources of Social Desirability Bias in Different Modes: Evidence from Eye-tracking," Institute for Social & Economic Research, University of Essex, Essex, 2013.

[40] N. Vaney, A. Dixit, T. Ghosh, R. Gupta and M. Bhatia, "Habituation of event related potentials: a tool for assessment of cognition in headache patients," *Delhi Psychiatry Journal*, vol. 11, no. No. 1, pp. 48-51, 2008.

[41] N. B. Turk-Browne, B. J. Scholl and M. M. Chun, "Babies and brains: habituation in infant cognition and functional neuroimaging," *Frontiers in Human Neuroscience*, vol. 2, p. Article 16, 2008.

[42] N. Malhotra, J. Hall, M. Shaw and P. Oppenheim, "Essentials or Marketing Research, An Applied Orientation," Pearson Australia, 2007, p. 227.

[43] Readex Research, [Online]. Available: http://www.readexresearch.com/understanding-survey-data/. [Accessed 04 11 2018].

[44] R. S. Nickerson, "Confirmation Bias: A Ubiquitous Phenomenon in Many Guises," *Review of General Psychology*, vol. 2, no. 2, pp. 175-220, 1998.

[45] J. P. Lavrakas, "Question Order Effects," in *Encyclopedia of survey research methods*, Thousand Oaks, CA, Sage Publications, 2008, p. 664.

[46] J. H. M. S. P. O. Naresh Malhotra, "Essentials or Marketing Research, An Applied Orientation," Pearson Australia, p. 227.

[47] U.S. Dept. of Health and Human Services. The Research-Based Web Design & Usability Guidelines, Enlarged/Expanded edition. Washington: U.S. Government Printing Office, 2006. [Online]. Available: https://www.usability.gov/how-to-and-tools/methods/card-sorting.html. [Accessed 06 02 2019].

[48] Y. Keshtcher, "The 4 UX Problems When Designing Blockchain-Based Smart Contracts," Medium, 17 08 2018. [Online]. Available: https://blog.prototypr.io/the-4-ux-problems-when-designing-blockchain-based-smart-contract-d37ee4c8c64b. [Accessed 07 02 2019].

[49] O. Faridi, "$170,000: Bitcoin Investor Fails to Backup Wallet, Loses Access to Funds," Cryptoglobe, 09 12 2018. [Online]. Available: https://www.cryptoglobe.com/latest/2018/12/170-000-bitcoin-investor-fails-to-backup-recovery-password-loses-access-to-funds-bitcoin-wallet/. [Accessed 07 02 2019].

[50] Sudhir Khatwani, "Security Risks of Mobile, Web & Desktop Bitcoin Wallets [Must Know]," Coinsutra, 13 10 2018. [Online]. Available: https://coinsutra.com/security-risks-bitcoin-wallets/. [Accessed 07 02 201].

[51] B. Vishnubhotla, "How to get widespread adoption: Improve the notoriously bad UI/UX in crypto-investing," Hackernoon, 22 05 2018. [Online]. Available: https://hackernoon.com/improving-the-notoriously-bad-ui-ux-in-crypto-investing-7acb73285a50. [Accessed 07 02 2019].

[52] faast, "WHY is Cryptocurrency SO Complicated?," Medium, 10 25 2018. [Online]. Available: https://medium.com/faast/why-is-cryptocurrency-so-complicated-5cfd9aadf598. [Accessed 07 02 2019].

[53] E. A. Tartakovsky, "Ten Hacker-Proof Steps to Secure Your Crypto Assets," Hackernoon, 21 01 2018. [Online]. Available: https://hackernoon.com/ten-hacker-proof-steps-to-secure-your-crypto-assets-b564fe938e8. [Accessed 07 02 2019].

[54] "What is blockchain," IBM, [Online]. Available: https://www.ibm.com/blockchain/what-is-blockchain. [Accessed 31 01 2019].

[55] "Examples of Open-Ended and Closed-Ended Questions.," YourDictionary, [Online]. Available: http://examples.yourdictionary.com/examples-of-open-ended-and-closed-ended-questions.html. [Accessed 19 02 2019].

Appendix A

This appendix contains all the pages that were taken into account when analysing the solutions of competitors.

A.1 Questions

Wallet	Number of times mentioned
Guarda 2 (mobile)	2
imToken Wallet (mobile)	1
ACGN Ethereum Wallet (mobile)	1
Atomic Wallet (mobile)	1
Coinpayments (mobile)	1
TrustWallet (mobile)	2
BRD/Breadwallet (mobile)	2
Parity	1
Ledger Nano S 10	12
Trezor	10
KeepKey	6
Geth	1
Exodus	11
Mist	8
MetaMask	8
Jaxx (mobile)	11
Coinomi (mobile)	1

MyEtherWallet	12
Coinbase (mobile)	7
ETHAdress	7

https://captainaltcoin.com/top-ethereum-wallets/

https://coinsutra.com/best-etherum-wallets/

https://coinswitch.co/news/top-12-best-ethereum-wallets-2018

https://medium.com/@ACGN_Official/top-10-best-ethereum-wallets-2018-edition-best-ethereum-wallets-to-secure-your-cryptocurrency-5688f3a3f9a7

https://theindependentrepublic.com/2018/08/10/top-5-ethereum-wallets/

https://ripplecoinnews.com/best-ethereum-wallets

https://cryptocurrencynews.com/best-ethereum-wallets/

https://www.buyersguidex.com/best-ethereum-wallets/

https://steemit.com/altcoin/@cryptosdecoded/the-10-best-ethereum-wallets-for-2018

https://www.buybitcoinworldwide.com/ethereum/wallets/

https://99bitcoins.com/ethereum-wallets/

https://www.bitpremier.com/ethereum/wallets

Appendix B Test-plan

This Appendix contains additional data created during the usability test phase

Purpose

To evaluate the structure of the proposed design and the overall user experience

Research questions

Questions to be answered after each usability test

Learnability

Can a user make a transaction without any guided help?

Is it easy to find the account address?

Does the user understand the concept of seed after using the application once?

Efficiency

How quickly can a user set up his own account?

How long does it take to make a transaction?

Errors

Does the application prevent the user from making errors?

What kind of errors are easily made?

Satisfaction

How does the user feel about the onboarding process?

Is the onboarding process too long?

Does the security page appeal to the user?

Does the security page motivate the user to continue securing the account?

Data to be collected

5. *Objective/quantitative data*
    - Task success
    - Task time
    - Errors
    - Whether TL needed to intervene
6. *Objective/qualitative*
    - Description of faults
    - Cues given by researcher
    - Expressions made by the participant
7. *Subjective/quantitative*
    - Questions with a grading of 1-5
8. *Subjective/qualitative*
    - Open questions

Scenarios, tasks and questions (verbal questions are marked cursive)

Scenario: You are buying a jacket online when you notice the option of paying in ether. You are in a hurry because it is the last one available in your size and you decide to pay with your credit card as you usually do. However, the option of paying with ether intrigued you and you decide to do a little research. Turns out, ether is a currency that can be used as any other currency when shopping online. You decide that you want to try it out next time you shop online and so, you exchange some SEK for some ether.

Task 1. Onboarding

You have recently bought ether on an exchange and wish to transfer your assets to a private account. You've decided to download application X and wish to create an account **without** a hardware component. Create the account.

How intuitive was the onboarding process?

Not at all		Fairly		Very much so
1	2	3	4	5

Question 1: In the onboarding process the concept of seed was presented to you, can you tell me what you remember about it?

Follow-up question: What would happen if you would lose your seed?

Task 2. Find account address

In order to transfer your assets to your new account you need to send your assets to your account address. Find the address of your new account.

Was it easy to locate your account address?

Not at all		Fairly		Very much so
1	2	3	4	5

Question 2: Was the location of your account address where you expected it to be?

Follow-up question: Where did you expect it to be?

Task 3. Make transaction

You've now had your account for a couple of days and you've also managed to transfer your ether to your new account which now holds all your ether. You owe your friend some money and wish to send 0.1 ether to your friend's address, 0x9474A0a566e0a78C783545f0Fe7E83F6aa9b3621. Make the transaction to your friend

How was your understanding of the different steps when making the transaction?

Low		Neither low or high		High
1	2	3	4	5

Question 3 Let's look at the different steps again, tell me what you think was clear and unclear

Follow-up question: How would you like it to be?

Task 4. Security

Lately you've heard a lot about people losing their assets because of poor wallet security. You decide to investigate what you can do to secure your wallet. Determine how safe the account is and what steps can be taken to pursue further securing of the account

Was it obvious to you which steps have been taken so far and which have not?

Not at all		Fairly		Very much so
1	2	3	4	5

Question 4: Express your opinion regarding this page (security page)

Follow-up question: What do you think is good/bad? Do you have any questions that arise when looking at it? What do you expect there to be when pressing one of the features?

Methodology

Test participants will be given a short verbal introduction of the project. Different tasks will be handed out together with questions and verbal questions will be asked after each task. Verbal responses will be noted before each new task is started. Same type of task answers were grouped under the same headings thus, creating quantitative results (see data presentation). Based on the results, research questions will be answered.

Selection of participants

Participants are selected based on user personas and have some form of relationship with the author.

The role of the test-leader

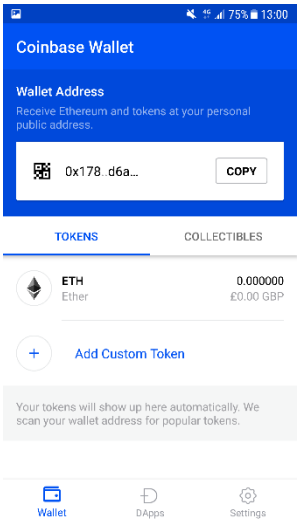
The test leader is the author of this thesis and is fully in charge of the usability testing. The test leader takes notes and asks the questions, guides the participant whenever needed.

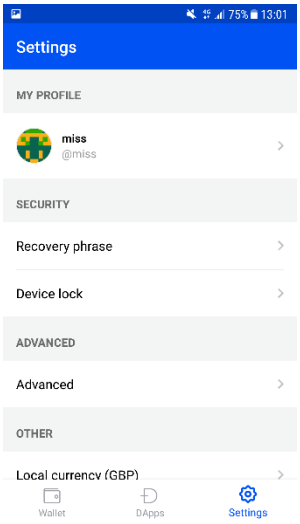
Data presentation

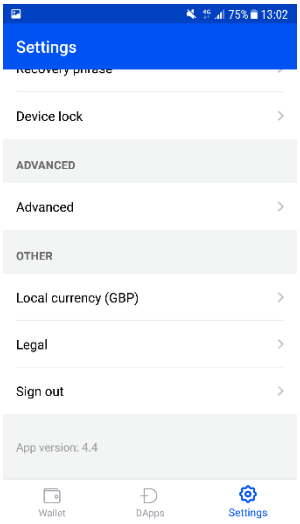
All data will be documented and presented and structured accordingly with the research questions. In the occasion of multiple equal responses, equal responses will be summed and presented once, together with the number of participants that stated the same response.

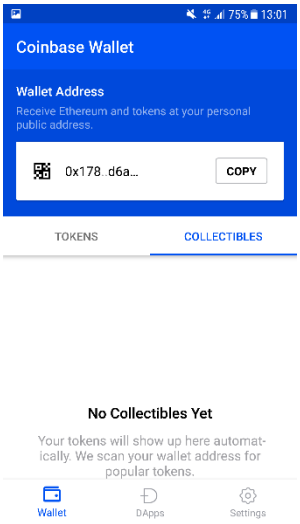
Appendix C

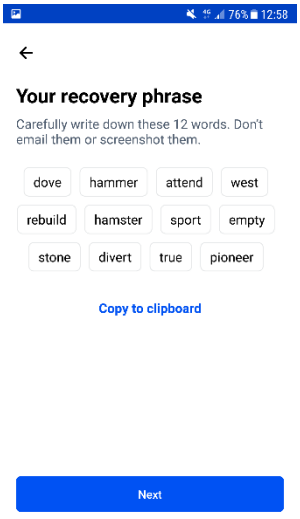
C.1 Coinbase Wallet – Ethereum Wallet & DApp Browser (formerly Toshi)

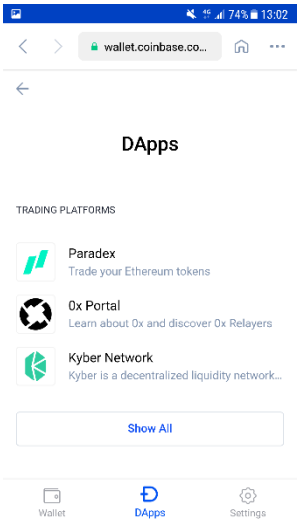




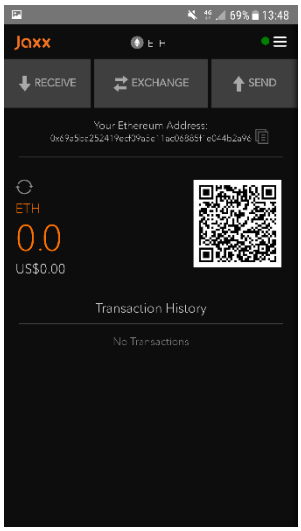


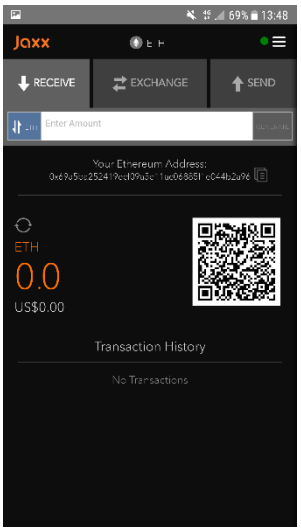


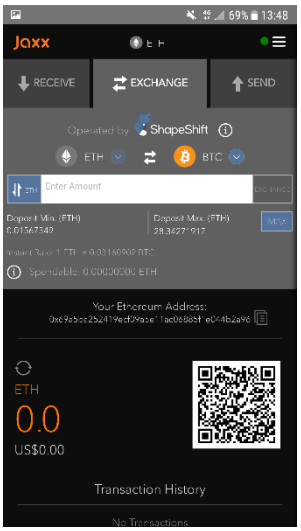


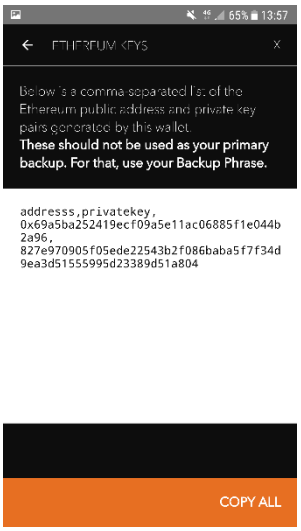


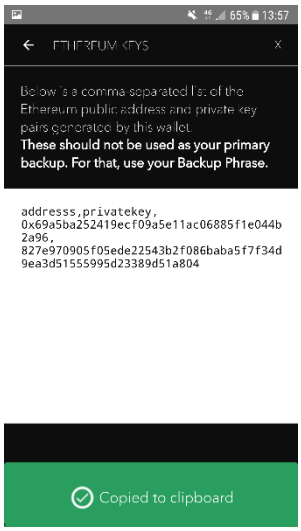
C.2 Jaxx Blockchain Wallet



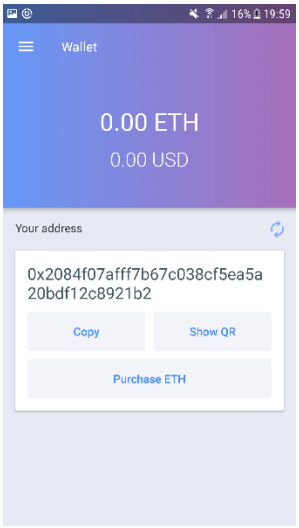


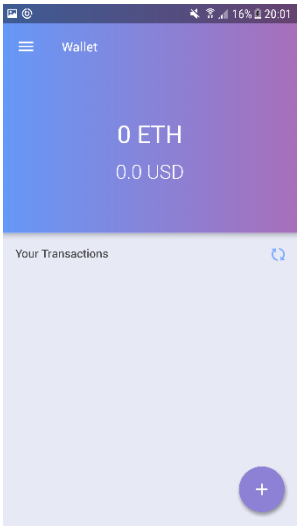


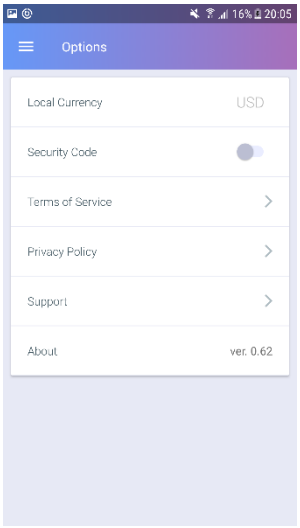


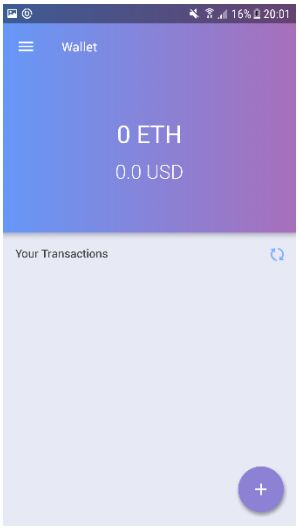


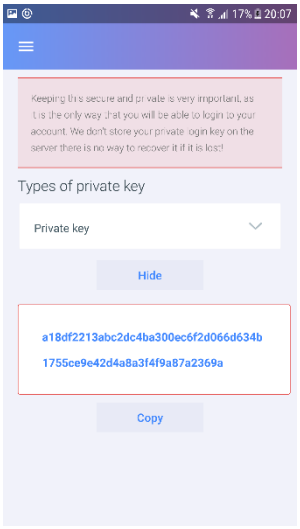
C.3 Guarda Wallet

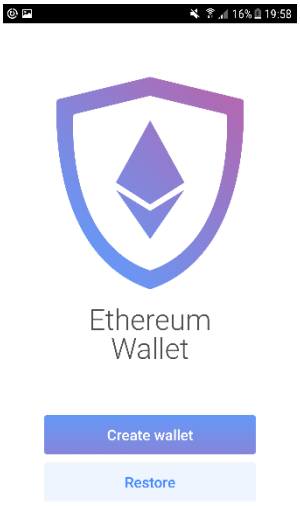




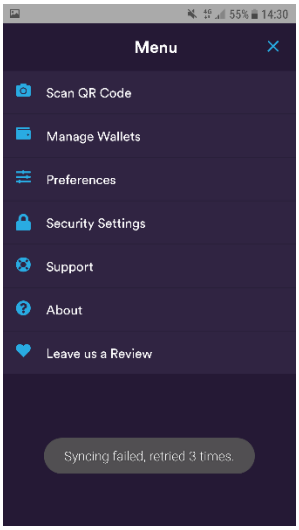


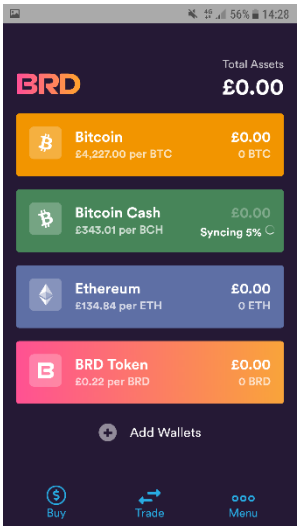


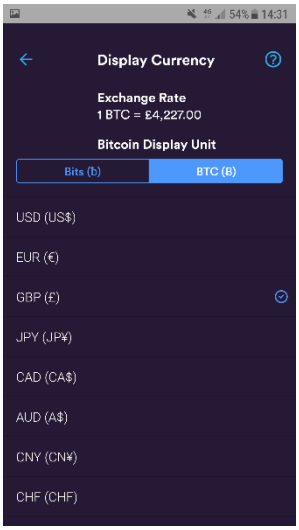


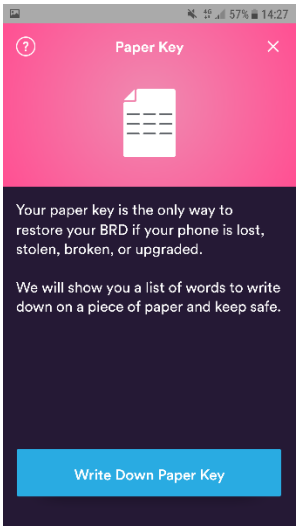


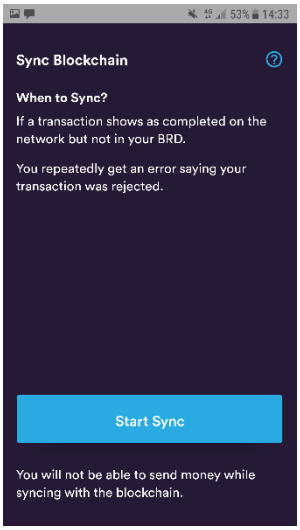
C.4 BRD –bitcoin wallet

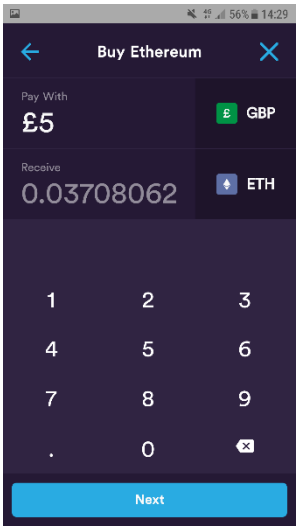












C.5 Trust – Ethereum & ERC20 Wallet