University of Zurich^UZH

Improving Usability for Non-Technical Users of Decentralised Applications

Yujue Chen
Zurich, Switzerland
Student ID: 21-737-689

Supervisor: Daria Schumm, Katharina Müller, Prof. Dr. Burkhard Stiller
Date of Submission: September 15, 2025

MASTER THESIS – Communication Systems Group, Prof. Dr. Burkhard Stiller

University of Zurich
Department of Informatics (IFI)
Binzmühlestrasse 14, CH-8050 Zürich, Switzerland

ifi

Master Thesis
Communication Systems Group (CSG)
Department of Informatics (IFI)
University of Zurich
Binzmuehlestrasse 14, CH-8050 Zurich, Switzerland
URL: http://www.csg.uzh.ch/

Declaration of Independence

I hereby declare that I have composed this work independently and without the use of any aids other than those declared (including generative AI such as ChatGPT). I am aware that I take full responsibility for the scientific character of the submitted text myself, even if AI aids were used and declared (after written confirmation by the supervising professor). All passages taken verbatim or in sense from published or unpublished writings are identified as such. The work has not yet been submitted in the same or similar form or in excerpts as part of another examination.

The declared tools used in this thesis is:

1. Grammarly: used for grammar checking and expression improvement.
2. GPT-5 mini: used for translation and text polishing, including prompts to improve sentence logic and clarity. All outputs were reviewed and edited by the author.

Zürich, 15.09.2025

Signature of student

Abstract

In den letzten Jahren basierte die Authentifizierung von Internetidentitäten hauptsächlich auf grossen Identitätsanbietern. Allerdings kann diese zentrale Verwaltung von Benutzerdaten zu Datenschutzrisiken führen. Self-Sovereign Identity (SSI) bietet einen benutzerzentrierten, dezentralen Ansatz, bei dem die vollständige Kontrolle über die Daten an die Nutzer übergeht. Ihre Usability und Nutzererfahrung werden jedoch nur selten berücksichtigt. Diese Studie zielt darauf ab, die Usability von SSI für nicht-technische Nutzer zu verbessern, und kombiniert dazu Literaturrecherche, Prototypenentwicklung sowie zwei Runden von Benutzertests und Interviews. Wichtige Usability-Herausforderungen wurden identifiziert, und die Auswirkungen spezifischer Schnittstellenmerkmale auf die Nutzererfahrung analysiert. Basierend auf den Ergebnissen werden umsetzbare Designempfehlungen vorgeschlagen, die praktische Orientierung für die Entwicklung von SSI-Anwendungen bieten.

In recent years, Internet identity authentication has mainly relied on large identity providers. However, this centralised management of user data may lead to privacy risks. Self-Sovereign Identity (SSI) offers a user-centred, decentralised approach, handing over complete data control to users. However, its usability and user experience are rarely considered. This study aims to improve SSI usability for non-technical users through literature review, prototype design, and two rounds of user testing and interviews. Key usability challenges were identified, and the effects of specific interface features on user experience were analysed. Based on the findings, actionable design recommendations are proposed, providing practical guidance for the development of SSI applications.

Acknowledgments

During the research and writing of this thesis, I received valuable guidance and support from my supervisors, Daria Schumm, Katharina Müller, and Prof. Dr. Burkhard Stiller. Their professional advice and patient assistance enabled me to make continuous progress in my research and successfully complete this thesis. I would like to express my sincere gratitude to them.

I would also like to thank my friends who participated in the user tests. They committed a considerable amount of time and maintained great patience throughout the process, which provided essential support for the successful completion of this thesis.

Finally, I would like to express my deep gratitude to my family. Their unconditional support and encouragement made the completion of this thesis possible.

Contents

Chapter 1

Introduction

This chapter first introduces the background of usability in decentralised applications and the motivation for this thesis. It then defines the general and specific objectives of the thesis, explains the methods used, and outlines the structure and logic of the thesis.

1.1 Motivation

Over the decades, authentication on the Internet has mainly depended on identity providers like Google [67]. These large identity providers store data on servers and manage it centrally [67]. However, central management may lead to potential abuse issues [57, 67], so that users' data privacy can not be well protected.

Self-sovereign Identity (SSI) is a new identity management model that is user-centred and emphasises privacy protection [57]. It does not centrally manage user data like traditional models, but gives complete control in the hands of the users. The World Wide Web Consortium (W3C) has proposed two key standards: Decentralised Identifiers (DIDs) and Verified Credentials (VCs) [57]. Although technological maturity is a prerequisite for the development of SSI identity management systems, the ultimate user adoption still depends on their experience [56]. However, User Experience (UX), usability, and socioeconomic considerations are largely overlooked and rarely considered in the SSI domains [14, 35, 37].

Addressing usability and UX challenges, while preserving decentralisation, is essential to ensure effective and safe identity management for non-technical users [27, 62]. Importantly, it is not advisable to promote user-centred design solely from a development perspective without the involvement of end-users [56]. Therefore, this thesis will focus on how to improve the usability and UX of SSI systems by actively involving non-technical users. The non-technical users referred to in this thesis are those who have basic digital literacy but lack an in-depth understanding of SSI technologies.

1.2 Thesis Goals

The general objective of this thesis is to explore how to improve the usability for non-technical users of decentralised applications, with a focus on SSI systems. To achieve this goal, several specific objectives are listed as follows.

- **Research on the role of usability for non-technical users.** To establish the background on the basis of usability and UX, its principles, and their applicability to software applications. Moreover, to explore how non-technical users are impacted by the poor usability and UX practices.
- **Investigation of guidelines and recommendations on usability and UX for SSI systems.** To conduct a comprehensive study of usability and UX guidelines and recommendations, this research starts with SSI applications by combining a literature review and analysis of existing SSI applications, and extends to decentralized applications.
- **Identify limitations and research gaps.** To highlight the current limitations and identify the research gap through analysis of the existing systems and literature.
- **Design and prototype.** To extract usability and UX features that can be used for the prototype, focusing on user communication, accessibility, and ease of use based on the explored guidelines. To design and prototype a front-end for an SSI application, applying selected guidelines and recommendations.
- **Study design and data collection.** To design a study that utilises appropriate measures for usability and research methods to collect data from a substantial but practical number of participants for the selected research method, with the goal of obtaining data for analysis.
- **Data analysis.** Analyse both quantitative and qualitative data collected from the user study. Apply statistical data analysis to describe the relationship between the user interface features and usability of a decentralised application. Capture usability challenges, and inform actionable design recommendations for improving SSI applications for non-technical users. Showcase the findings with appropriate graphics.

1.3 Methodology

This study used a mixed-methods approach to address the research questions. The study included a literature review, prototype development, and two rounds of user testing. The first round collected user feedback on interface features, usability challenges, and included quantitative measures of user experience. The second round was a short-term longitudinal study, aimed at capturing new and recurring usability issues. Data were collected through User Experience Questionnaire (UEQ) and semi-structured interviews, combining both quantitative and qualitative data.

1.4 Thesis Outline

This thesis aims to improve the usability of SSI applications for non-technical users. These chapters follow a logical process from basic theory to practical design guidance.

- Chapter 2 reviews existing literature on SSI and decentralised applications (Dapps). It summarises design principles and recommendations for SSI and DApps, and analyses several representative SSI wallets currently available in the market.
- Chapter 3 details the study design of user testing, data collection process, and methods for analysis.
- Chapter 4 presents the design process and the final prototype of the SSI wallet, which served as a key material in the user tests.
- Chapter 5 shows the findings from user testing, answering RQ2 by outlining key usability challenges and RQ3 by linking specific features to user experience.
- Chapter 6 combines the findings from Chapter 5 with the design principles and recommendations from Chapter 2 to generate actionable design recommendations, answering RQ1.
- Chapter 7 summarises the research work, highlights the core contributions, and discusses potential directions for future research and practical implementation.

Chapter 2

Fundamentals

2.1 Background

This section provides background information on user experience and Self-Sovereign Identity (SSI).

2.1.1 Usability and User Experience

2.1.1.1 Foundation Theories and Principles

The International Organisation for Standardisation (ISO) 9241-11:2018 defines usability as the ”extent to which a system, product or service can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use” [64]. Specifically, effectiveness addresses the accuracy and completeness of user achievement of specified objectives. Efficiency stands for resources like time or money used to attain the outcomes. Finally, satisfaction reflects how well a system, product, or service meets a user's emotional, cognitive, and physical needs [64]. ISO's definition of usability can be described as situational usability [56], as it emphasises the specific context of use, including the environment, target users, and intended objectives. For example, assuming all other factors remain constant, the usability requirements of younger individuals may differ significantly from those of older participants, since each age group tends to have distinct needs and preferences. In contrast, the definition of usability proposed by Nielsen consists of five attributes: learnability, efficiency, memorability, errors, and satisfaction [48]. According to [31], this definition reflects perceived usability, which concerns the user's subjective experience.

The ISO 9241-210:2019 defines user experience as the ”user's perceptions and responses that result from the use and/or anticipated use of a system, product or service” [65]. Usability includes both subjective and objective aspects of the use of a system, product, or service, whereas user experience evaluates subjective perceptions and responses during the whole interaction [56]. Therefore, a user experience analysis is not just about functionality, but also extends to hedonic and pragmatic aspects, such as aesthetics and fun.

The two terms are still closely related despite those differences [56].
Nielsen's 10 usability heuristics are widely applied in various contexts, and heuristic evaluation is considered a more efficient method than user testing [30]. Table 2.1 summarises Nielsen's 10 usability principles [48].

Table 2.1: Nielsen's 10 Usability Principles

Principle	**Description**
Simple and natural dialogue	Dialogue should not contain irrelevant information, and all information should be presented in a natural and logical order.
Speak the users' language	Use words that are familiar to the user rather than system-oriented terminology.
Minimise the users' memory load	Users do not have to memorise the information in each section, and the system description should be clearly located or easily retrievable.
Consistency	Users do not have to suspect whether different words, situations or actions mean the same thing.
Feedback	The system should provide appropriate feedback to let the user know what is happening.
Clearly marked exits	Users can incorrectly select system functions, and there needs to be clear markers for users to leave without lengthy dialogue.
Shortcuts	Accelerators that are not visible to novice users may often speed up expert interactions so that the system caters for both experienced and inexperienced users.
Good error messages	They should use plain language, point out problems and constructively propose solutions.
Prevent errors	Even better than good error message alerts is preventing errors from happening in the first place.
Help and documentation	Any help and documentation should be easily searchable, focused on the user's task, listing the specific steps to be performed, and not be too long.

However, there is a major issue with the above principles. Since the principles of usability were first proposed, technology has advanced significantly. In other words, the analysis at that time was based on the usability issues of previous systems, and it is likely that usability issues have also changed today [30].

For decentralised systems, there are frameworks like Decentralised Identifiers (DIDs) [46], which offer guidance on user-centric design. Although the European Digital Identity (EUDI) Regulation is not specifically designed for SSI, it incorporates decentralised principles, such as user control over identity data and selective disclosure of personal data. [69]. Among them is the topic of user consent, a concern that has also emerged due to the development of technology and evolving privacy regulations. It can be seen that the principle of usability also needs to keep pace with the times, in light of the progress of society and the development of science and technology.

2.1.1.2 Practical Applications in Real-World Systems

There is a wide variety of software available in the app store, such as tools for work and study, films and social media apps for entertainment, and online shopping apps. These apps are constantly involved in our lives, especially in today's electronic age. Different apps naturally have different focuses. For example, productivity apps, which focus more on efficiency, such as Excel, Word, etc., provide shortcuts that allow the user to process data and text faster [33, 39]. The concept of components in Figma is also very efficient, as users can reuse them, with the added benefit of reducing the risk of inconsistency in teamwork, as there is no need to re-create them [20]. In addition, the autocomplete function for search engines reduces the user's cognitive load [66]. Moreover, the autosave history function in Overleaf allows the user to go back to the previous editing node, thus effectively preventing possible accidental deletions. Social media applications, on the other hand, will pay more attention to the interaction between users, and the corresponding feedback will be quite important. For example, WhatsApp will indicate whether a message has been read or not via an icon in the message box. This provides users with timely feedback, with two brightly colored check marks indicating that the message sent to the other party has been read. WeChat supports a message withdrawal mechanism to avoid the embarrassment of sending the wrong message. Meanwhile, likes and comments in the friend circle will only be shown to mutual friends, which, to some extent, not only protects users' privacy but also encourages interaction.

Cross-cultural design is also a point to consider, and needs to be tailored to the user's specific cultural background and needs. For example, red and green have opposite meanings in China and the West, with red meaning good in China. Correspondingly, in a Chinese stock application, red means up and green means down, while in the West, it is just the opposite. The colours should be used accordingly to the mental models of different users. As mentioned above, as new technologies are created, usability principles need to follow as well. In a case study of virtual reality, researchers found that 77% of user feedback could be reflected in Nielsen's principles [73]. This suggests that even in emerging fields, basic principles may be useful as a guide in the early stages of research.

2.1.2 Self-Sovereign Identity

2.1.2.1 Definition

Self-sovereign identity (SSI) is an identity management model [11, 63], or rather a user-centric decentralised identity approach [14]. Sovrin defines SSI as "a lifelong, portable digital identity that is independent of any central authority and can never be deprived" [68]. SSI extends the application of asymmetric encryption technology in identity management [28], allowing individuals to have sovereignty over their digital selves [68], thereby enabling them to freely declare their identities without relying on centralised third parties [11]. In this new model, user identities are stored privately on their own devices, and they manage the data themselves, allowing them to control the degree of data sharing and only display it when needed [68, 75]. The concept of SSI has developed with the success of blockchain technology, which provides it with the necessary ecosystem [11, 14]. This concept solves one of the most important problems faced by the Internet: establishing, owning, and controlling a persistent verifiable identity [44]. In the future, self-sovereign digital identity is expected to solve the identity crisis [68].

2.1.2.2 Ten Principles

In the context of the lack of applicable rules for self-sovereignty [68], Christopher Allen proposed the ten principles of SSI to promote discussion and development in this field [44, 58]. These principles have been considered to define the advanced functionalities and interactions required for the SSI interface layer. We have summarised these principles [4] in Table 2.2.

Table 2.2: SSI 10 Principles

Principle	**Description**
Existence	Users must exist independently.
Control	Users must control their identities.
Access	Users must be able to access their own data.
Transparency	Transparency must be ensured in systems and algorithms.
Persistence	Identities must be long-lasting.
Portability	Information and services related to identity must be transportable.
Interoperability	Identities should be used as widely as possible
Consent	Users must consent to the use of their identity.
Minimalisation	Disclosure must be minimised as much as possible.
Protection	User rights must be protected.

2.1.2.3 Key Technological Components

- Decentralised identifiers (DIDs): DIDs are the core component of the SSI model, developed by the World Wide Web Consortium (W3C) [63]. They are globally unique, persistent, and represented by their independence from any centralised authority for management [14, 63]. DIDs are generated based on cryptographic key pairs, and their ownership can be verified through cryptographic methods such as digital signatures [63]. This feature enables it to establish unique, private, and secure connections between entities [14].

- Verifiable Credential (VCs): VCs are a core specification developed by the W3C [63]. It is a machine-readable and interoperable data structure used to express cryptographically verifiable and tamper-proof claims [11, 14, 63]. In the VCs ecosystem, there are three key roles: issuer (the entity that creates credentials), holder(the entity that controls credentials), and verifier (the entity that verifies credentials) [63]. The issuer can create and issue VCs to the holder [11, 14]. After that, the holder can forward it to the verifier, and in this process, the selective presentation of information is supported to meet the principle of data minimalisation [11].

- Verifiable Data Registry: The Verifiable Data Registry is an important component of the SSI ecosystem, responsible for mediating the basic data required for generating or using VCs [63]. Its function is to establish trust between different entities without relying on a single centralised institution, and is usually implemented by blockchain or other decentralised systems [14]. However, the concept of Verifiable Data Registry is not limited to blockchain; other forms of trusted databases (such as government identity databases) can also be considered as one of them [63]. In addition, an SSI deployment can integrate multiple types of registry [63].

2.1.3 Needs and Challenges of Non-Technical Users

Non-technical users are often considered to be people who are not part of the software team [53]. They often lack a background in the relevant technology and rely heavily on intuition. Some of the characteristics of non-technical users and the challenges they face are presented below with some examples.

1. **Lack of confidence** Non-technical users may lack confidence in learning new technologies and tend to give up due to frustration. Some studies have shown that older adults accept the use of technology. It is just that they are less confident in themselves and do not think they will be able to successfully complete the task, and generally feel anxious [16]. Studies have also pointed out that the higher the users' technology acceptance and technology self-efficacy, the more positive their attitudes towards technology-based self-directed learning, which further illustrates the importance of confidence in technology adoption [52]. This places greater demands on system design, not only to help alleviate technology anxiety but also to provide clear and timely feedback to enhance user confidence.

2. **Rely on intuition** Non-technical users often tend to use their intuition to understand problems in the new system. Research has shown that experience with similar features in the past has an influence on intuitive interaction [8]. People are more inclined towards designs that align with real-world metaphors, such as using a trash can icon to represent the delete function in computer design [42, 48]. Affordance is the connection between a person and a material good that encourages particular behaviours, while a signifier is any perceivable indicator that conveys proper conduct to an individual, a way to indicate that the affordance is present. When a signifier conflicts with a physical affordance, users are often attracted to the physical affordance [50]. For example, a bucket with a no littering sign is usually full of litter. Moreover, command lines are often used in the computer industry, but some new users might find them difficult to use due to the lack of a visual interface. Research shows that the system administrators surveyed prefer graphical user interfaces for interaction, as they have a shorter learning curve than CLIs [71]. These cases tell us the design should conform to real-life metaphors, i.e., to the user's cognition and mental models, to better communicate system functions.

3. **Do not understand technical terms** Many novice users face difficulties with the terminology. Specialised terminology can place an unnecessary cognitive burden on

non-technical users, and users without the relevant background knowledge need an explanation of what is being done and what the relevant options mean [48]. User-centred design should use the user's language rather than the system's language [48], such as using simple descriptive language for error feedback instead of codes like 404. In summary, it is essential to use user-friendly language. Just as you would explain professional knowledge to your grandmother, you should use the most accessible language to explain complex concepts.

4. **Prefer learning by doing** Non-technical users are often reluctant to read lengthy manuals and prefer to learn through hands-on practice. This behaviour is consistent with the "active user paradox" proposed by [12], which states that users tend to try out new operating systems directly rather than undergoing extensive training that prevents them from getting started. The "minimal manual" offers a more efficient approach, as it is more concise, does not emphasise reading, and encourages action [13]. This requires designers to create concise and effective learning manuals or precise error alerts to reduce the learning burden on users.

Poor design affects non-technical users, potentially causing them to feel confused, frustrated, and even abandon the product. For example, a usability evaluation of a mobile ticketing solution for public transport in Porto, Portugal [5] found that although most users believe that the route tracking feature is useful and relatively easy to understand, first-time users reported difficulty distinguishing between the complete route displayed on the interface and their current location. This design ambiguity can cause cognitive strain for new users. Furthermore, the app does not provide a clear indication that the journey has ended, leaving users, especially new users, unsure whether they have completed the journey. This may lead users to doubt the system's reliability. Another important issue is that there is no help button to guide users through the payment process, which increases the learning cost for users. Another study on the usability of electronic voting machines [19] found that while electronic voting machines scored highly in terms of user satisfaction, over 60% of participants did not notice that the voting machine had tampered with their selections on the review screen. This suggests that there may be issues with the design, specifically that the interface failed to effectively guide users through critical verification steps. Research indicates that this may come from users' tendency to trust the system, leading them to overlook errors even when the design is flawed. Additionally, 6% of participants in the study left the voting terminal before completing the final submission step. This behaviour is classified as a post-completion error. Such errors particularly affect non-technical users, who rely more heavily on clear operational guidelines and system feedback. These findings underscore the importance of optimising system design. The other study of the UK COVID-19 contact tracing app [74] showed that many users felt uneasy and refused to use it due to a misunderstanding about the app's functions, unclear privacy protection mechanism, and failure to consider the risk of social stigmatisation. This confirms how design flaws can increase the burden of understanding for non-technical users and ultimately reduce product adoption rates.

2.2 Related Work

2.2.1 Literature Search

The initial literature screening was conducted primarily through keyword searches in academic databases such as IEEE Xplore and the ACM Digital Library. Search terms included combinations of ”SSI”, ”usability”, ”ux” or ”user experience”, and ”principle” or ”guideline”. In addition to database searches, a snowballing strategy was applied, specifically backwards snowballing, where the reference lists cited in key papers were reviewed to identify further relevant literature. Moreover, a thematic review approach was conducted to extract and combine common design recommendations from the reviewed literature, resulting in a set of guidelines for SSI user interface design. This flexible analysis method allows for a rich and detailed description of data, highlighting patterns and similarities, which is useful for summarising key features across the reviewed literature [10].

2.2.2 Design Guidelines and Recommendations for SSI

Current research focusing specifically on usability, user experience, patterns and best practices in SSI applications remains limited [15]. Moreover, there is no standard set of design principles tailored for SSI systems from a user experience perspective. Nevertheless, existing studies consistently emphasise the importance of user-centred design, which is critical to easing the development of reliable SSI solutions [14, 36, 44, 56]. In the study [56], the usability challenges should be taken seriously because they affect non-technical users even more.

1. **Design for simplicity, but support understanding** Simplicity is regarded as the foundational guiding principle when designing a user interface in SSI applications [44]. In other words, SSI solutions should be straightforward and intuitive to use [45]. Simplicity is also recognised as a key factor influencing how novel a system appears to users [56]. Prior work emphasises that effective user interaction should minimise user cognitive load—specifically by hiding system complexity and eliminating the need for prior technical knowledge [44, 56, 58, 68, 75]. For example, users should not be required to understand complex concepts such as decentralisation to use the system effectively. However, for users to truly appreciate the security and privacy benefits of SSI, they need at least a basic understanding of how the system works before meaningful interactions become possible [44, 56]. With SSI, users need to manage the data themselves rather than just consent to its disclosure. So it is not just the company, but the user themselves who are responsible for protecting their privacy. The result is that users must know their own data and privacy to protect them [67]. Misconceptions about how the digital identity system operates can directly impact both security and privacy in practice [40]. Therefore, the interface should help users make sense of their choices and understand how those decisions affect their personal data and privacy [40]. Since SSI is designed for average users, it is essential that

users can distinguish how SSI is different from other systems that may look similar [56]. In particular, users need at least some technical knowledge to understand the added value of SSI, especially in terms of privacy and security, and make thoughtful decisions cite sartor2022love, teuschel2023don, Khayretdinova2022. In this context, ensuring users have a clear understanding of both the benefits and limitations of digital identity solutions becomes an essential goal that SSI wallets should aim to address [40]. After all, if the user can not understand what is happening in the moment and can not reason about it, the user is not sovereign [58].

2. **Use clear, non-technical terminology** Terminology plays a key role: labels and prompts should be easy to understand and feel natural to users [56, 57]. However, despite these usability guidelines, many digital identities are still designed based on technicians' understanding of 'user-friendly' or 'easy to use', but lack consideration of users' technical background [40], and [35] found that users' logic may not correspond to the developers' expectations. As a result, technical or specialised terminology is often used in practice, making it difficult for non-technical users to interpret system behaviour [28, 67]. Insufficient technical understanding may lead to reduced trust or even security fatigue, a state of mental exhaustion after long cognitive activities [40, 49, 56]. Simple terminology may help support user confidence in the system. Adding descriptive text beside the icon may help improve clarity and prevent misunderstanding for users [57].

3. **Align workflows with user mental models** To further enhance usability, aligning system workflows with real-world processes is seen as a way to improve usability by matching the underlying mental models of users with the design of the system [58, 68]. A user experience study involving end users of SSI wallets supports this, indicating that adopting real-world patterns in the interface design increases the overall user experience [56]. For example, presenting graphical credentials rather than text-based ones yielded better usability results, as users associate them with physical documents [56]. Similarly, displaying credentials in a structured way (e.g., in alphabetical order) can further support user navigation and recognition [56]. In contrast, a non-traditional workflow may cause insecurity for the user [28].

4. **Provide intuitive guidance and explanations** [35] pointed out the importance of providing solid explanatory guidance to ensure a great user experience. Further studies show that basic instructions may not be enough, and users could benefit more when they are given reasons behind certain required actions, which builds confidence in the system's logic and reliability [35, 56]. While gaining more knowledge may give users a better understanding of the concepts, in practice, this also requires a higher level of effort and may negatively affect the user experience [67]. An empirical study on SSI wallets further suggests that more intuitive interfaces with the instructions can help non-technical users feel more comfortable and confident when using the app [57]. For instance, users often experience a slight delay when retrieving or verifying credentials and may not understand the reason. This is typically due to the wallet synchronising with a public blockchain and updating the distributed ledger. Compared to traditional apps, digital wallets can be slower in such cases, which emphasises the importance of providing timely and clear feedback to help users understand what is happening [57]. Additionally, wallets should warn users

about the risks of not backing up. The recovery phrase is crucial to the wallet, and users need to understand its importance and be reminded not to lose or forget it. This information can be clearly explained in the app's onboarding screens [57] or using push alerts and other warning messages to remind users [35]. According to [56], understandable explanations are essential for users to fully benefit from SSI.

5. **Support multiple authentication methods** SSI digital wallets typically do not rely on centralised third-party authentication, nor do they require registration and password logins as in traditional methods. Users can interact with external services through the wallet and its data. Support for both biometrics and passwords is necessary to protect stored sensitive personal information [57]. Some wallets, such as Gataca, do not support passwords. A more comprehensive analysis of this digital wallet will be provided later in the article.

6. **Improve QR code interaction** [36, 57] suggested reducing the reliance on QR codes, which may improve efficiency. The study found that all digital wallets depend heavily on QR scanning to establish a connection with the verifier or issuer. However, scanning QR codes is not ideal in many use cases, as it often interrupts the user flow [36, 57, 75]. [75] pointed out that not all people involved are in the same location. As a workaround, the issuer or verifier may ask the user to enter a website URL and then scan a QR code. The study suggested that entering the URL could replace the QR scanning step, which would make the process simpler. On the other hand, [57] recommended using QR codes only to create the initial connection. After that, information should be exchanged through the already established secure channel, and the user will see the request directly in the app. Another benefit of reducing the reliance on QR codes is that it allows us to rethink the user interaction model, so that instead of using a laptop and a mobile device at the same time, users can communicate between apps using only a mobile device [36]. This better aligns with people's daily habits and is more convenient.

7. **Design based on real user behaviour :** Although many users claim to value privacy, they often share their sensitive data [67]. This mismatch between user stated preferences and actual behaviours highlights the importance of supporting user decisions through clear design, rather than relying on assumptions about user intent.

2.2.3 Design Guidelines and Recommendations for Decentralised Applications

In addition to the above recommendations tailored for SSI applications, the following general design principles for decentralised applications can further support the interface design of SSI systems.

1. **Prioritise clarity** The application's operational features should be intuitively understandable to users at first glance. To support this, the interface design needs to emphasise critical elements to reduce cognitive load while ensuring visual cues are naturally understood [6]. At the same time, when faced with unfamiliar operations,

users may abandon the product if they feel confused, so the design should aim to simplify this complexity [1]. To address this, it is important that users do not need prior knowledge, for example, they do not need to understand what decentralisation is to use related products [38]. Accordingly, to help new users get started quickly and reduce learning costs, the application should guide them through the journey from the very beginning [22]. In this context, onboarding is very important for new users, as it often provides explanations of new concepts and has a significant impact on new user adoption rates [3]. [22] found that providing onboarding can improve the usability of cryptocurrency wallets. In addition to onboarding, tooltips and FAQs can help clarify specific terms or concepts as they arise [1, 3, 51]. Moreover, progressive disclosure is an effective strategy to enhance usability by revealing more advanced details only when necessary, allowing users to gradually transition from simple to complex topics [1, 3, 51]. This educational process is particularly important, especially when it comes to addressing common misconceptions [23, 24, 34, 72]. By guiding users through a clear task flow, designers can introduce the complexity of web3 in a more approachable way and build user understanding over time [9]. Beyond those approaches, using concise language to help users understand complex blockchain concepts remains a key challenge. Many blockchain platforms use a large number of technical terms, making it difficult for users to navigate [1, 3, 6, 51]. An effective approach, for example, is to use the more user-friendly term ”network fees” instead of ”gas fees” [51]. Overall, it is necessary to seamlessly integrate education and security into the user journey [9, 17]. From another perspective, [72] indicates that enhancing users' understanding of relevant concepts not only benefits users but also reduces the burden on developers and customer support teams.

2. **Enhance user feedback and notifications** Feedback informs users about what is happening in the system and helps build trust. It can take the form of messages, such as error notifications, or visual cues, like a button changing colour when clicked [6]. Lack of feedback can confuse users[51]. When an error message appears, it should clearly explain the reason for the failure in simple language and offer guidance on what to do next [1]. Consistent feedback and clear status indicators throughout the interactions are essential for a seamless experience [9]. The problem that prevents mainstream users from adopting decentralised applications is that passwords can not be recovered. For inexperienced and new users, this must be communicated with absolute clarity. Experts agreed that simply saying ”Do not lose your password” is not enough, and it must be emphasised repeatedly. This can be achieved through concise and precise reminder dialogues. However, the focus should not be on the technical limitations themselves. Instead, the benefits, such as complete ownership and control over personal data, should be highlighted, which effectively turns limitations into unique selling points [29].

3. **Design for trust and Security** Building trust is essential in a decentralised economy, where users have full control over their assets [3]. Since users are solely responsible for their own data, many actions are irreversible. Therefore, the interface design requires careful attention to security [1, 3]. For each irreversible operation, the system should provide clear alerts that explain both the purpose and the potential consequences of the action. A good practice is to use checklists or confirmation steps before critical operations to reduce user error. Above all, design should be thoughtful

rather than simply fast [3]. Additionally, attractive design influences trust [2]. Being drawn to something makes it easier for users to build trust, increasing the likelihood they will use it.

4. **Mobile-first and responsive design** With a significant portion of users accessing blockchain applications via mobile devices, it is essential to prioritise interfaces optimised for touchscreens. Good practices include providing shortcuts for frequently performed actions and implementing responsive layouts for vertical scrolling, ensuring a smooth user experience [1, 51].

5. **Use familiar patterns** The interface design for web3 should adopt familiar patterns from web2, structuring interactions around users' natural workflows rather than being driven by technical concepts. Leveraging interaction patterns that users already recognise allows them to apply existing mental models when engaging with new systems. This helps guide users more smoothly from traditional platforms to the blockchain ecosystem [3, 9, 29]. For example, [72] suggests mimicking existing payment systems to reduce friction for users and improve overall usability.

6. **Consistency and accessibility** Keeping the typography and colours consistent helps make the app easier to understand and use. The design should take into account as many users as possible. For example, using high-contrast colours and adding alternative text for images can improve accessibility [6].

7. **Focus on mainstream use cases** Focus on real-world problems that most users face, and find scenarios that match these problems. It should be clear what problem the user is trying to solve. It is also important to note that early adopters are more likely to accept new technology if it is easy to understand, fits into their lives smoothly, and is more effective than existing solutions [38].

8. **Allow personalized settings** [72] suggests that it is feasible to distinguish between advanced and new users at the interface level, as the design of cryptocurrency wallets with different user profiles can enhance the overall user experience. For instance, new users may only need to see the default options, while experienced users and experts would be able to access advanced options, such as importing and exporting keys. Similarly, [29] proposes the development of both general and platform-specific tutorials tailored to users' varying levels of expertise. These tutorials should be categorised according to the knowledge level, so that users are able to access the information they need at the appropriate level.

2.2.4 Existing SSI Applications

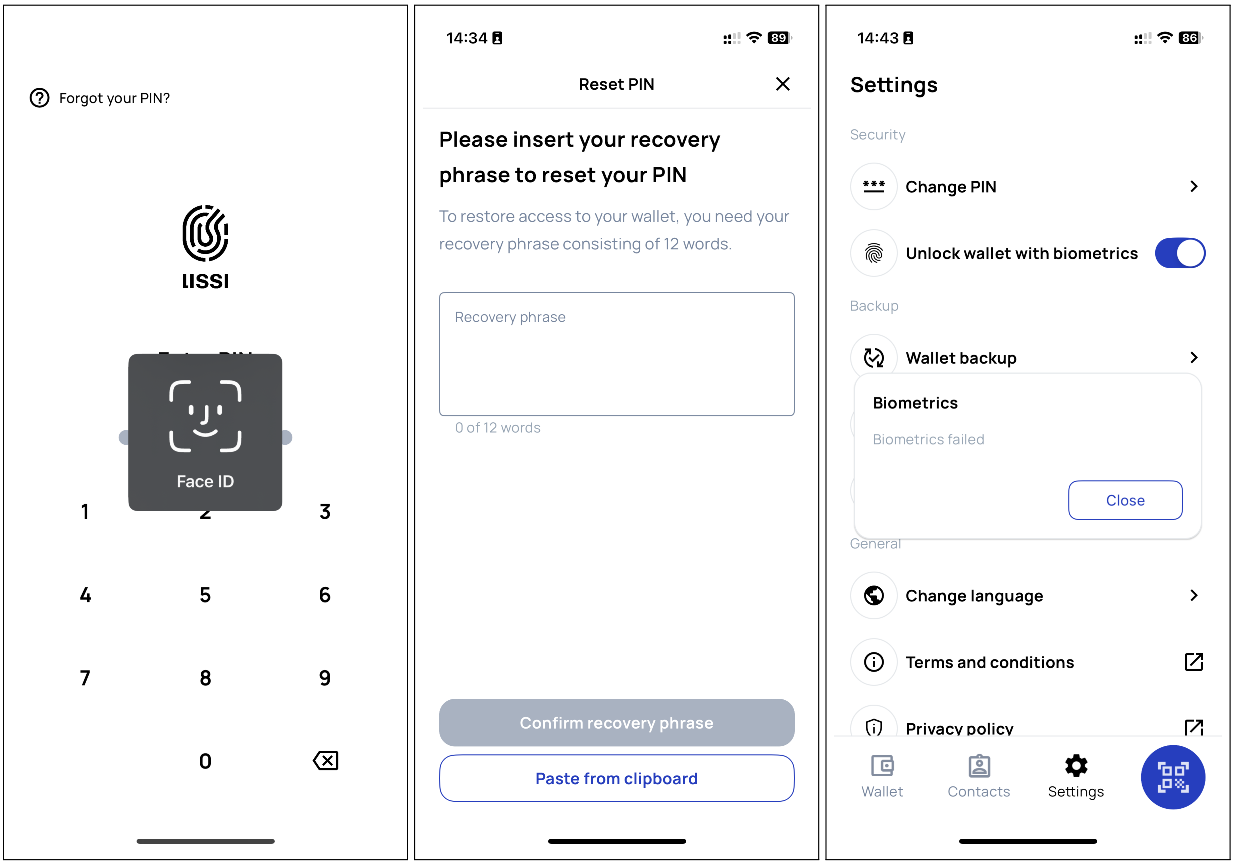
2.2.4.1 Overview of Current Applications

Evaluations of existing SSI wallets need to be performed iteratively, as new applications continue to emerge, and previously evaluated ones may be updated, discontinued, or become inaccessible. However, longitudinal studies focusing on SSI wallets remain scarce. This gap is consistent with the findings in related domains, for instance, [22] observed a similar lack of longitudinal analyses for cryptocurrency wallets, despite their dynamic evolution. A range of companies and governments are actively developing SSI wallets, and several are already available, such as esatus Wallet [18], Gataca [25], and Lissi Wallet [43]. However, they are still in early stages and vary in implementation, user experience, and supported features [15]. During the selection of applications for analysis, it was observed that many apps restrict functionality in certain regions. For example, the Louisiana Wallet app, despite having around 1.5 million downloads, could not be fully tested because of regional restrictions [21]. Below, we selected several digital wallets available on the App Store for analysis. Some of these wallets have been discussed in the literature, while others have not. For the latter, we used principle-based analysis. By combining both approaches, we aim to develop a relatively comprehensive understanding of current digital wallets. The selected wallets were chosen because they are frequently mentioned in existing literature or have been tested by users [56, 57, 67], and are still available for download on the App Store.

1. **Gataca Wallet** The Gataca Wallet [25], developed by the Spanish company Gataca.io, is supported by the European Commission and integrated with the European Blockchain Services Infrastructure (EBSI), making it a key candidate for the EU digital wallet initiative [56]. A user experience study published in 2022 found that 12.5% of the interviewees felt some of the terms used in the Gataca Wallet were too technical, such as 'levels' and 'DID', which they found difficult to understand. Other participants also described the interface as too plain in terms of the layout, colours and fonts [56]. The perceived novelty was below average, and users gave neutral ratings for privacy and security features, which may reflect a lack of user understanding [56]. Notably, most participants were young, technically educated, and digitally literate, suggesting that usability issues could be even greater for non-technical users. Since the study, the wallet has improved the presentation of credentials by switching from a text-based format to a graphical one. This is in line with the previously mentioned principle of aligning system design with users' mental models. Additionally, during initial setup, the app could not be used without enabling biometric authentication, but no clear message or guideline was provided. If users refuse at first, they have to go to the phone's settings to manually enable facial recognition, which may confuse or frustrate some users.

2. **Lissi Wallet** The Lissi Wallet [43] was developed by Main Incubator GmbH as part of a large German project with more than 40 private companies. Like other SSI wallets, the Lissi Wallet communicates with a blockchain infrastructure [56]. Among the evaluated wallets in the user study, the Lissi Wallet received the highest average score in terms of attractiveness, which reflects both functional and emotional qualities perceived by users [56]. Users appreciated the Lissi Wallet for its "clarity" and "simplicity", but some participants mentioned that more detailed initial guidance could help them better understand how to start using the app [56]. One possible reason for Lissi's perceived simplicity is its use of the more familiar and user-friendly term "Wallet" (see Figure 2.1c), whereas the esatus wallet uses the more technical term "Credentials" (see Figure 2.2b), which may be less intuitive for non-technical users. Additionally, the Lissi Wallet uses a six-digit password for authentication, while the esatus Wallet uses only a five-digit password. On the novelty scale, which

measures how new or innovative a system appears, the Lissi Wallet scores slightly above average. However, the general trend across all wallets showed relatively low scores in this dimension, suggesting a limited understanding of the new concepts behind SSI [56]. Similarly, when asked about users' sense of security regarding personal data, their responses were only neutral, and this may suggest that users do not fully understand that their data is stored locally and not shared with any central entity [56]. Moreover, the Lissi Wallet received higher ratings for the visual design of the contact overview [56]. Compared to esatus, it offers a "Forgot your PIN?" option on the initial interface (see Figure 2.1a). However, it should be noted that the information is not stored centrally, so it is not the same as the traditional way for users to retrieve their passwords. Users can only recover their accounts through 12 seed words recovery (see Figure 2.1b). In the Lissi Wallet settings, users can enable biometric authentication, but "unlock wallet with biometrics" will fail if Face ID has not been authorised for the app in the phone's settings (see Figure 2.1c). Once biometrics are enabled, users can access the app using Face ID without entering a password.



Please insert your recovery phrase to reset your PIN

To restore access to your wallet, you need your recovery phrase consisting of 12 words.

Biometrics failed

(a) Initial screen with "Forgot your PIN?"

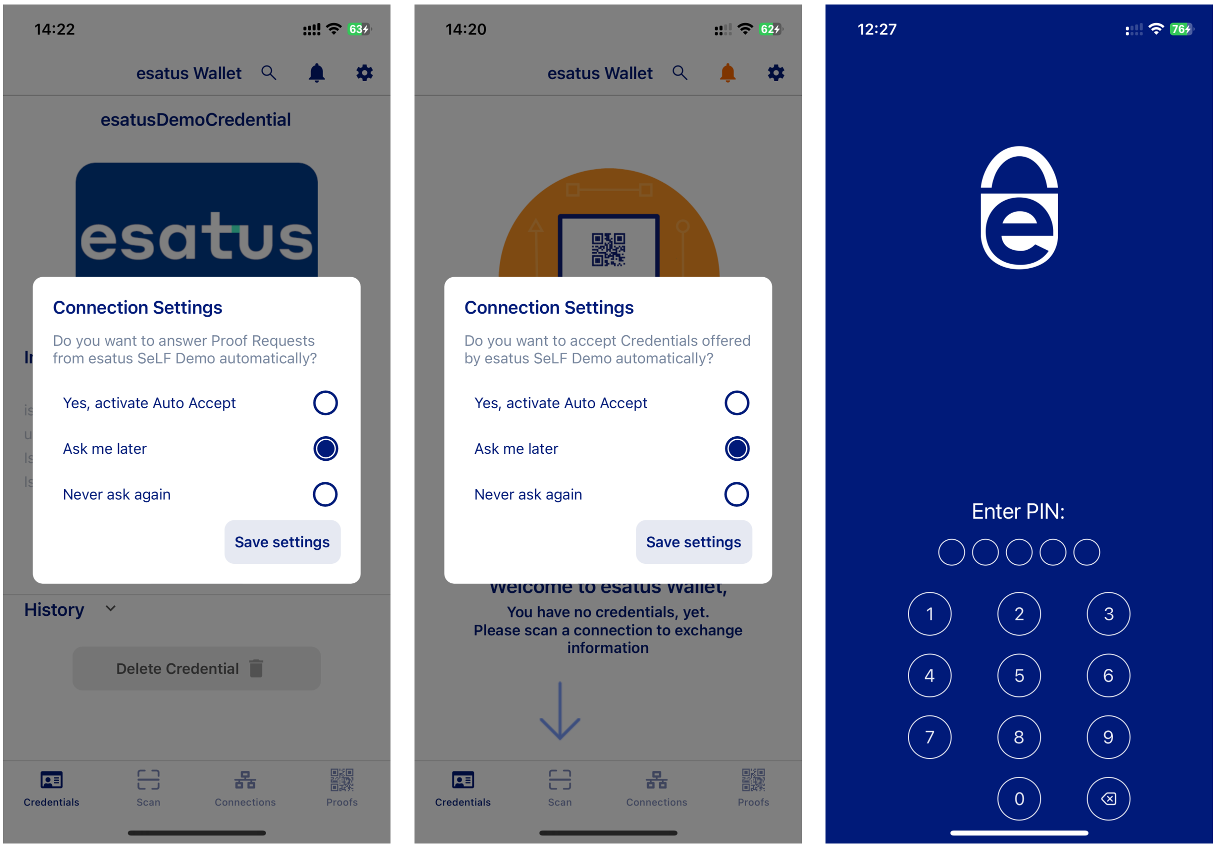
(b) Reset PIN screen

(c) Biometric login error due to missing Face ID authorisation

Figure 2.1: Screenshots from the Lissi Wallet

3. **esatus Wallet** esatus [18] is one of the leading companies providing software solutions based on SSI [28]. The company develops digital wallet applications for end-users,

which achieve a reasonable level of standardisation and interoperability [56]. When interacting with the esatus Wallet in its test network, the app prompted users to decide how to handle future claims from the same verifier after sending a claim (see Fig.2.2a), and a similar prompt appeared when receiving claims (see Fig.2.2b) [67]. The default choice was 'Ask me later', shown in the centre. If users selected 'Yes, active Auto Accept', they could also choose to receive notifications, which were not enabled by default [67]. However, this could lead users to send their verifiable credentials to malicious organisations, since most digital wallets do not clearly show information about the issuer or verifier. Only a few wallets, like Lissi Wallet, provide such details. This problem becomes more serious if requests are accepted by default, which is the case in esatus Wallet [67]. The study also mentioned a language issue, where English and German were mixed in the interface. However, based on my experience, this problem seems to have been fixed in the current version. In Lissi Wallet, users can scan QR codes via a button, while in esatus Wallet, this feature is located in a separate tab [67]. In another usability study, five core tasks were used to evaluate SSI wallet user interactions: configuration (T1), establishing connections (T2), receiving/sharing credentials (T3-T4), and backup/restore (T5). Regarding configuration, unlike some other wallets, the esatus Wallet does not include a quick start guide to help users understand its features. During setup, the



Connection Settings

Do you want to answer Proof Requests from esatus SeLF Demo automatically?

Yes, activate Auto Accept ○

Ask me later ●

Never ask again ○

Connection Settings

Do you want to accept Credentials offered by esatus SeLF Demo automatically?

Yes, activate Auto Accept ○

Ask me later ●

Never ask again ○

Welcome to esatus Wallet,

You have no credentials, yet. Please scan a connection to exchange information

Enter PIN:

(a) esatus Wallet asking about future behaviour with the verifier

(b) esatus Wallet asking about future behaviour with the issuer

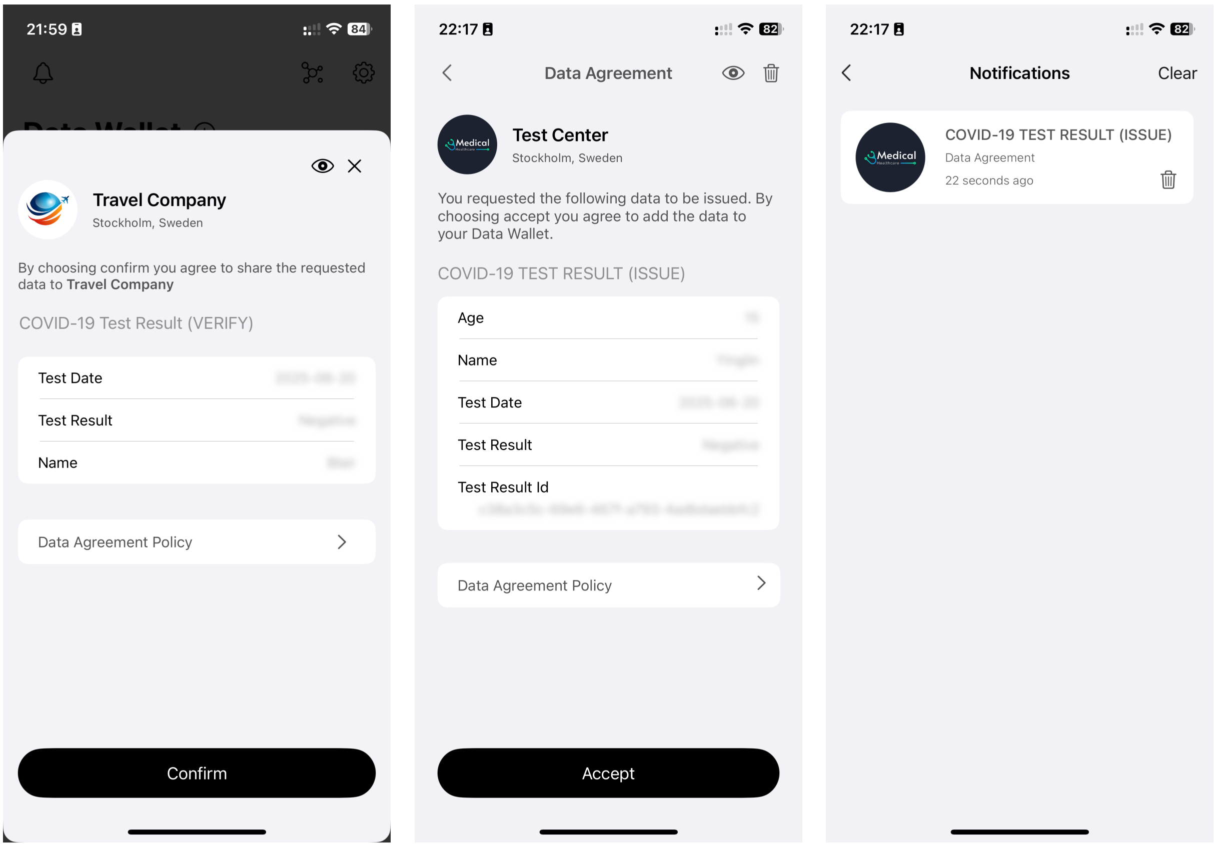
(c) esatus Wallet initial screen

Figure 2.2: Screenshots from the esatus Wallet

app only prompts users to create a PIN and enable notifications. However, if users forget the PIN, they cannot access the wallet, and there is no clear way to reset it. Biometric authentication can be enabled manually via the settings menu. The recovery phrase is located under the ”Create/Export backup” option in settings, which may not be intuitive—one study participant, for example, failed to locate it when asked, indicating potential usability issues [57]. In terms of establishing connections, all main functions (Connections, Credentials, Scan, and Settings) are easily accessible from the home screen and clearly labelled with both icons and text, which is consistent with the recommendation made by [57]. Once a user connects with a third party, the connection appears in the Connections tab. The app also provides a clear interaction history for each connection, allowing users to see past exchanges with that party [57]. In terms of receiving and sharing credentials, all received credentials are shown in the ”Credentials” tab, which also serves as the app's home screen. The app displays these credentials in a horizontally scrollable list. While this layout works well when there are only a few credentials, it becomes less user-friendly as the number increases. In comparison, Lissi Wallet displays credentials in a grid layout, unlike esatus Wallet, which presents them one by one [67].Additionally, there is a ”Proofs” tab on the home screen that allows users to create proofs, but the app does not offer any guidance or explanation about how this feature works. When opened for the first time, the screen simply shows the message ”No Gateways found”. The terminology used here may be too technical for the average user [57]. As with other wallets, recovery in the esatus Wallet is not possible if the wallet file has not been backed up. Creating a backup is simple, and users can go to the ”Create/Export backup” under the settings and follow the provided instructions. The app also checks whether users have correctly saved the recovery phrase [57]. This ensures that the user has memorised the 12-word recovery phrase in order. Within the study, the esatus Wallet was the best performer with the highest task completion. The study found that tasks related to receiving (T3) and sharing credentials (T4) were the easiest for participants, while backing up and restoring the wallet (T5) proved to be the most difficult across all tested wallets, indicating a common usability challenge in this area [57].

4. **Data Wallet** Data Wallet [32] by iGrant.io encountered issues during testing, as some demo workflows failed at the beginning due to invalid QR codes detected by the app itself [67]. To receive verifiable credentials, users must first select a claim type and then scan a QR code, and they can also establish connections with organisations via QR code scanning [67]. Although previous literature [67] noted that the information list about the institution in the Data Wallet can become lengthy due to the inclusion of data agreements, my observation revealed a more structured approach in the current version of the app. Specifically, when verifying credentials, the detailed information is not displayed all at once. Instead, the data agreement is placed behind a separate button labelled ”Data Agreement Policy” (see Figure 2.3a). This design choice allows users to access detailed terms only when needed, improving the clarity of the interface. As shown in Figure 2.3b, the claims appear blurred by default during credential interactions, but can be revealed with an additional tap. Additionally, during the credential receiving process, the ”Accept” interface does not appear automatically. Users must manually navigate to the notification and open

the pending request themselves to review and accept the credential (see Figure 2.3c). This adds an extra step to the interaction and may reduce user experience for less experienced users. In some cases, the Data Wallet takes more time than traditional methods to receive certain credentials. However, during this waiting period, the interface only displays a spinning loading indicator without any progress feedback. This may lead users to misinterpret the delay as a system lag or crash.



Travel Company
Stockholm, Sweden

By choosing confirm you agree to share the requested data to **Travel Company**

COVID-19 Test Result (VERIFY)

Test Date
Test Result
Name

Data Agreement Policy

Confirm

Data Agreement

Test Center
Stockholm, Sweden

You requested the following data to be issued. By choosing accept you agree to add the data to your Data Wallet.

COVID-19 TEST RESULT (ISSUE)

Age
Name
Test Date
Test Result
Test Result Id

Data Agreement Policy

Accept

Notifications Clear

COVID-19 TEST RESULT (ISSUE)
Data Agreement
22 seconds ago

(a) Separate access to data agreement

(b) Receiving blurred claims

(c) Credential request notification

Figure 2.3: Screenshots from the Data Wallet

5. **VIDwallet** The VIDwallet [70] is the only wallet that explicitly requested users to accept data protection terms upon first launching the app [67]. The demo offered three methods for receiving verifiable credentials: linking a phone number, linking an email address, or using an ID document such as a passport or identity card.

2.2.4.2 Usability Challenges of Existing Systems

Addressing these usability challenges is key to solving the [36] "How to encourage adoption of complex yet well-intentioned technologies"

1. **Interaction friction** The SSI model generates a higher level of friction than the centralised model. This is related to a lack of understanding of the concepts involved, cognitive engagement and the need for users to take on more responsibility [44].

2. **Missing mental model** Many of the concepts and mechanisms in the SSI system are unfamiliar to users, and they lack sufficient mental models to understand and operate these systems [35, 40, 44]. Although the interface may be well designed, users still have difficulty using the system effectively when faced with complex steps and responsibilities. It is difficult for them to truly and effectively use such systems without adequate guidance. However, research has shown that optimising the interface alone is not enough to solve the problem, as the complexity of the entire SSI system itself creates a significant barrier to the construction of an effective mental model for users [44].

   Usability studies of SSI wallets have consistently reported issues, such as the use of difficult technical language, lack of interface guides, and user limitations caused by abstraction [28, 56, 57]. For example, a user may have difficulties locating the recovery phrase within the app or fail to understand its function altogether. In some cases, the app interface uses only icons for navigation tabs, which further increases ambiguity and confusion [57]. This missing or inconsistent mental model is also reflected in the heterogeneous user responses observed in previous studies, where evaluated SSI wallets received generally low scores for stimulation and novelty, accompanied by high variance across users. These differences are believed to come from users' different backgrounds and interpretations of the system. This divergence, in turn, highlights how a lack of shared understanding can impact user experience evaluations [56].

   A lack of understanding regarding privacy and security features is another indicator of missing mental models. Prior studies found that users gave neutral assessments in these areas, likely because they did not comprehend the fact that personal data is stored locally on the user's device [56]. Similarly, participants in other evaluations reported that security was their major concern [35]. These findings suggest that users are often unaware of how SSI protects their data, highlighting the importance of helping them to build accurate mental models. Furthermore, learnability has been identified as a particular challenge for end users when interacting with SSI systems [36].

3. **Cognitive overload** High cognitive load for new users leads to adoption challenges. The study further points out that even if users have some understanding of the system, they still need to rely heavily on internalised cognition. In addition, the concept of SSI emphasises a high degree of self-management responsibility for the user, who needs not only to understand personal data and its value but also to manage it. Friction problems, as mentioned earlier, are mainly caused by internalised processes [44] when it comes to cryptocurrencies, which are not SSI applications but still involve decentralisation. [38] pointed out that conceptual barriers can make it hard for most users to understand how the application works. These barriers include difficulty in understanding terminology, like the concept of blockchain.

4. **Key management and account recovery** Key management and key recovery remain fundamental usability issues. The challenge lies not only in the technology itself but also in the learning costs for users. It is important to support non-technical users to manage their keys in an efficient and secure way [27, 57, 61, 62]. In traditional identity management, the identity provider is primarily responsible for managing

the identity data, while in the SSI model, it is the user who takes on responsibility and its associated risks [11, 63]. There have been many examples of users losing their cryptographic keys, resulting in the loss of valuable information [63]. This shift in responsibility can be especially challenging for non-technical users, as poor management of private keys remains a significant usability barrier in SSI systems [27]. While the literature emphasises the importance of key recovery, in practice, many SSI applications do not provide a clear ”key management” or ”key recovery” interface. Instead, user studies of SSI wallets often use the term ”account recovery” or ”identity recovery”, which typically implies that a key recovery mechanism is embedded in the process. In the context of cryptocurrency wallets, studies have found that most systems do not expose the process of generating keys to their users, hiding some of the technology in this way will be more convenient for users who do not want to manage the keys themselves, but may not be transparent enough for others [47]. This observation is also relevant for SSI systems, which similarly rely on cryptographic keys for identity control. [35, 75] highlights the issue with the difficulty of backing up and recovering an identity. [75] note that many SSI systems use a seed phrase for backup and recovery, typically including 12 words. Users are expected to write down and memorise these to restore their identity if access is lost. However, the authors argue that this method is not particularly usable. Similarly, [35] point out that recovery processes are often either too complex to perform correctly or are not presented clearly enough, which leads to failed recovery attempts. Prior studies on cryptocurrency systems have suggested implementing design mechanisms that require users to re-enter parts of their backup phrase during the process in order to ensure they have properly saved it cite mai2020user. A similar approach has been adopted in the esatus Wallet, reinforcing user awareness of key management responsibilities.

5. **QR codes dependency** Many SSI wallet applications heavily rely on QR code scanning for interactions such as authentication and credential issuing. [57, 75] both highlight that requiring users to scan a QR code may be less than ideal and could cause usability issues. For example, users might use their phones' built-in QR code scanner instead of the one inside the app [36].

6. **Consent fatigue** According to Article 4 of the General Data Protection Regulation (GDPR) [26], valid user consent must be specific, informed, freely given, and unambiguous. However, properly implementing such consent within current identity models remains challenging. Additionally, requiring users to agree to numerous privacy policies repeatedly has led to ”consent fatigue”, where users become overwhelmed by frequent consent prompts [63]. [35] notes that theoretical control of one's own identity is similar to the experience users have with complete control over cookies when visiting a website. Manually managing these detailed preferences through annoying dialogue boxes may easily frustrate users. As mentioned earlier, users often prefer the more convenient option, even if it means exposing more privacy [45, 67].

7. **Build for early adopters** Many existing decentralised and SSI applications are developed for early adopters, who are already technically knowledgeable and appreciate privacy or sovereignty. However, most users do not share the same background or

motivation. As a result, the interface design and workflows often fail to support broader adoption [38]. Although this originally refers to cryptocurrency applications, similar usability challenges can also be found in many SSI systems.

8. **System latency and insufficient feedback** Users sometimes experience longer delays compared to centralised applications, when interacting with the blockchain, particularly during tasks like credential issuance [57]. These delays can cause confusion, as users may not receive direct feedback indicating whether the operation was successful or is still processing.

9. **Unclear benefits to users** The usability study of some SSI wallets found that they do not clearly convey their novelty and benefits to users. As a result, users may perceive SSI wallets as similar to traditional applications, even though they represent a fundamentally novel solution. One possible reason is that the user interfaces of SSI wallets do not significantly differ from conventional app designs [56]. This visual similarity may prevent users from recognising the conceptual shift of SSI, leading to a lack of perceived novelty. In the end, this lack of understanding can limit user appreciation of the system's benefits and negatively affect the adoption rate [56].

2.2.5 Problem Statement

While several studies have proposed improvements for the SSI system, few have implemented or tested suggestions in real-world practice. This lack of practical evaluation represents a gap in the field, especially given that the adoption of SSI technologies depends heavily on their practical usability, not just theoretical advances [55]. In addition, most prior exploratory studies [5, 35, 56] are limited to brief, single-session interactions, which may not fully capture the range of usability challenges that non-technical users encounter during real-world use. This is a lack of longitudinal research that assesses usability over multiple sessions. Moreover, many existing recommendations are presented in descriptive language, which is not easy to directly apply in design. There is a lack of research that translates these ideas into clear functional requirements that are suitable for prototyping.

This thesis aims to address these gaps, which include the lack of practical evaluation, the absence of longitudinal studies, and the need for operational design suggestions, by answering the following questions:

1. RQ1: How can SSI-based applications be designed to reduce usability challenges and better support non-technical users?

2. RQ2: What usability challenges do non-technical users encounter when using SSI-based applications?

3. RQ3: How do specific interface features in an SSI-based prototype (e.g., onboarding guidance, vertical arrangement of credentials) relate to users' perceived usability and overall user experience?

The core research question (RQ1) investigates how SSI-based applications can be designed to reduce usability challenges for non-technical users. To support this, RQ2 investigates the specific usability challenges users encounter, while RQ3 evaluates how particular interface features in the prototype influence perceived usability and overall user experience. As illustrated in Figure 2.4, these two analyses together provide a solid foundation for addressing RQ1 and formulating actionable design recommendations.

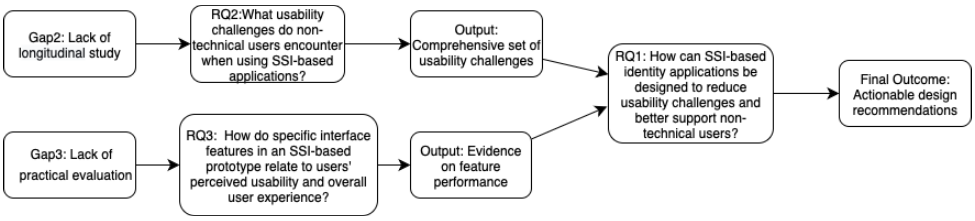

Gap2: Lack of longitudinal study
RQ2:What usability challenges do non-technical users encounter when using SSI-based applications?
Output: Comprehensive set of usability challenges
Gap3: Lack of practical evaluation
RQ3: How do specific interface features in an SSI-based prototype relate to users' perceived usability and overall user experience?
Output: Evidence on feature performance
RQ1: How can SSI-based identity applications be designed to reduce usability challenges and better support non-technical users?
Final Outcome: Actionable design recommendations

Figure 2.4: Research framework

Chapter 3

Methodology

This chapter outlines the methodology used to answer the research questions. It details the study design, participant recruitment, testing materials and procedures, data collection, and data analysis.

3.1 Study Design

This study used a prototype-based, task-oriented user study. First, a prototype SSI wallet was developed, inspired by previous literature, existing applications, and a pre-questionnaire. This prototype served as the test material for both rounds of user testing. The first round focused on the relation between prototype interface features and user experience, and collected initial user feedback through interviews and questionnaires. The second round was conducted a week later as a short-term longitudinal user study primarily to identify new usability challenges encountered by non-technical users. This interval was chosen due to practical time constraints and because certain issues, such as forgotten passwords [15], may arise within this period. Although brief, this design also allows the observation of recurring or delayed usability challenges that may not be captured in single-session studies. Data from both rounds were analysed to support design recommendations and answer the research questions. The overall study design is presented in Figure 3.1.

3.2 Target Group

The non-technical users referred to in this thesis are those who have basic digital literacy but lack an in-depth understanding of SSI technologies. The user group's age range is 18 to 45 years old, with a diverse educational background, in order to evaluate the usability and user experience of the SSI system more comprehensively. A total of five non-technical users were recruited to participate in the user test, and the participants came from the author's personal social circle. This number was chosen in line with findings in human-computer interaction research, which suggest that five participants are often sufficient

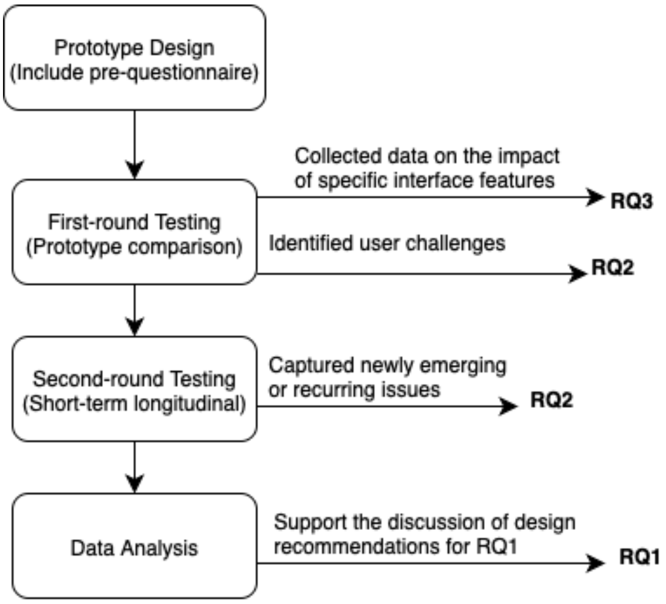

Prototype Design
(Include pre-questionnaire)
First-round Testing
(Prototype comparison)
Collected data on the impact
of specific interface features
RQ3
Identified user challenges
RQ2
Second-round Testing
(Short-term longitudinal)
Captured newly emerging
or recurring issues
RQ2
Data Analysis
Support the discussion of design
recommendations for RQ1
RQ1

Figure 3.1: Overview of the study design

to identify around 80% of usability issues [41]. Moreover, the recruited group aligns with recommendations that usability testing should focus on those most likely to use the application [57].

3.3 First Round of Testing

A within-subjects design was used, and each participant tested two existing SSI wallets and the prototype. The order of wallet testing was counterbalanced to reduce order effects. Although the design does not control for all confounding variables, the within-group comparisons and counterbalancing help reduce bias, making the observed relationship between interface features and usability more reliable.

3.3.1 Testing Materials

The wallets selected for this study include Lissi and esatus. The reason for choosing these wallets is that they are often mentioned in existing literature [14, 56, 57, 67] and applied for usability testing [56, 57], and they follow the SSI principle and common standards [57]. Moreover, both wallets can be downloaded from the Apple App Store and maintained regularly. The selected wallets both support core SSI functionality, and official demo test cases are provided, making them suitable as applications for user testing. A prototype SSI wallet was also used, and its design will be described in Chapter 4.

3.3.2 Testing Task

Currently, there is no SSI application on the market that has demonstrated sufficient market dominance [36]. So, based on previous literature and existing SSI products, this study has extracted the following user testing tasks.

1. Establish a connection.
2. Get a credential.
3. Share a credential.
4. Delete a credential.
5. Backup/Recover the digital wallet.

3.3.3 Testing Procedure

Before starting the study, we obtained consent forms from participants and gave a brief introduction to the test. Participants were asked to install the apps on their devices. All participants used Apple iPhones, running iOS 14.1 or later. The research sessions were conducted via remote video calls. During task execution, participants followed the "think-aloud" protocol. The author observed, recorded usability issues, and marked specific points where users encountered difficulties. Each session lasted approximately 2.5 hours, including task execution, questionnaires, and interviews. Breaks were allowed as needed to reduce fatigue.

Each session was conducted as follows:

- Perform tasks on the first wallet, then complete the UEQ for the first wallet.
- Perform tasks on the second wallet, then complete the UEQ for the second wallet.
- Perform tasks on the third wallet, then complete the UEQ for the third wallet.
- Conduct a semi-structured interview.

3.3.4 Data Collection

For the first round of testing, data were collected using a combination of quantitative and qualitative methods. Quantitative data were collected via the User Experience Questionnaire (UEQ), and qualitative data were collected through observation notes and interview records. The interview guide for the first round is provided in the Appendix A.

The UEQ was selected as the research tool because it can extract a wider and deeper range of user-centric aspects than the System Usability Scale (SUS) [56] and effectively assesses both product usability (e.g., efficiency, dependability) and user experience (e.g., stimulation, novelty). The questionnaire consists of 26 pairs of semantically opposed terms, covering six dimensions: attractiveness, efficiency, dependability, perspicuity, stimulation, and novelty. Participants rate each item using a 7-point Likert scale. To minimise response bias, half of the items begin with positive terms and the other half begin with negative terms, with the presentation order of all items randomly arranged [35, 56]. Observation notes and interview records were collected during the testing sessions to capture detailed user behaviours that cannot be fully measured through the questionnaire.

In addition, [56] indicates that successful usability studies combine quantitative and qualitative methods to obtain a more comprehensive perspective. Therefore, the combined approach of interviews and questionnaires is highly suitable for the objective of this study.

After the first round of user testing, a total of 15 UEQ results were collected (5 participants × 3 wallets).

During this testing, all conversations were recorded, intended for analysing task completion rates and operation times. However, due to interface freeze, crashes, and interaction limitations in existing wallets and the prototype, these quantitative data cannot reliably reflect the actual usability of the system. Therefore, this study eventually did not use task completion rate and operation time as analysis indicators. The data analysis was mainly based on the scores of the UEQ questionnaire and users' subjective feelings collected in the interviews.

3.4 Second Round of Testing

The same group of participants participated in a second round of testing, with a one-week interval. The testing tasks were the same as those used in the first round.

3.4.1 Data Collection

During the second round, qualitative data were collected through observation and interview records, focusing on both new usability challenges and recurring difficulties. These observations, combined with the first-round qualitative data, provide the basis for identifying user challenges. The interview guide for the second round is provided in the Appendix B.

3.5 Data Analysis

This section introduces how both qualitative and quantitative data were analysed to answer the research questions of this study.

3.5.0.1 Identification of User Challenges

To address RQ2, observation notes and interview records from both rounds of user testing were transcribed into textual form to identify usability challenges encountered by non-technical users. Inductive thematic analysis was applied to the notes, excluding those related to the predefined prototype theme. Inductive thematic was chosen because this method ensures that themes naturally come from user feedback, thereby gaining a deep understanding of usability challenges from users' perspective [54].

The encoding process was carried out using an affinity diagram. Specifically, initial affinity notes were created to capture users' original voice, and then these notes were grouped into blue labels, which were also created in the user's voice. Blue labels were then abstracted into pink labels, preserving the user's perspective. Finally, Green labels represented top-level core themes, summarising the Pink labels and capturing major aspects of the user challenges. Miro was used to create the affinity diagram, as presenting the transcriptions as sticky notes allowed flexible organisation and visualisation of the data. In the second round, the data were analysed iteratively in relation to the first-round codes to capture additional user challenges. The complete affinity diagram is provided in the Appendix D.

3.5.0.2 Analysis of the Relationship Between Interface Features and User Experience

To address RQ3, the analysis focused on how specific interface features in the prototype related to user experience. Quantitative data from the User Experience Questionnaire (UEQ) were combined with qualitative user feedback related to a predefined prototype theme from the first round.

- **User Experience Questionnaire (UEQ)** The UEQ data were analysed using Excel following the standard UEQ data analysis procedure. First, the original scores were re-coded onto a continuous scale from -3 (most negative evaluation) to +3 (most positive evaluation). This re-coding ensures consistency in the scoring direction, as the questionnaire includes both positively and negatively worded items to mitigate agreement bias. In this study, higher scores correspond to more positive evaluations.

  After re-coding, the mean and standard deviation were calculated for each wallet and each UEQ dimension. The mean reflects the overall user evaluation, while the standard deviation indicates the consistency of responses. A horizontal comparison was then conducted across the six dimensions (attractiveness, perspicuity, efficiency, dependability, stimulation, and originality) to assess the relative performance of the tested wallets. Additionally, the results were compared against the UEQ official benchmark database, allowing for an evaluation of each wallet's user experience relative to industry standards.

  It should be noted that technical issues, like crashes, may have an influence on UEQ scores. Therefore, these quantitative results are considered only for reference.

- **Observation notes and interview records** Deductive coding was applied to a predefined theme related to the prototype interface, categorising all relevant user comments. Due to technical issues, these qualitative data were the main source for analysing the relationship between interface features and user experience.

3.5.0.3 Generate Design Recommendations

To answer RQ1, this study combines the findings of RQ2 and RQ3 and proposes several actionable design suggestions. We first transform the main difficulties encountered by users in using SSI applications into improvement suggestions at the interface and interaction levels, which come from the analysis results of RQ2. In addition, based on the positive feedback from users on some interface features during prototype testing, we have also summarised design elements worth preserving and promoting, which are based on RQ3.

3.6 Ethical Issues

Before collecting data, the purpose of the study and the use of the data will be clearly stated. Participation is voluntary and can be withdrawn at any time without any consequences. No personal identity information will be shared with any individual or organisation. No personal identifiers will be used, thereby anonymising the data. User privacy will be protected, and irrelevant sensitive information will not be collected. For example, age groups will be used instead of specific ages.

Chapter 4

Design

This chapter describes the design of the SSI wallet prototype. It summarises insights from the pre-questionnaire, outlines typical usage scenarios, explains key design choices, and discusses design limitations. For the contents of the pre-questionnaire, see Appendix C.

4.1 Pre-Questionnaire

A total of 15 participants filled out the questionnaire, all belonging to the target group defined in this paper. The participants are generally heavy mobile phone users, with 11 people using their phones for more than 6 hours a day, and over half having experience using Apple Pay or Google Pay. Most participants self-reported moderate proficiency in using digital applications, typically scoring themselves 3 out of 5.

In terms of conceptual understanding, participants generally had low familiarity with SSI and related terminology. Six participants had never heard of SSI, six had heard of it but were unclear about its meaning, and only three expressed a vague understanding of it. Most participants (10/15) were unfamiliar with more specialised terms such as verified credentials, seed phrases, and decentralised identifiers. Notably, 10 participants indicated that the term ”credential” was understandable, which appears contradictory. This contrast may be due to the way the question was framed.

The questionnaire included a mix of existing wallet features (e.g., Dual login, forced confirmation of recovery phrase backup) and potential features proposed by the author (e.g., single-device QR code scanning, introductory animation). Participants' responses reflect their preferences for these features: combination authentication received the highest trust (11/15), while single authentication methods were less popular. Participants showed relatively high tolerance for wallets without central recovery (12/15 marked ”acceptable with clear warning”). However, this feature did not receive priority in the specific feature selection process, which indicates a gap between users' conceptual acceptance and actual functional priorities. Preferred features included dual login, credential classification, and single-device QR code scanning. Overall, security was considered the most important.

These insights guide the following prototype design on security settings and feature prioritisation.

4.2 Usage Scenarios

This section presents several typical usage scenarios for the prototype. They reflect common situations in which non-technical users need to interact with digital credentials, and are used to guide the design of the system.

1. **Obtain a verifiable digital degree certificate from the university**. Newly graduated Jane needs to obtain a verifiable digital degree certificate. She opens the wallet application and realises that she needs to apply for identity verification from the university. She scans the QR code provided by the university. She expects this to create a secure communication channel for data transmission. The system validated that a secure connection was established, which makes her understand that all further data will be private and reliable. After the connection is established, according to the system prompts, the student scans the new QR code, and the system redirects to the university identity verification page. After providing her student identity and necessary personal information, she expects real-time verification with the university's records. The successful authentication confirmation indicates that her request has been officially approved. After a moment, she receives an encrypted, signed digital certificate containing her complete academic information, such as the degree, the field of study and the graduation date. She carefully examines the displayed credential preview and confirms that all details are accurate. Jane confirms acceptance of the credential and receives confirmation that the credential is securely stored in the digital wallet. Jane believes that she has successfully obtained her degree certificate. She plans to use this digital certificate when applying for work or continuing education in the future.

2. **Share a digital degree certificate for a job application** A graduate, Jane, needs to prove to the company during the job application process that she has at least a bachelor's degree. She opens the wallet app and plans to provide proof of her education level to the company. She scans the QR code provided by the company. She expects this to create a secure communication channel for data transmission. The system validated that a secure connection was established, which makes her understand that all further data will be private and reliable. After the connection is established, according to the system prompts, the student scans the new QR code, and the system will provide her with certificate selection options. The system automatically identifies educational certificates that meet the company's requirements and only shows the minimum disclosure information, such as degree level, while other sensitive information is hidden. But Jane has the opportunity to review and potentially disclose additional fields, although the system maintains the default privacy priority setting. After confirming the sharing request, her education certificate will be transmitted to the company through a secure channel. The system confirms

the successful delivery, strengthening her understanding that only basic and authorised information is shared. After receiving the certificate, the company's system will verify the digital signature to confirm whether the academic certificate is issued by the university and whether it has not been tampered with. Also, the system is unable to view any other unauthorised information of the user. After the company confirms that the certificate is valid and meets the requirements, their recruitment team will proceed to the next step of the application process. Jane can view this shared event in the history within the wallet.

3. **Delete COVID-19 test certificate** Jane is a college student. During the epidemic, she often needs to upload the negative certificate of a COVID-19 test to enter the campus. Now that the epidemic is over, the university no longer requires these certificates, and she hopes to clean up this information that is no longer needed. She opens her wallet and finds the COVID-19 test record, thinking to herself, "This is no longer useful; keeping it will take up space, let me just delete it". She expects that there should be an option to delete the corresponding records. After she chooses to delete, the system does not immediately perform the deletion operation, but instead asks for confirmation. This meets her expectations that the system should double-check irreversible operations, which increases her trust in the application. After confirming the deletion, the system immediately displays a prompt indicating successful operation. Jane checks the credential list and finds that the test result has indeed disappeared. If the deletion fails, Jane expected the system to clearly inform her of the failure and suggest trying again later, rather than without any prompts.

4. **Backup digital wallet** Jane realises one day that "if I lost my phone, all my credentials will disappear. This won't work, I need to back them up first". She obtains 12 recovery phrases arranged in sequence through the backup function provided by the system, and understands that this is the only way for future recovery. After carefully writing down those words, the system asks her to fill in the randomly missing phrase position to verify her memory. After successful verification, the system confirms that the backup has been completed and guides her to store the backup files in the specified location. After completing the operation, Jane knows that in the future, the wallet can be restored by backing up files. If the verification fails, the system will prompt to recheck the complete phrase instead of allowing the process to continue.

4.3 Design Choices

This design focuses on the target user group defined in Section 3.2, who need an easy and reliable way to manage digital credentials without much technical knowledge. While earlier studies have suggested improvements for SSI systems, these recommendations have rarely been tested in practice. To address this, the design features in the prototype follow these suggestions, and their effectiveness will be evaluated in a follow-up user study. The goal is to produce a prototype that can be tested further. The overall design of the application is based on existing software, such as Lissi wallet and esatus wallet. Below are some design choices and an explanation of why they were designed in this way.

1. **Dual authentication and early warning - guideline: support multiple authentication methods** At present, some SSI wallets support password and biometric dual authentication, but there are still wallets that only provide a single method (Gataca), which only supports biometric authentication. In addition, not all applications prompt to enable biometric recognition upon first use (esatus). Due to the password not being stored on the central server, users can only restore access through 12 recovery phrases. If users do not record recovery phrases and forget their password, they will not be able to access the wallet. However, enabling biometric recognition can unlock wallets locally and reduce risks. Based on literature recommendations to support multiple authentication methods, and combined with pre-questionnaire results, this study adopts a dual identity authentication approach: biometric recognition is enabled during initial setup, and a clear warning is added to this process (informing users that centralised password recovery is not possible). The questionnaire shows that users conceptually accept decentralised recovery, but will not actively prioritise this warning. Therefore, integrating the warning into the biometric activation process can ensure security and inform users clearly.

2. **Random position verification - guideline: design for simplicity** In the confirmation stage of backup and recovery phrases, this prototype adopts a simplified design where users only need to click on three randomly placed words (represented by numerical positions) to verify that they have recorded the recovery phrases. In contrast, Lissi wallet requires users to drag words to randomly generated positions, while esatus requires users to click on all the correct words in the proper order. Although these existing methods are stricter, they increase the complexity of interaction. This design follows the principle of simplicity, maintaining a certain level of security while also reducing the number of clicks for users during their first use.

3. **QR code scanning via image upload - guideline: improve QR code interaction** This prototype follows the typical SSI wallet pattern of QR code scanning to establish connections and obtain credentials. To simulate single-device QR code scanning, the prototype includes an image upload option, allowing users to select a saved QR code image. In practice, the scanning process is simplified: users can simply click on a QR code placeholder to proceed, representing the interaction without requiring a second device or actual camera scanning. Although this design has not fully addressed the limitation of heavily relying on QR codes, as pointed out in the literature, it represents a practical improvement in usability.

4. **Coach mark and walk through - guideline: support user understanding** In the initial stage of the application, this study used coach marks, which point buttons or key interface elements in the form of bubbles and gradually guide users on how to establish connections, apply for credentials, etc. Unlike the text prompts on the interface, coach marks not only explain the function of a button but also provide a coherent operating procedure, allowing users to learn the process in actual operation. The purpose of this design is to help users better understand the core concepts of the SSI wallet and reduce their cognitive burden when using it for the first time. This

method is aligned with the suggestions proposed in previous literature to support user understanding.

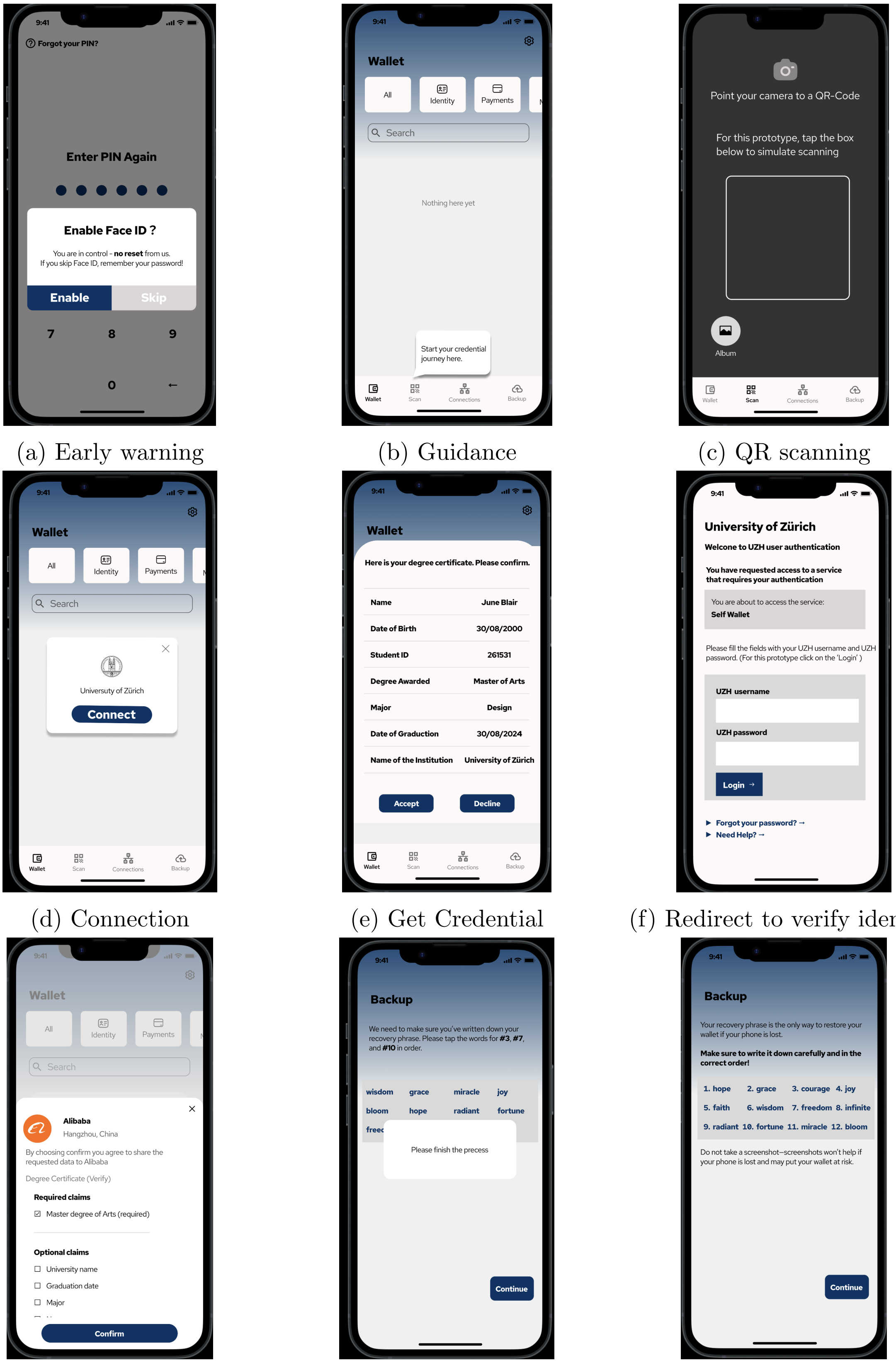
5. **Six-digit password - guideline: use familiar patterns** Initially, SSI wallets required users to set passwords. Unlike conventional apps, users can retrieve their passwords through email or other methods. SSI wallets rely on users to manage their own passwords to keep their data safe if the device is lost. Lissi wallet uses a six-digit password, aligning with typical mobile phone password conventions, while the esatus wallet uses a five-digit password. A six-digit password was chosen because it is consistent with the users' familiar password patterns. This choice also aligns with the design principles of simplicity and reducing cognitive load.

6. **Tab bar for key tasks - guideline: prioritise clarity** The tab bar design of this prototype is generally consistent with existing SSI wallets. However, adjustments were made to improve the discoverability of key functions. The scanning function is placed directly in the tab bar, with both an icon and a label, making it more intuitive than presenting it as a button alone. This also reduces steps, allowing users to switch between items more efficiently. Additionally, the backup function is given a separate position in the tab bar, rather than being hidden in secondary menus. These adjustments make core tasks easier to locate and help reduce confusion during use.

7. **Vertical arrangement of credentials - guideline: align workflows with user mental models** The presentation of credentials in this prototype differs from Lissi's grid layout and esatus' horizontal layout. Instead, a vertical, scrollable list is used, allowing users to browse in a single direction and view several credentials on the same page. Since SSI wallets may need to manage many credentials in the future, quickly locating a target credential becomes critical. A study on mobile user interfaces shows that scrollable lists take less time than grid layouts when locating and selecting targets, making them more suitable for efficient localisation needs [59]. Similar to popular social platforms like Instagram or Red Book, this prototype presents credentials in a vertical, scrollable list, which allows continuous browsing in a single direction. This is consistent with user mental models, making it easier and faster to locate and recognise items.

8. **Credential categorisation - guideline: focus on mainstream use cases** In practical applications, considering the possibility of future development, the SSI wallet is likely to store a large number of credentials, and presenting credentials will be a frequent operation. Therefore, following the user cases and drawing inspiration from existing applications (Gataca), this feature is adopted in the prototype.

9. **Terminology choice - guideline: use clear, non-technical Terminology** In this prototype, we chose the term ”wallet” because most participants in the initial survey were unfamiliar with technical terms such as DIDs and VCs. Although many participants indicated that the term ”credential” was understandable, as mentioned earlier, we consider this result unreliable, given the way the question was formulated and therefore follow the previous literature.



Enable Face ID ?

You are in control - **no reset** from us.
If you skip Face ID, remember your password!

(a) Early warning

Start your credential journey here.

(b) Guidance

Point your camera to a QR-Code

For this prototype, tap the box below to simulate scanning

(c) QR scanning

(d) Connection

Here is your degree certificate. Please confirm.

Name	June Blair
Date of Birth	30/08/2000
Student ID	261531
Degree Awarded	Master of Arts
Major	Design
Date of Graduction	30/08/2024
Name of the Institution	University of Zürich

(e) Get Credential

University of Zürich

Welcone to UZH user authentication

You have requested access to a service that requires your authentication

You are about to access the service:
Self Wallet

Please fill the fields with your UZH username and UZH password. (For this prototype click on the 'Login')

UZH username

UZH password

(f) Redirect to verify identity

Alibaba
Hangzhou, China

By choosing confirm you agree to share the requested data to Alibaba

Degree Certificate (Verify)

Required claims

☑ Master degree of Arts (required)

Optional claims

☐ University name
☐ Graduation date
☐ Major

(g) Share credential

Backup

We need to make sure you've written down your recovery phrase. Please tap the words for **#3**, **#7**, and **#10** in order.

wisdom	grace	miracle	joy
bloom	hope	radiant	fortune
freec			

Please finish the precess

(h) Back up recovery phrases verification

Backup

Your recovery phrase is the only way to restore your wallet if your phone is lost.

Make sure to write it down carefully and in the correct order!

1. hope	2. grace	3. courage	4. joy
5. faith	6. wisdom	7. freedom	8. infinite
9. radiant	10. fortune	11. miracle	12. bloom

Do not take a screenshot—screenshots won't help if your phone is lost and may put your wallet at risk.

(i) Backup error prompt

Figure 4.1: Interfaces of the prototype

4.4 Prototype Implementation

The study used the prototyping software Figma to create a prototype for user testing. Figure 4.1 shows several screenshots from the prototype. The reason to choose Figma is that it allows for rapid interface modifications and supports reusable design components, which saves much time. Additionally, when sharing the link, the prototype can be digitally distributed during user testing, allowing for remote evaluation and making the user testing process more convenient.

From the four dimensions of the prototype: 1) In terms of look, it maintains a relatively high level of visual quality to match the user's real-life experience and reduce the gap in look between following testing with existing applications. 2) In terms of breadth, the prototype covers most usage scenarios, including core tasks such as establishing connections, obtaining credentials, and sharing credentials, but recovery functionality is not included. 3) In terms of depth, the prototype has reached a moderate level. It provides detailed process feedback and supports process redirection, such as redirecting to the university authentication interface when applying for a degree certificate, but only for simulated verification operations (users can jump to the next interface after clicking login). In addition, the prototype also considers abnormal process states in the backup function, such as when the user clicks ”continue” directly without completing necessary operations, the system can also provide corresponding prompts. 4) In terms of interaction level, the prototype is at a moderate level. Users can experience the main processes of receiving, verifying, and backing up, including clicking buttons, page jumping, and receiving corresponding feedback. However, in terms of QR code interaction, the prototype only simulates a scanning button and has not implemented the full camera scanning function. This design ensures the smoothness of the system demonstration while meeting the testing needs of users for core functions.

Chapter 5

Results

5.1 Demographics

The participants of this study are five users aged 20-30 who have never heard of SSI and related concepts, which perfectly fits the positioning of the non-technical users that this study aims to investigate. On this basis, the specific composition of the participants is as follows: in terms of educational background, three individuals hold bachelor's degrees (accounting, textile engineering, fine arts) and two hold master's degrees (Management, computer science). In terms of tech-savvy, all participants rated themselves as either technically neutral or technically novice. However, all participants had extremely high levels of smartphone usage, with an average daily usage time of over 6 hours, and 40% of respondents had used Apple Pay or similar mobile payment tools.

5.2 Qualitative Findings

After coding and organising the interviews from five participants in the first round, a total of 126 initial codes were generated. These codes were refined and grouped into several core categories, resulting in four themes related to RQ2 and RQ3. Of the initial codes, 8 were excluded due to external factors, such as website redirects that did not reflect realistic usage scenarios. Another 22 codes did not directly address RQ2 or RQ3 and were also excluded from the main analysis, though some of these insights are discussed in the Chapter 6. In the second round, 30 additional codes were generated, of which 8 did not directly answer RQ2 or RQ3 and were similarly excluded. Integrating the remaining codes from both rounds ultimately yielded four themes. Three themes reflect the usability challenges non-technical users encounter when interacting with SSI applications, and one theme shows appreciation of specific prototype features.

5.2.1 Challenge One: Backup and Recovery

The task of backing up and restoring SSI wallets was identified as the main usability challenge faced by participants. All participants reported that the backup and recovery tasks were too complex, and the 12 recovery phrases were not only confusing but also cumbersome. They expressed a hope for a simpler and more intuitive method.

5.2.1.1 Overall Process Complexity and User Resistance

Participants generally expressed confusion and resistance to the 12 recovery phrases. This sentiment was captured by descriptions like *complex* and even *rubbish* (U5-02): *"12 words are really rubbish, so troublesome"*. For the recovery process, all participants complained that re-entering 12 words was unreasonable (U4-10): *"It's too much work..."*. Over half of the participants made mistakes when inputting the recovery phrase and had to recheck. This undoubtedly increased their workload. In the second round of backup testing, two wallets had completely opposite design patterns, with Lissi's backup phrases that did not change over time, while esatus generated new phrases every time. The study found that participants preferred the Lissi, saying it was a more *reasonable* operation, which allowed them to avoid the need to repeatedly record phrases in future backups. In contrast, esatus was regarded as inconvenient and a greater burden (2:U4-06): *"Backup is not easy to remember..."*. This clear preference indicated that users favoured security solutions that minimised their workload. Furthermore, participants did not merely criticise the system, but actively expressed their expectations for innovative solutions. They considered the existing backup methods to be *outdated* and *had room for improvement*, and suggested adopting more self-related alternatives, such as using custom security questions for recovery (U2-22): *"Can't we use some personal questions..."*.

5.2.1.2 Inconsistent Interface Design During Recovery

This study found that during the backup task, inconsistencies in interface design seriously affected participants' understanding and operational processes, posing significant usability challenges. The esatus wallet backup process in this study provided a typical case: the recovery phrases were displayed vertically, but became horizontally arranged during verification. This inconsistency in interaction logic seriously violated user expectations and caused strong dissatisfaction (U4-11): *"... how is it arranged vertically."*; (U5-04): *"... very unreasonable."*. In addition, although the system provided numerical identifiers as prompts before vertically arranged phrases, users often ignored such system prompts and followed their inherent habits (i.e. reading order from left to right, top to bottom) to operate. Moreover, the study found that the same problem occurred repeatedly for the exact same participants in the second round (2:U5-02): *I lost again, this vertical order is very useless*. Further issues arose in the logic of data presentation. In the verification phase, the application provided the user with repeated correct options (such as two "wear"), which triggered the user's self-doubt (U4-12): *"... I thought there was some subtle difference, which misled people."*. This indicated the application failed to present selection phrases with logical consistency.

5.2.1.3 User Behaviour and Security Trade-offs

The backup process prompt ”write down carefully” was strongly questioned by participants (U4-14): *”I don't even have a pen and paper to write down 12 phrases.”*. Consequently, not a single user followed the system's instructions. Instead, they commonly adopted insecure practices that prioritised immediate convenience. The dominant behaviour was to send screenshots to themselves through social media, while others saved them in their albums. As (U5-25) admitted: *”I will take a screenshot and send it to myself.”*. This consistent deviation of users from system expectations reflected design flaws that the recommended security method did not match the participants' behavioural habits. Inevitably, it pushed users towards a less secure path. It was worth noting that this may not have been a blind choice made by the user, but rather the result of weighing the trade-off. They even realised the security risks they faced when storing backup files (U5-24): *”For convenience, I will store the 12 recovery phrases and files in one place, which poses a security risk.”*, but ultimately chose convenience above security.

5.2.2 Challenge Two: Lack of Trust and Concerns About Safety

Most participants lacked confidence in the security of the SSI system, primarily due to doubts about simplifying processes, concerns about the lack of enhanced validation, and anxiety about data autonomy. Firstly, participants comprehended user autonomy as a lack of official responsibility and were concerned that data loss could not be retrieved (U2-17): *”There is no fallback plan”*; (U4-27): *”If there is an official endorsement, I would feel safer ... ”*. In extreme cases, participants would rather choose centralised storage due to a lack of trust in autonomy (U3-13): *... I don't believe I have autonomous control over data; it's definitely all monitored.”*. In scenarios such as opening a bank account, the process of SSI was much more straightforward than the complex process that users were familiar with. Its simplicity was negatively interpreted as insufficient security (U4-08): *”I don't think it's very safe. The bank gave the credentials too quickly”*; (U3-20): *”This application is easy to apply...The actual operation process of the bank app is very complicated.”*. Finally, participants expressed their expectations for enhanced verification, generally hoped to introduce strong verification factors such as biometric or passwords in key operations, like sharing, deleting, transferring (U2-10): *”If the deletion operation involves biometric recognition, I think it's safer”*; (U2-15): *”There was no double check when sharing”*; (U4-20): *”I hope more security measures can be provided, and some documents can be encrypted twice...especially when operations involving money.*. Most participants believed that the combination of passwords and biometric recognition ensured security (U1-16): *”I feel more at ease with dual authentication.”*, while only one participant opposed it due to privacy concerns with uploading biometric information (U4-17): *”Having a password is enough, no need for facial recognition.”*.

5.2.3 Challenge Three: Lack of Intuitive Guidance and Feedback

The study showed that if SSI applications could not provide simple and practical guidance and interaction, non-technical users were confused and even doubted the reliability of the system.

5.2.3.1 Lack of Initial Onboarding and Direction

Most participants did not know what to do when using the SSI wallet for the first time. One participant reported confusion when setting the password (U5-01): *"...I didn't know it was set by myself."*. The lack of guidance was particularly noted in the Lissi wallet, with participants generally stating (U2-11): *"At first, I didn't understand what I was going to do."*. This indicated that Lissi did not clearly lead the participant to use the scan function within the application. Moreover, during the first QR scanning process, some participants were not clear about which tool to use (U1-02): *"Is it using the built-in QR code function on my phone?"*, which caused confusion at the very beginning of the journey.

5.2.3.2 Unclear Processes and Unexplained Workflows

There were unclear processes and unexplained jumps, and users felt completely confused about the workflow of establishing connections and obtaining credentials. The operation of scanning QR codes multiple times for different purposes was confusing, and participants could not differentiate between these steps (U5-09): *"...These two steps are not distinguished, and it feels the same to me."*. Many users believed that credentials would automatically appear after establishing a connection (U4-02): *"I thought the credentials were stored in the connection."*.

5.2.3.3 Missing Feedback and Counterintuitive Interaction

The lack of clear feedback after the operation was completed was a problem. For example, when there was no successful prompt after saving the backup file, participants were not sure if they had succeeded (U5-05): *"After successful storage, there are no prompts."*. The most serious interaction issue was the drag-and-drop function used to verify 12 recovery phrases in the Lissi wallet, which all users found difficult to use and which lacked tactile or visual feedback (U3-08): *"Dragging words didn't respond, and clicking didn't feel like bouncing back."*. Regarding this, users suggested implementing more intuitive interactions, such as *animated buttons* (U3-22), to provide clear feedback.

5.2.3.4 Authentication and Password Recovery Issues

In the second round of testing, it was discovered that three users had forgotten their passwords. Two of them succeeded within three attempts, while the other failed all three attempts. However, their situations were not quite the same. One did not like to authorise biometric information, so the tested applications required passwords. The other two users did not reject biometric information, but because the application (esatus) did not automatically ask for it in the initial stage, and users did not manually enable biometric authorisation, confusion occurred (U1-04(2)): *"Why didn't this have a face ID? I forgot my password."*.

5.2.4 Prototype Features Supporting Usability

This study found that multiple design features in the prototype had been appreciated by users. The recovery phrase verification method used in the prototype (randomly selecting words and allowing users to click based on clear numerical instructions) was favoured by most participants. Compared to esatus and Lissi, this design was considered the most direct and easy method (U4-15): *"...is the easiest...clicking on the corresponding word with a clear number."*. Participants generally found the initial onboarding screen helpful, saying it made it easier to get started (U1-15): *"There are hints that make it easier for me to get started."*. The scanning function that supported image choices added to the prototype was considered convenient by all users (U5-13): *"It is more convenient to select screenshots..."*, which provided the possibility of single device operation. In terms of terminology selection, the term 'credential' was broader than 'wallet' since it was not just for financial situations, so users tended to prefer it (U5-14): *"Using wallet is too narrow, and there are also degree certificates..."*. In addition, participants preferred having both intelligent classification and autonomous editing when managing credentials (U4-25): *"I prefer editable automatic classification."*.

Therefore, in answer to RQ2, the key usability challenges identified are: 1) backup and recovery complexity, 2) lack of trust and concerns about security, and 3) lack of intuitive guidance and feedback.

5.3 Quantitative Findings

5.3.1 UEQ Scores

Figure 5.1 shows the results of the User Experience Questionnaire (UEQ) collected in 15 guided interviews and compared according to different wallets (Lissi, esatus and prototype). The y-axis represents the overall score, which ranges from -3 to +3 on a 7-point Likert scale. The x-axis represents six key attributes: attractiveness, perspicuity, efficiency, dependability, stimulation and originality. For the convenience of interpreting the results, this study referred to the official UEQ general benchmark (based on a summary of 468 product evaluations), which divides the performance of each dimension into four levels: excellent (within the top 10% of best results), good, above average, and below average [60]. When the attractiveness is higher than 1.84, perspicuity is higher than 2.00, efficiency is higher than 1.88, dependability is higher than 1.70, stimulation is higher than 1.70, originality is higher than 1.60, the application is considered to have excellent performance. This means that the application is leading in the corresponding dimension. On the contrary, when the attractiveness is below 0.69, perspicuity is below 0.72, efficiency is below 0.60, dependability is below 0.78, stimulation is below 0.50, originality is below 0.16, the software is classified as below average, indicating that the application experience in relevant dimensions is significantly weaker than most products.

According to the UEQ handbook, attractiveness includes two aspects: pragmatic quality (perspicuity, efficiency, dependability) and hedonic quality (stimulation and originality).

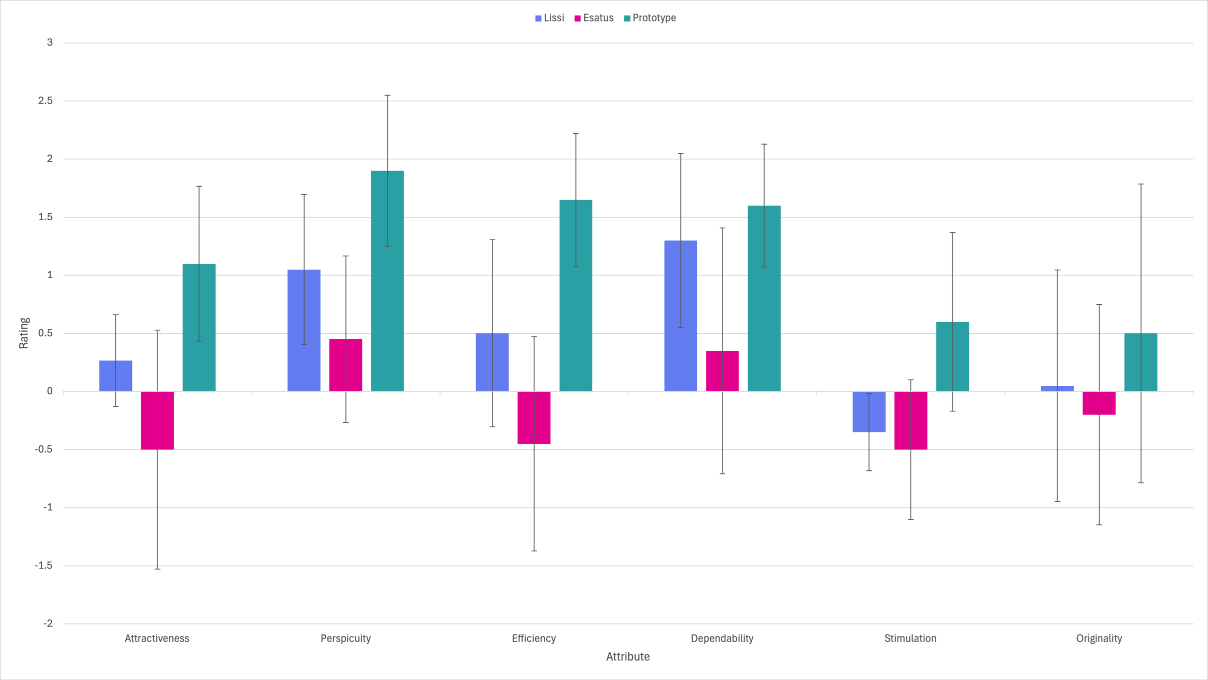


Figure 5.1: Mean scores per attribute and wallet with 95% confidence intervals.

Attractiveness scored the highest in the prototype (1.1), followed by Lissi (0.27), and esatus scored negative (-0.5). This indicated that the prototype was considered the most attractive overall, whereas esatus's current design was regarded as insufficient. One possible explanation for the low score of esatus was that the data transmission in the official demo was abnormally slow, even requiring users to redo the task, resulting in a poor user experience. Overall, for all applications, the score of pragmatic quality was higher than that of hedonic quality.

In terms of pragmatic quality, the prototype received the highest score, with perspicuity (1.9), efficiency (1.65), and dependability (1.6), all within the range of good to excellent compared to the general benchmark. In contrast, esatus scored lower in these attributes, with perspicuity (0.45), efficiency (-0.45), and dependability (0.35), all of which were lower than average compared to the benchmark. Lissi's performance was moderate, showing positive results in perspicuity (1.05) and dependability (1.3), which were above average compared to the benchmark. However, its efficiency score was only weakly positive (0.5). This may have been related to the official demo, which automatically redirected to its webpage after scanning the QR code, but the page often failed to load and appeared blank. Participants needed to switch back to the application for the following tasks. Regarding the hedonic quality, the stimulation score of all wallets was negative or close to zero, with esatus (-0.5) and Lissi (-0.35), while the prototype's average score was a bit higher, 0.6. This indicated that users did not find this type of application experience particularly exciting or motivating. Similarly, originality scores were also low across all tested wallets, with esatus (-0.2), Lissi (0.05), and prototype (0.5). This suggested that although these wallets actually integrated various innovative technologies, the innovation perceived by users was very limited, or even completely imperceptible.

The above results show that the prototype version outperforms Lissi and esatus in all attributes, which indicates that the user experience and usability have been improved. It is worth noting that in terms of efficiency, the prototype score is higher than esatus, and the confidence interval does not overlap, although technical issues in all tested wallets, including freezes and crashes, may have influenced the scores. However, because of the small sample size, this difference cannot be used as statistically significant evidence, but only for reference. Therefore, together with the qualitative data, in answer to RQ3, the enhanced interface features in the prototype appear to have a positive impact on perceived usability and user experience, although these findings remain exploratory.

Chapter 6

Discussion

Based on findings from RQ2 and RQ3, this section presents design recommendations for SSI-based applications. It reviews key issues from Chapter 5 and additional findings, aiming to support the development of SSI systems that reduce usability barriers and support non-technical users, thereby addressing RQ1.

6.1 Key Design Challenges

6.1.1 Challenge One: Backup and Recovery

This study found that the unique backup methods of the SSI wallets, like twelve recovery phrases, impose a huge burden on users. In contrast, a previous user study did not report critical usability challenges regarding the use of recovery phrases [57]. One possible reason is that the previous study may have focused more on task completion than on users' subjective experience. Successfully completing a task does not necessarily indicate that the process is easy or usable.

During the backup task in the tested application, users experienced difficulties with the vertical layout of recovery phrases, despite the use of numerical labels. Users tended to read the words horizontally, in line with their habitual reading pattern, and all those who faced this issue in the first round faced it again in the second round. This indicates that the inconsistency with users' mental models is a design issue rather than a task that can be learned over time. Therefore, interfaces should be designed to align with users' mental models, consistent with recommendations in the literature [58, 68].

During the backup process, several users had to re-enter their recovery phrases because mistakes were only discovered at the end of the task. This caused them to go back and retype the entire twelve words, which increased frustration. The main reason for this re-entering problem was the lack of real-time feedback during input, as users were not warned of formatting errors until all words were entered.

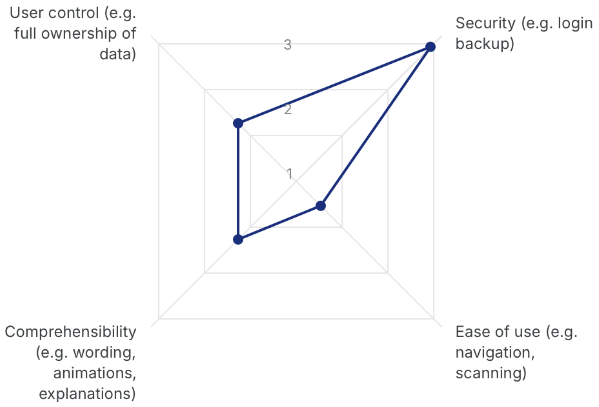


Figure 6.1: Importance features for users

6.1.1.1 Design Recommendations

1. **Real-time feedback for recovery phrases** The system provides real-time feedback on formatting errors as users enter recovery phrases, helping them correct mistakes instantly. In this way, if the user has any problems in the middle, they do not have to wait until all twelve words are input before going back to check. By doing this, it reduces the cognitive load for users, aligning with the design recommendations of minimising cognitive load [44, 56, 75], and enhancing user feedback [9].

2. **Recovery phrases presentation and verification** Recovery phrases are suggested to be presented in a horizontal layout with numerical labels on the initial backup page, which aligns with users' reading habits. The verification interface should maintain the same layout to ensure consistency. Instead of requiring users to select all phrases in the correct order, a randomised verification method is recommended to be adopted. Like asking users to click on three randomly placed words (represented by numerical positions, e.g. #3, #6, #9), which can help users quickly locate the desired phrases.

6.1.2 Challenge Two: Lack of Trust and Concerns About Safety

Users lack trust in the system mainly because the process operation is too simple compared to real scenarios. Moreover, there is a lack of verification operation for key steps, which users feel could lead to data leakage. This concern is consistent with the findings of [35] that most participants across different digital wallets agreed that security was the most important aspect for improvement. Similarly, the results of the pre-questionnaire collection show that security is ranked first by most users (see Figure 6.1). This indicates that ensuring application security is the primary requirement. One possible practice is to involve users in the security verification process, allowing them to experience that the system is secure intuitively to build trust. Below, we propose two suggestions to increase user engagement in security, which are in line with the principle design for trust and security [1, 3], and the SSI principle of transparency [4].

6.1.2.1 Design Recommendations

1. **Secondary verification of key operations** Adding a confirmation of biometric information or password when sharing credentials to increase users' trust in the system. When users authorise biometric information, the system automatically uses it to reduce friction.

2. **Security verification of QR codes** After the user scans the code, the application first recognises the QR code for confirmation. It provides feedback to the user that the system is verifying the security of the QR code, without directly jumping to the next step. After the system verifies that the QR code is secure, it guides the user to connect with a third party.

6.1.3 Challenge Three: Lack of Intuitive Guidance and Feedback

Lack of clear initial guidance can lead to confusion for users. In this study, novice users often struggle to know where to start and misuse the scanning function, relying on their phone's built-in camera instead of the in-app scanner. Even in the second round of testing, some participants still forgot to use the in-app scanner. This finding is consistent with [56], further indicating that the location where users should scan the QR codes needs to be clearly indicated.

Some users failed to complete the backup task because they did not click the ”save file” button on the final screen. This type of problem has been referred to as post-completion errors in previous research [19], stressing users' dependence on clear system feedback. This result is in line with the recommendation to provide clear feedback and intuitive guidance.

In the second round of testing, some users could not log in after forgetting their password, as facial recognition was not enabled. The user actually does not object to using this feature, but the application did not actively prompt to turn it on during initial use, and no participants manually activated the feature during testing. This indicates that the system needs to predict potential issues that users may encounter during the design and prevent them through early guidance or default settings, which corresponds to Nielsen's prevent errors principle, which states that preventing errors from happening in the first place is even better than good error message alerts. [48].

6.1.3.1 Design Recommendations

1. **Initial guidance** It is recommended to add initial guidance for novice users, as this is often missing in many applications. In addition, when there is no credential in the application, it is suggested that the main interface always guide users to scan a QR code. This recommendation is consistent with the suggestions to provide intuitive guidance and explanations [35, 57].

2. **Biometric login guidance** When the application is first launched, a prompt should automatically pop up asking the user if the biometric feature is enabled, and the user can freely choose to accept or reject it. Suggest adding a brief text prompt on the pop-up window to remind users that they cannot retrieve their password through traditional methods.

6.2 Prototype Features and Insights

User testing revealed a strong tendency for participants to set simple, predictable passwords (e.g., “123456” or “111111”), significantly increasing security risks. This is particularly critical for SSI wallets, as physical access to an unprotected device grants control over highly sensitive information. Also, as mentioned in the last chapter, users often forget their passwords. This presents a challenge for designing secure but user-friendly ways for users to access the application.

During the user testing process, a large number of QR code scanning operations are involved. This study found that participants often subconsciously searched for options related to images. This behaviour comes from a common experience in real life: many applications (such as Google Translate) have deeply integrated image scanning functionality. Users gradually form corresponding mental models through long-term practice, so they will naturally follow this habit in testing. This is highly consistent with the phenomenon mentioned earlier that non-technical users rely more on intuition for operations [8].

While participants found most prototype features convenient, placing the backup button separately on the tab bar led to an increase in false clicks during testing. Both of the other test wallets have backup functions within their settings. As a result, users habitually expected the prototype to do the same and often ignored the tab bar option. This deviation suggests that inconsistent design standards can cause users to form different mental models for each application, thereby increasing their cognitive burden. If there are unified industry design standards for core processes, users do not need to learn repeatedly, which can reduce their burden and improve usability. This consistency echoes the principle of portability in SSI [4]. Just as a unified design can save learning costs, portability allows identities to be universal across various platforms, eliminating the need for users to repeatedly adapt.

In addition to the suggestions mentioned in the previous section, this study proposes the following suggestions based on user feedback on prototype functionality and analysis of users’ actual operations.

6.2.1 Design Recommendations

1. **Pattern lock authentication** To address both the security and memorability challenges, we propose implementing a pattern lock as an alternative login method. This approach is supported by [7], which mentioned that humans are better at memorising visual information. Therefore, by doing this, it cannot only reduce users’

memory burden but also enhance security. Moreover, this suggestion extends the recommendation for multiple authentication [57], which focuses on biometrics and passwords.

2. **QR code scanning** For the QR code scanning function, the prototype simulated a combination of image upload and traditional camera scanning. User testing showed that participants appreciated the image upload option, especially when only one device is available. This is in line with the design principle of aligning workflows with user mental models [68], using familiar patterns [9, 29], and improving QR code interaction [75]

3. **Credential layout** In the prototype, credentials were arranged vertically, and user feedback indicated that this layout was well received. However, if the credentials are arranged horizontally, it is recommended that a real-time location prompt be provided to the user, such as (1/2), to help them understand the credentials' current location. At the same time, the total number of credentials should be clear to the user and how they are arranged. This recommendation follows the principle of providing clear feedback and intuitive guidance, which emphasises helping users understand system status and actions [57].

6.3 Additional Observations

6.3.1 Terminology

In terms of terminology selection, there is a notable inconsistency between the findings of this study and those of the previous literature. For example, the "wallet" and "contacts" used in Lissi Wallet are rated as "clarity" and "simplicity" [56]. However, this study found that users prefer to use "credential", believing that its concept is more comprehensive, while "wallet" is more financially oriented. One possible explanation is that the interviews in this study were conducted in depth, and participants were more likely to consider the semantics and actual scope of the terms used in communication, rather than just interface intuitiveness. In addition, the participants in previous studies were mostly young users with technical backgrounds, who may be more concerned about the clarity and simplicity of interface operations. So in terms of terminology selection, it may need to be adjusted according to the target user group.

6.4 Summary of Recommendations

Table 6.1 summarises actionable recommendations for SSI-based applications.

Table 6.1: Summary of usability challenges and recommendations

Usability Challenges	Design Recommendations
Recovery phrases entry difficulty	Provide real-time feedback during input to reduce re-entry and cognitive load. Present recovery phrases horizontally with numerical labels, and use randomised verification.
Lack trust in credential sharing	Add confirmation of biometric info or password when sharing credentials, and use biometric automatically to reduce friction.
Lack trust in QR codes	Verify QR code security before proceeding, and give the user clear feedback.
Unclear starting point	Display onboarding guidance and scanning cues when no credentials exist.
Unable to log in due to inactive biometric and forgotten password	Display a notification at first launch to enable biometric login, with a brief reminder that passwords cannot be recovered through traditional methods.
Weak and forgotten passwords	Use pattern lock and support multiple authentication methods (biometrics, passwords).
Dual-device QR code inconvenience	Support both image upload and in-app camera scanning.
Credential arrangement confusion	Use vertical layout. If horizontal, provide real-time location indicators (e.g., 1/2).

6.5 Validity Considerations

This section investigates the potential limitations of this study and their impact on the results. We will analyse from three dimensions: construct validity, internal validity, and external validity.

6.5.1 Construct Validity

1. **Missing backend** Figma does not have backend logic, so it can not verify whether user input is consistent with expectations. For example, in a wallet recovery scenario, the ideal interaction is that when the user enters the wrong recovery phrase, the system redirects them back to the initial backup interface. However, implementing this logic in prototype tools is complex. To make the design process more controllable, we simplified the interaction path and only displayed the successful process under ideal conditions, without implementing comprehensive error handling. However, the prototype still provides limited error feedback. For example, if a user attempts to continue without clicking any words, the system gives pop-ups to remind the user to complete the process. This trade-off, to some extent, reduces the applicability of the prototype, as it cannot reflect all error feedback and exception recovery. However, it allows users to focus on key design goals, such as clarity of terminology and

understandability of processes.

2. **Simulated QR code scanning function** The QR code scanning function in the prototype is simulated through a click box and does not interact with a real network or servers. This means that behaviours involving network connections cannot be validated in the prototype. Although the prototype can not test network-related anomalies or provide real-time feedback, we can still focus on understanding the core process.

6.5.2 Internal Validity

One limitation of internal validity comes from the insufficient counterbalancing of the task order. There are six possible orders for the three wallets. To achieve complete counterbalancing, the ideal design requires a sample size that is a multiple of six. In this way, every possible order could be assigned to an equal number of participants. However, this study only had five participants and could not achieve such a perfect balance. Although our method successfully ensured that no wallet was consistently placed in the first or last, the inability to equally cover all six combinations means that order effects may affect the validity of the results.

6.5.3 External Validity

1. **Small sample size** There were only five participants in this study. Although the main usability issues were identified, due to the small sample size, some less common but important usability challenges may have been overlooked.

2. **Demographic characteristics** The findings provide recommendations to young people who lack relevant background knowledge. However, their general applicability to a wider non-technical user group is limited. This includes older adults with lower digital literacy. In addition, the long duration of smartphone usage and the educational background of the sample can lead to an overestimation of usability.

   One possible way to promote the SSI model to the elderly population is to support multi-user modes, such as allowing adult children to help them manage credentials. However, since this model allows others to assist in management, it could have an impact on security. For example, children might use their elders' identities for unauthorised loans. Therefore, in promoting this technology, special consideration should be given to potential security risks.

Chapter 7

Final Considerations

This chapter includes a summary of the research work, core contributions, and reflections on future research and practice.

7.1 Summary

7.1.1 Implementation Steps

The specific implementation process for this thesis is as follows:

1. **Literature review and existing application analysis:** First, a literature review was conducted to summarise the design principles of existing decentralised applications and SSI applications. The study also explored currently available SSI wallets to understand their functionality and interface features.

2. **Prototype design:** A prototype was designed in Figma, incorporating inspiration from the literature and existing applications, as well as the functional preferences collected through the pre-questionnaire.

3. **User testing and interviews:** Two rounds of user testing were conducted. The first round included the UEQ questionnaire and semi-structured interviews, while the second round only included semi-structured interviews to gather user experience and feedback.

4. **Data analysis and design recommendations:** The questionnaire data and interview content were analysed to identify the main challenges encountered by users and ultimately provide a series of actionable design improvement recommendations for decentralised applications, focusing on SSI.

7.1.2 Modifications and Adjustments

Given that decentralised applications (SSI-based applications) are still in the early stages of development and there are few mature systems available, strict hypothesis testing or statistical comparisons with existing applications make it difficult to draw universal conclusions. Therefore, this study adopts an exploratory user research method, focusing on capturing the usability challenges encountered by non-technical users during use, and proposing feasible functional design suggestions to improve the user experience of decentralised applications.

Specifically, the core research question (RQ1) of this study aims to explore how to design decentralised applications to reduce usability challenges for non-technical users. To support this goal, RQ2 investigates the specific usability challenges faced by users during use, while RQ3 analyses the impact of interface features (such as initial guidance, vertical arrangement of credentials, etc.) in prototype applications on users' perceived usability and overall experience. The discovery of RQ2 and RQ3 directly provides actionable design recommendations for RQ1.

This method selection is not only highly aligned with the research objectives but also more practical and instructive in the current stage of SSI technology development. Through this exploratory analysis, this study can propose improvement solutions tailored to user needs, rather than just verifying hypotheses, thus providing a reference for the design and optimisation of future decentralised applications.

7.2 Conclusions

The main work value of this thesis is reflected in the following aspects:

1. Through user testing and interviews, usability challenges that non-technical users may encounter during the actual use of decentralised applications were identified, providing a basis for the next improvements.

2. Analysed the relationship between prototype feature improvements and user usability, revealed how different interface features affect user experience, and provided a reference for later design suggestions.

3. Based on the above two findings, a series of actionable design recommendations has been proposed, which can not only be directly applied to existing or future SSI applications but also provide practical guidance for developers and designers.

   Overall, this thesis has practical value in capturing user needs, improving user experience, and providing a reference for the future development of SSI applications.

7.3 Future Work

7.3.1 Functional Expansion

Participants hope that the digital wallet can be used not only to store identity documents such as degree certificates or residence permits, but also to expand to entertainment and other daily scenarios, such as storing Disney theme park cards or hotel membership cards. At the same time, they expect digital wallets to be widely recognised in real-world scenarios and even automatically provide relevant credentials based on actual situations. Although some users are sceptical about the integration ability of the application with a large number of third parties, the overall feedback is still positive. Especially in the second round of testing, all users reported smoother operations, indicating that the digital wallet has good learnability. Based on this feedback, future work can explore the functional expansion, third-party integration, and offline scenario adaptation of digital wallets to enhance user experience and application universality.

7.3.2 Authentication Strengthening

SSI applications may also have issues with identity borrowing, especially voluntary identity borrowing. Under force, neither facial recognition nor passwords can prevent it. However, by adding passwords or biometric authentication, voluntary borrowing behaviour can be prevented to some extent, with biometric information being particularly effective as it cannot be shared, while passwords can be given in advance. In addition, if identity information is entirely digitised, identity borrowing behaviour may develop into an industrial chain in the future, forming illegal identity leasing. Therefore, the study of authentication strengthening methods to prevent identity borrowing is not only of great practical significance but also provides guidance for the formulation of relevant laws.

Bibliography

[1] Rashika Ahuja. *Designing for Blockchain: Try These 8 Best UX Practices.* 2025. URL: https://procreator.design/blog/designing-for-blockchain-best-ux-practices/.

[2] Hayder Albayati, Suk Kyoung Kim, and Jae Jeung Rho. "A study on the use of cryptocurrency wallets from a user experience perspective". In: *Human Behavior and Emerging Technologies* 3.5 (2021), pp. 720–738.

[3] Alien. *Web3 UX Design: Crafting Seamless Experiences in a Decentralized World.* 2024. URL: https://www.thealien.design/insights/web3-ux-design.

[4] Christopher Allen. *The Path to Self-Sovereign Identity.* 2016. URL: https://www.lifewithalacrity.com/article/the-path-to-self-soverereign-identity/.

[5] Daniel Meireles de Amorim, Teresa Galvão Dias, and Marta Campos Ferreira. "Usability evaluation of a public transport mobile ticketing solution". In: *International Conference on Human Systems Engineering and Design: Future Trends and Applications.* Springer. 2018, pp. 345–351.

[6] Archit3ct. *Designing User Interfaces for DApps: Principles and Best Practices.* 2023. URL: https://archit3ct.io/designing-user-interfaces-for-dapps-principles-and-best-practices/.

[7] Robert Biddle, Sonia Chiasson, and Paul C Van Oorschot. "Graphical passwords: Learning from the first twelve years". In: *ACM computing surveys (CSUR)* 44.4 (2012), pp. 1–41.

[8] Alethea Blackler, Vesna Popovic, and Doug Mahar. "Investigating users' intuitive interaction with complex artefacts". In: *Applied ergonomics* 41.1 (2010), pp. 72–92.

[9] Polina Bobrova and Paolo Perego. "The Development of User-Centric Design Guidelines for Web3 Applications: An Empirical Study". In: *Computers* 14.2 (2025), p. 46.

[10] Virginia Braun and Victoria Clarke. "Using thematic analysis in psychology". In: *Qualitative research in psychology* 3.2 (2006), pp. 77–101.

[11] Clemens Brunner et al. "Did and vc: Untangling decentralized identifiers and verifiable credentials for the web of trust". In: *Proceedings of the 2020 3rd international conference on blockchain technology and applications.* 2020, pp. 61–66.

[12] John M Carroll and Mary Beth Rosson. "Paradox of the active user". In: *Interfacing thought: Cognitive aspects of human-computer interaction.* 1987, pp. 80–111.

[13] John M Carroll et al. "The minimal manual". In: *Human-computer interaction* 3.2 (1987), pp. 123–153.

[14] Špela Čučko, Vid Keršič, and Muhamed Turkanović. "Towards a catalogue of self-sovereign identity design patterns". In: *Applied Sciences* 13.9 (2023), p. 5395.

[15] Špela Čučko and Muhamed Turkanović. “Decentralized and self-sovereign identity: Systematic mapping study”. In: *IEEe Access* 9 (2021), pp. 139009–139027.

[16] Sara J Czaja and Chin Chin Lee. “The impact of aging on access to technology”. In: *Universal access in the information society* 5.4 (2007), pp. 341–349.

[17] Alona Dobshynska. “Analyzing and improving user experience in cryptocurrency applications”. In: *Scientific Research Journal* 12 (Aug. 2024), pp. 24–32.

[18] esatus. URL: https://esatus.com.

[19] Sarah P Everett. “The usability of electronic voting machines and how votes can be changed without detection”. PhD thesis. Rice University Houston, TX, 2007.

[20] Therese Fessenden. *Design Systems 101*. 2021. URL: https://www.nngroup.com/articles/design-systems-101/.

[21] World Economic Forum. *Reimagining Digital ID: Insight Report June 2023*. Tech. rep. World Economic Forum, 2023.

[22] Michael Fröhlich et al. “Blockchain and cryptocurrency in human computer interaction: a systematic literature review and research agenda”. In: *Proceedings of the 2022 ACM Designing Interactive Systems Conference*. 2022, pp. 155–177.

[23] Michael Fröhlich et al. “Don’t stop me now! exploring challenges of first-time cryptocurrency users”. In: *Proceedings of the 2021 ACM designing interactive systems conference*. 2021, pp. 138–148.

[24] Michael Fröhlich et al. “Is it better with onboarding? Improving first-time cryptocurrency app experiences”. In: *Proceedings of the 2021 ACM Designing Interactive Systems Conference*. 2021, pp. 78–89.

[25] Gataca. URL: https://gataca.io.

[26] *General Data Protection Regulation (GDPR) - official Legal Text*. 2020. URL: https://gdpr-info.eu/.

[27] Fariba Ghaffari et al. “Identity and access management using distributed ledger technology: A survey”. In: *International Journal of Network Management* 32.2 (2022), e2180.

[28] Jana Glöckler et al. “A systematic review of identity and access management requirements in enterprises and potential contributions of self-sovereign identity”. In: *Business & Information Systems Engineering* 66.4 (2024), pp. 421–440.

[29] Leonhard Glomann, Maximilian Schmid, and Nika Kitajewa. “Improving the blockchain user experience-an approach to address blockchain mass adoption issues from a human-centred perspective”. In: *International Conference on Applied Human Factors and Ergonomics*. Springer. 2019, pp. 608–616.

[30] Emily Gonzalez-Holland et al. “Examination of the use of Nielsenâs 10 usability heuristics & outlooks for the future”. In: *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*. Vol. 61. 1. SAGE Publications Sage CA: Los Angeles, CA. 2017, pp. 1472–1475.

[31] Morten Hertzum. “Images of usability”. In: *Intl. Journal of Human–Computer Interaction* 26.6 (2010), pp. 567–600.

[32] iGrant.io. URL: https://www.igrant.io/datawallet-for-eudi-wallet.html.

[33] Jo Rain Jardina et al. “Keyboard Shortcut Users: They Are Faster at More than Just Typing”. In: *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*. Vol. 53. 15. SAGE Publications Sage CA: Los Angeles, CA. 2009, pp. 975–979.

[34] Ali Kazerani, Domenic Rosati, and Brian Lesser. “Determining the usability of bitcoin for beginners using change tip and coinbase”. In: *Proceedings of the 35th ACM International Conference on the Design of Communication*. 2017, pp. 1–5.

[35] Alina Khayretdinova et al. “Conducting a Usability Evaluation of Decentralized Identity Management Solutions”. In: *Selbstbestimmung, Privatheit und Datenschutz : Gestaltungsoptionen für einen europäischen Weg*. Ed. by Michael Friedewald, Michael Kreutzer, and Marit Hansen. 2022, pp. 389–406.

[36] Maina Korir, Simon Parkin, and Paul Dunphy. “An empirical study of a decentralized identity wallet: Usability, security, and perspectives on user control”. In: *Eighteenth symposium on usable privacy and security (SOUPS 2022)*. 2022, pp. 195–211.

[37] Gabriella Laatikainen et al. “The State of Self-Sovereign Identity in Spring 2021: Results of a Survey”. In: *JYU Reports* 8 (2022).

[38] Crypto Research & Design Lab. *UX in Cryptocurrency: An overview of user experience in cryptocurrency applications*. Aug. 2022. URL: https://static1.squarespace.com/static/642ee3613ff85374fe5a01d1/t/645e6ac92d45f0635ec851fd/1683909329123/CRADL+Report+-+UX+in+Cryptocurrency.pdf.

[39] David M Lane et al. “Hidden costs of graphical user interfaces: Failure to make the transition from menus and icon toolbars to keyboard shortcuts”. In: *International Journal of Human-Computer Interaction* 18.2 (2005), pp. 133–144.

[40] Yorick Last and Patricia Arias-Cabarcos. “Vision: Towards True User-Centric Design for Digital Identity Wallets”. In: ().

[41] Jonathan Lazar, Jinjuan Heidi Feng, and Harry Hochheiser. *Research methods in human-computer interaction*. 2017.

[42] William Lidwell, Kritina Holden, and Jill Butler. *Universal principles of design: 100 ways to enhance usability, influence perception, increase appeal, make better design decisions, and teach through design*. 2003.

[43] Lissi. URL: https://www.lissi.id.

[44] Mick Lockwood. “An accessible interface layer for self-sovereign identity”. In: *Frontiers in Blockchain* 3 (2021), p. 609101.

[45] Stanislav Mahula, Evrim Tan, and Joep Crompvoets. “With blockchain or not? Opportunities and challenges of self-sovereign identity implementation in public administration: Lessons from the Belgian case”. In: *Proceedings of the 22nd Annual International Conference on Digital Government Research*. dg.o ’21. 2021, pp. 495–504.

[46] Markus Sabadello Drummond Reed Orie Steele Christopher Allen Manu Sporny Dave Longley. *Decentralized Identifiers (DIDs) v1.1*. 2025. URL: https://www.w3.org/TR/2025/WD-did-1.1-20250710/.

[47] Md Moniruzzaman, Farida Chowdhury, and Md Sadek Ferdous. “Examining usability issues in blockchain-based cryptocurrency wallets”. In: *Cyber Security and Computer Science: Second EAI International Conference, ICONCS 2020, Dhaka, Bangladesh, February 15-16, 2020, Proceedings 2*. Springer. 2020, pp. 631–643.

[48] Jakob Nielsen. *Usability engineering*. 1994.

[49] Calvin Nobles. “Stress, burnout, and security fatigue in cybersecurity: A human factors problem”. In: *Holistica Journal of Business and Public Administration* 13.1 (2022), pp. 49–72.

[50] Don Norman. *The design of everyday things: Revised and expanded edition*. 2013.

[51] OQTACORE. *UX/UI Design for Blockchain: Creating Seamless Web3 Experiences*. 2025. URL: https://blog.oqtacore.com/ux-ui-design-for-blockchain-web3/.

[52] Xiaoquan Pan. "Technology acceptance, technological self-efficacy, and attitude toward technology-based self-directed learning: learning motivation as a mediator". In: *Frontiers in Psychology* 11 (2020), p. 564294.

[53] Eduardo G Pinheiro et al. "On the contributions of non-technical stakeholders to describing UX requirements by applying proto-persona". In: *Journal of Software Engineering Research and Development* 7 (2019), pp. 8–1.

[54] Kevin Proudfoot. "Inductive/Deductive Hybrid Thematic Analysis in Mixed Methods Research". In: *Journal of Mixed Methods Research* 17.3 (2023), pp. 308–326.

[55] Alexander Rieger et al. "Not yet another digital identity". In: *Nature Human Behaviour* 6.1 (2022), pp. 3–3.

[56] Sebastian Sartor et al. "Love at First Sight? A User Experience Study of Self-Sovereign Identity Wallets." In: *ECIS*. 2022.

[57] Abylay Satybaldy. "Usability evaluation of SSI digital wallets". In: *IFIP International Summer School on Privacy and Identity Management*. 2022, pp. 101–117.

[58] Frederico Schardong and Ricardo Custódio. "Self-sovereign identity: a systematic review, mapping and taxonomy". In: *Sensors* 22.15 (2022), p. 5641.

[59] Mark Schneider, Ansgar Scherp, and Jochen Hunz. "A comparative user study of faceted search in large data hierarchies on mobile devices". In: *Proceedings of the 12th International Conference on Mobile and Ubiquitous Multimedia*. 2013, pp. 1–10.

[60] Martin Schrepp. *User experience questionnaire handbook*. 2023. URL: https://www.ueq-online.org/Material/Handbook.pdf.

[61] Daria Schumm, Katharina OE Müller, and Burkhard Stiller. "Are We There Yet? A Study of Decentralized Identity Applications". In: *arXiv preprint arXiv:2503.15964* (2025).

[62] Aiden Slavin. *Reimagining Digital ID*. 2023. URL: https://www.weforum.org/publications/reimagining-digital-id/.

[63] Reza Soltani, Uyen Trang Nguyen, and Aijun An. "A Survey of Self-Sovereign Identity Ecosystem". In: *Security and Communication Networks* 2021.1 (2021), p. 8873429.

[64] International Organization for Standardization (ISO). *ISO 9241-11:2018. Ergonomics of human-system interaction — Part 11: Usability: Definitions and concepts*. URL: https://www.iso.org/standard/63500.html.

[65] International Organization for Standardization (ISO). *ISO 9241-210:2019. Ergonomics of human-system interaction â Part 210: Human-centred design for interactive systems*. URL: https://www.iso.org/standard/77520.html.

[66] Jaime Teevan et al. "The perfect search engine is not enough: a study of orienteering behavior in directed search". In: *Proceedings of the SIGCHI conference on Human factors in computing systems*. 2004, pp. 415–422.

[67] Moritz Teuschel et al. "'Don't Annoy Me With Privacy Decisions!'—Designing Privacy-Preserving User Interfaces for SSI Wallets on Smartphones". In: *IEEE Access* 11 (2023), pp. 131814–131835.

[68] Kalman C Toth and Alan Anderson-Priddy. “Self-sovereign digital identity: A paradigm shift for identity”. In: *IEEE Security & Privacy* 17.3 (2019), pp. 17–27.

[69] European Union. *REGULATION (EU) 2024/1183 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL*. 2024. URL: `https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32024R1183`.

[70] validatedid. URL: `https://www.validatedid.com/en/identity/vidwallet`.

[71] Artem Voronkov, Leonardo A Martucci, and Stefan Lindskog. “System administrators prefer command line interfaces, don’t they? an exploratory study of firewall interfaces”. In: *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. 2019, pp. 259–271.

[72] Artemij Voskobojnikov et al. “The u in crypto stands for usable: An empirical study of user experience with mobile cryptocurrency wallets”. In: *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. 2021, pp. 1–14.

[73] Wenting Wang, Jinghui Cheng, and Jin LC Guo. “Usability of virtual reality application through the lens of the user community: A case study”. In: *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems*. 2019, pp. 1–6.

[74] Simon N Williams et al. “Public attitudes towards COVID-19 contact tracing apps: A UK-based focus group study”. In: *Health Expectations* 24.2 (2021), pp. 377–385.

[75] Razieh Nokhbeh Zaeem et al. “On the Usability of Self Sovereign Identity Solutions”. In: 2021.

Abbreviations

Dapps	Decentralised applications
DIDs	Decentralised Identifiers
EBSI	European Blockchain Services Infrastructure
EUDI	European Digital Identity
GDPR	General Data Protection Regulation
ISO	International Organisation for Standardisation
UEQ	User Experience Questionnaire
UX	User Experience
SSI	Self-sovereign Identity
VCs	Verified Credentials
W3C	World Wide Web Consortium

List of Figures

List of Tables

Listings

Appendix A

Semi-structured Interview Guide - First Round

Post-test Interview Guide

Overall experience comparison (three wallets)

Which of the three wallets felt the easiest to use? Why?

Which parts confused you the most? Can you give a specific example?

Was there any feature that made you feel especially secure? Was there anything that felt less safe?

Prototype-specific (design validation)

–Onboarding (Coach mark + Walkthrough)

When you first opened the wallet, did you understand what to do?

In the prototype, there were some prompts (for example, a walkthrough when establishing a connection). Did you find these helpful or distracting?

–Security and recovery (Recovery Phrase)

When you first saw the Recovery Phrase (seed phrase), what was your understanding? How would you call it in your own words?

In different wallets, the system asked you to confirm the recovery phrase in different ways:

Sequential clicking

Drag and drop fill-in-the-blank

Random word selection (prototype)

Which method was the easiest to understand? Which was the most difficult?

Did you hesitate or pause during the process? What happened at that moment?

If the wallet supported both passwords and biometrics, would you feel more secure, or would that feel unnecessary?

When the system displayed ”no reset from us”, what was your first reaction?

If you were to store important credentials here, what additional security measures would you like to have?

–Simplified interactions (QR code scan + image upload)

During the test, you encountered QR code scanning. Did you find it convenient?

In daily life, do you prefer scanning a QR code directly or sometimes uploading a saved

screenshot? Which is more convenient for you?

–Credential interface preference

Example 1: Grid layout (Lissi)

Example 2: Horizontal card scrolling (esatus)

Example 3: Vertical list (prototype)

Which one do you prefer? Why?–Terminology preference

In some apps, health cards, student IDs, and driver’s licenses are called credentials. Did you find

this word clear, or a bit abstract?

Were there any terms you found confusing the first time you saw them?

This app is called a wallet. What is your first impression when you hear that word?

Do you associate it more with a payment tool or a place to store documents?

If it were not called a ”wallet,” what other word do you think would be more suitable?

–Credential management

If your wallet contained a dozen credentials (health card, student ID, work certificate, etc.), how would you prefer to find them?

Would you like them to be automatically categorised, for example, into ”Health”, ”Education”, or ”Work”?

Have you ever had trouble finding a credential? At that time, what kind of support would you have wanted from the wallet?

Overall (skip some)

Based on today's experience, what do you think is the biggest strength of these apps?

What limitations did you notice?

What needs or challenges do you think these apps have not yet addressed well?

If you had to use one of these SSI wallets every day, what would worry you the most?

Closing

Is there anything important about your experience that we haven't asked?

If you could give one suggestion to the development team, what would it be?

Appendix B

Semi-structured Interview Guide - Second Round

Second Round Interview

Compared to your first experience, what is the biggest difference this time?

Which steps felt smoother? Were there any steps that were still error-prone or confusing? (Ask based on the actual situation)

If the wallet were to be improved, what areas would you like to see enhanced? Are there any new features you like added?

Is there anything we didn't ask that you think is important about your experience?

If you could give one suggestion to the development team, what would it be?

Appendix C

Pre-questionnaire

What is your gender? Female, Male, Prefer not to say

What is your age in years? 18-25, 26-35, 36-45, above 45

What is the highest degree or level of school you have completed? High school diploma or equivalent, Bachelor's degree, Master's degree, Doctorate

What is your current employment status? Employed, Student, Retired, Prefer not to say

Do you use Apple Pay, Google Pay, or an equivalent? (Y/N)

On average, how many hours per day do you use your smartphone? Less than 1 hour, 1-2 hours, 3-4 hours, 5-6 hours, More than 6 hours

How would you rate your tech-savvy on a scale of 1 to 5? (1=not tech-savvy, 5=very tech-savvy) (1,2,3,4,5)

Have you heard of Self-Sovereign Identity?
No, never
Yes, but I don't know what it means
I've heard the term and have some ideas
I know what it means, or have used an SSI wallet

How well do you understand the following terms on a scale of 1 to 5? (1=not at all, 5=very much) (1,2,3,4,5) Seed phrase, Verifiable credential, Decentralised identifier (DID)

Which terminology would you find more understandable? Seed phrase, 12-word backup code, Recovery key, Other (please specify)

Is the word "Credential" understandable to you?
Yes
Not sure
No, what would you prefer (please specify)

How much do you trust the following login methods on a scale of 1 to 5? (1=not at all, 5=very much) (1,2,3,4,5) Password

Biometrics (face ID)
Combination (password + biometrics)

How would you feel if your identity wallet had no password recovery via phone/email (only recoverable with a 12-word backup key)?
Very concerned
Acceptable with a clear warning
Totally fine with it
I don't understand what that means

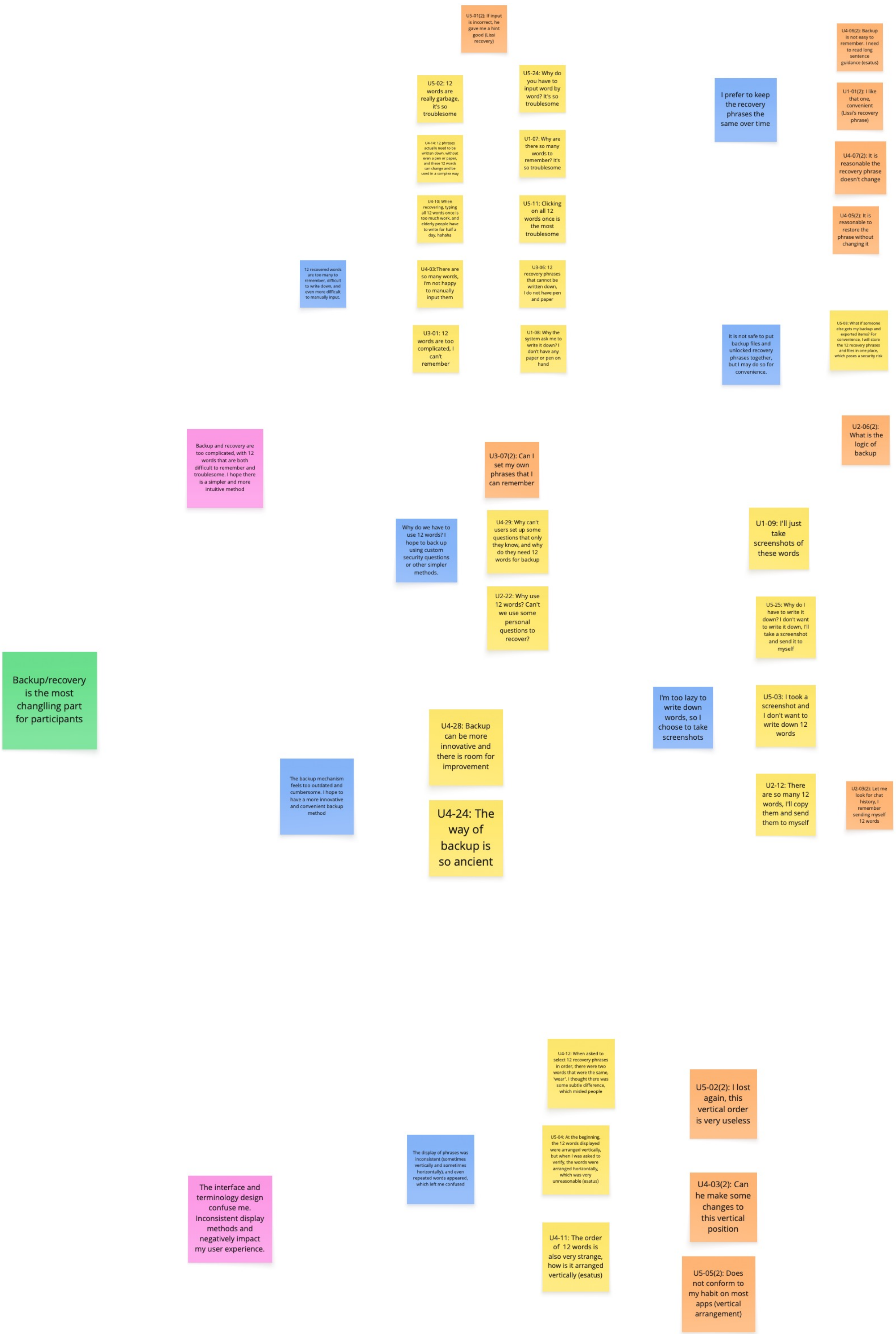
Which of the following features would be useful to you? (select all that apply)
Introductory animation explaining the wallet
Dual login (password + biometrics)
Early warning about no central recovery
Upload an image to scan the QR code from the same device
Credential categorisation (group by type)
Forced confirmation of seed phrase backup [seed phrase is a set of 12 words used to recover your wallet]
Other suggestions (please specify)

Which features are most important to you?
Security (e.g. login backup)
Comprehensibility (e.g. wording, animations, explanations)
User control (e.g. full ownership of data)
Ease of use (e.g. navigation, scanning)

Appendix D

Affinity Diagram

The following shows a summary of the affinity diagrams from both the first and second rounds of user testing.



Backup/recovery is the most changlling part for participants

12 recovered words are too many to remember, difficult to write down, and even more difficult to manually input.

U5-01(2): If input is incorrect, he gave me a hint good (Lissi recovery)

U5-02: 12 words are really garbage, it's so troublesome

U4-14: 12 phrases actually need to be written down, without even a pen or paper, and these 12 words can change and be used in a complex way

U4-10: When recovering, typing all 12 words once is too much work, and elderly people have to write for half a day. hahaha

U4-03:There are so many words, I'm not happy to manually input them

U3-01: 12 words are too complicated, I can't remember

U5-24: Why do you have to input word by word? It's so troublesome

U1-07: Why are there so many words to remember? It's so troublesome

U5-11: Clicking on all 12 words once is the most troublesome

U3-06: 12 recovery phrases that cannot be written down, I do not have pen and paper

U1-08: Why the system ask me to write it down? I don't have any paper or pen on hand

I prefer to keep the recovery phrases the same over time

U4-06(2): Backup is not easy to remember. I need to read long sentence guidance (esatus)

U1-01(2): I like that one, convenient (Lissi's recovery phrase)

U4-07(2): It is reasonable the recovery phrase doesn't change

U4-05(2): It is reasonable to restore the phrase without changing it

It is not safe to put backup files and unlocked recovery phrases together, but I may do so for convenience.

U5-08: What if someone else gets my backup and exported items? For convenience, I will store the 12 recovery phrases and files in one place, which poses a security risk

U2-06(2): What is the logic of backup

Backup and recovery are too complicated, with 12 words that are both difficult to remember and troublesome. I hope there is a simpler and more intuitive method

Why do we have to use 12 words? I hope to back up using custom security questions or other simpler methods.

U3-07(2): Can I set my own phrases that I can remember

U4-29: Why can't users set up some questions that only they know, and why do they need 12 words for backup

U2-22: Why use 12 words? Can't we use some personal questions to recover?

The backup mechanism feels too outdated and cumbersome. I hope to have a more innovative and convenient backup method

U4-28: Backup can be more innovative and there is room for improvement

U4-24: The way of backup is so ancient

I'm too lazy to write down words, so I choose to take screenshots

U1-09: I'll just take screenshots of these words

U5-25: Why do I have to write it down? I don't want to write it down, I'll take a screenshot and send it to myself

U5-03: I took a screenshot and I don't want to write down 12 words

U2-12: There are so many 12 words, I'll copy them and send them to myself

U2-03(2): Let me look for chat history, I remember sending myself 12 words

The interface and terminology design confuse me. Inconsistent display methods and negatively impact my user experience.

The display of phrases was inconsistent (sometimes vertically and sometimes horizontally), and even repeated words appeared, which left me confused

U4-12: When asked to select 12 recovery phrases in order, there were two words that were the same, 'wear'. I thought there was some subtle difference, which misled people

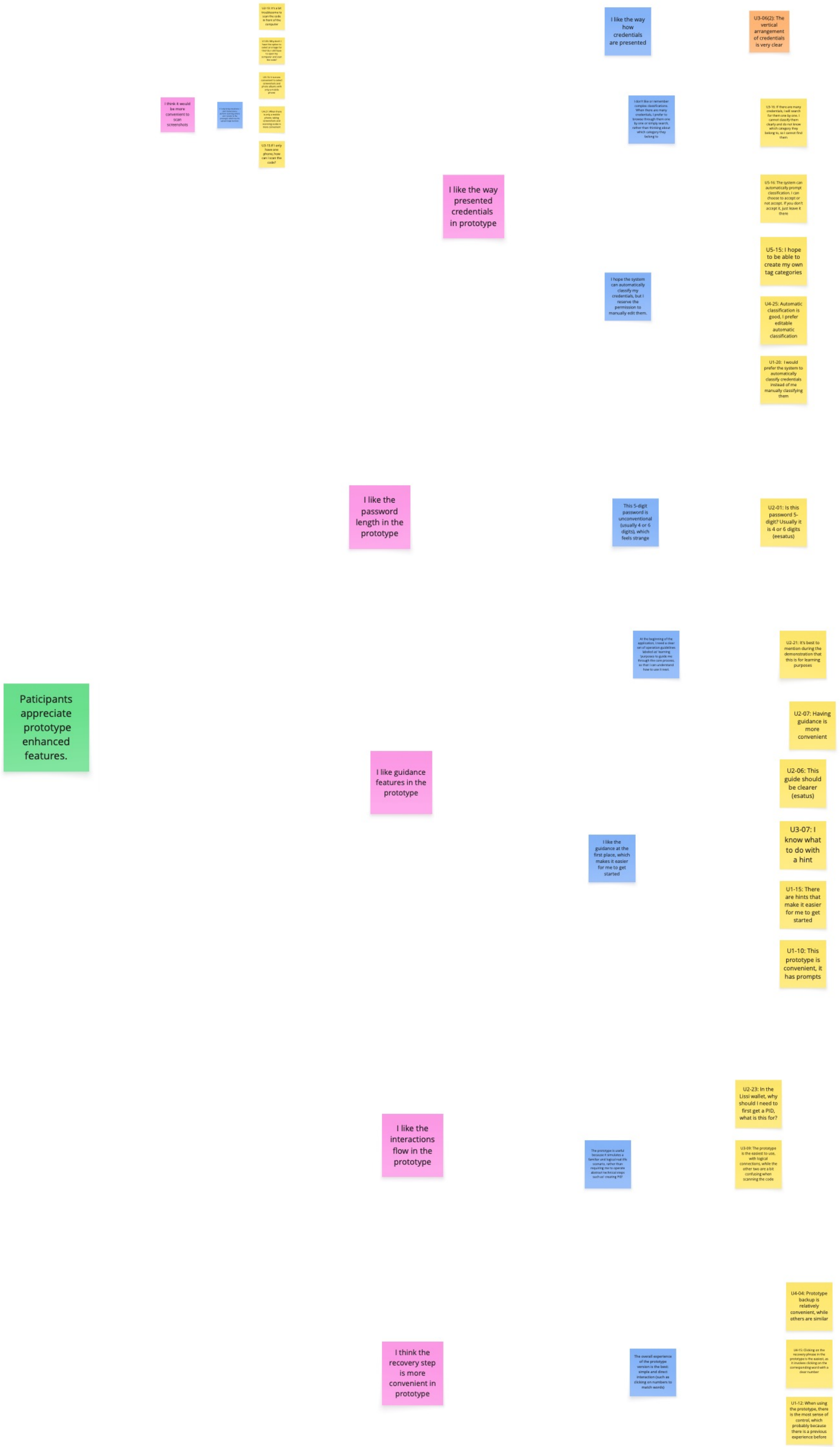
U5-04: At the beginning, the 12 words displayed were arranged vertically, but when I was asked to verify, the words were arranged horizontally, which was very unreasonable (esatus)

U4-11: The order of 12 words is also very strange, how is it arranged vertically (esatus)

U5-02(2): I lost again, this vertical order is very useless

U4-03(2): Can he make some changes to this vertical position

U5-05(2): Does not conform to my habit on most apps (vertical arrangement)



Paticipants appreciate prototype enhanced features.

I think it would be more convenient to scan screenshots

In daily living situations, I [illegible] perform scanning [illegible] the prototype, which has the upload image function

U2-13: It's a bit troublesome to scan the code in front of the computer

U1-06: Why don't I have the option to select an image for this? Do I still have to open my computer and scan the code?

U5-13: It is more convenient to select screenshots and photo albums with only a mobile phone

U4-21: When there is only a mobile phone, taking screenshots and scanning codes is more convenient

U3-15:If I only have one phone, how can I scan the code?

I like the way presented credentials in prototype

I like the way how credentials are presented

U3-06(2): The vertical arrangement of credentials is very clear

I don't like or remember complex classifications. When there are many credentials, I prefer to browse through them one by one or simply search, rather than thinking about which category they belong to

U3-16: If there are many credentials, I will search for them one by one. I cannot classify them clearly and do not know which category they belong to, so I cannot find them

I hope the system can automatically classify my credentials, but I reserve the permission to manually edit them.

U5-16: The system can automatically prompt classification. I can choose to accept or not accept. If you don't accept it, just leave it there

U5-15: I hope to be able to create my own tag categories

U4-25: Automatic classification is good, I prefer editable automatic classification

U1-20: I would prefer the system to automatically classify credentials instead of me manually classifying them

I like the password length in the prototype

This 5-digit password is unconventional (usually 4 or 6 digits), which feels strange

U2-01: Is this password 5-digit? Usually it is 4 or 6 digits (eesatus)

I like guidance features in the prototype

At the beginning of the application, I need a clear set of operation guidelines labeled as' learning 'purposes to guide me through the core process, so that I can understand how to use it next.

U2-21: It's best to mention during the demonstration that this is for learning purposes

U2-07: Having guidance is more convenient

U2-06: This guide should be clearer (esatus)

I like the guidance at the first place, which makes it easier for me to get started

U3-07: I know what to do with a hint

U1-15: There are hints that make it easier for me to get started

U1-10: This prototype is convenient, it has prompts

I like the interactions flow in the prototype

The prototype is useful because it simulates a familiar and logical real-life scenario, rather than requiring me to operate abstract technical steps such as' creating PID'

U2-23: In the Lissi wallet, why should I need to first get a PID, what is this for?

U3-09: The prototype is the easiest to use, with logical connections, while the other two are a bit confusing when scanning the code

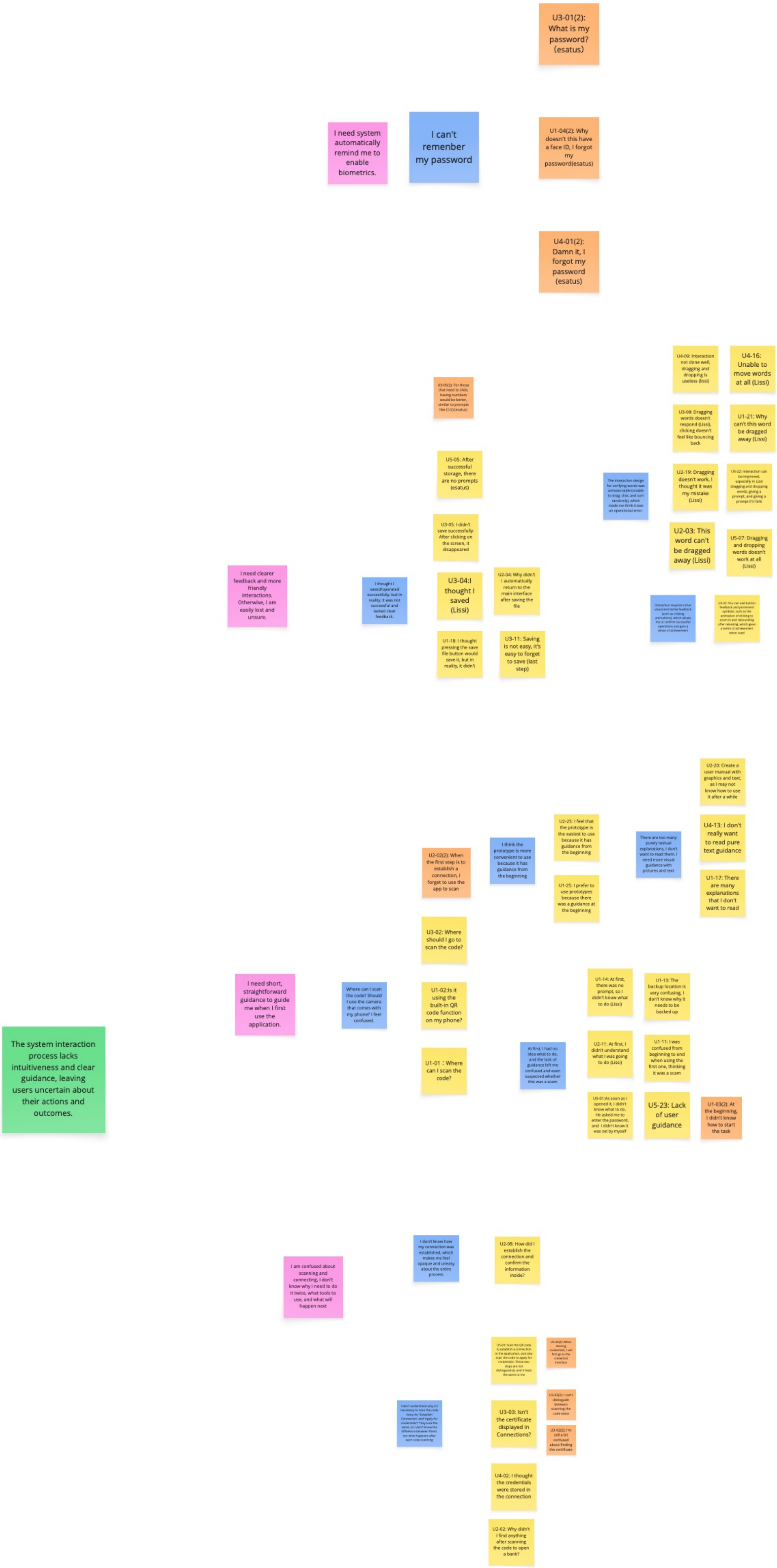
I think the recovery step is more convenient in prototype

The overall experience of the prototype version is the best: simple and direct interaction (such as clicking on numbers to match words)

U4-04: Prototype backup is relatively convenient, while others are similar

U4-15: Clicking on the recovery phrase in the prototype is the easiest, as it involves clicking on the corresponding word with a clear number

U1-12: When using the prototype, there is the most sense of control, which probably because there is a previous experience before



The system interaction process lacks intuitiveness and clear guidance, leaving users uncertain about their actions and outcomes.

I need system automatically remind me to enable biometrics.

I can't remember my password

U3-01(2): What is my password? (esatus)

U1-04(2): Why doesn't this have a face ID, I forgot my password(esatus)

U4-01(2): Damn it, I forgot my password (esatus)

I need clearer feedback and more friendly interactions. Otherwise, I am easily lost and unsure.

I thought I saved/operated successfully, but in reality, it was not successful and lacked clear feedback.

U3-05(2): For those that need to slide, having numbers would be better, similar to prompts like (1/2) (esatus)

U5-05: After successful storage, there are no prompts (esatus)

U3-05: I didn't save successfully. After clicking on the screen, it disappeared

U3-04:I thought I saved (Lissi)

U2-04: Why didn't I automatically return to the main interface after saving the file

U1-18: I thought pressing the save file button would save it, but in reality, it didn't

U3-11: Saving is not easy, it's easy to forget to save (last step)

The interaction design for verifying words was unreasonable (unable to drag, click, and sort randomly), which made me think it was an operational error.

U4-09: Interaction not done well, dragging and dropping is useless (lissi)

U4-16: Unable to move words at all (Lissi)

U3-08: Dragging words doesn't respond (Lissi), clicking doesn't feel like bouncing back

U1-21: Why can't this word be dragged away (Lissi)

U2-19: Dragging doesn't work, I thought it was my mistake (Lissi)

U5-22: Interaction can be improved, especially in Lissi dragging and dropping words, giving a prompt, and giving a prompt if it fails

U2-03: This word can't be dragged away (Lissi)

U5-07: Dragging and dropping words doesn't work at all (Lissi)

Interaction requires richer visual and tactile feedback (such as clicking animations), which allows me to confirm successful operations and gain a sense of achievement

U3-22: You can add button feedback and prominent symbols, such as the animation of clicking to zoom in and rebounding after releasing, which gives a sense of achievement when used

I need short, straightforward guidance to guide me when I first use the application.

Where can I scan the code? Should I use the camera that comes with my phone? I feel confused.

U2-02(2): When the first step is to establish a connection, I forget to use the app to scan

U3-02: Where should I go to scan the code?

U1-02:Is it using the built-in QR code function on my phone?

U1-01：Where can I scan the code?

I think the prototype is more convenient to use because it has guidance from the beginning

U2-25: I feel that the prototype is the easiest to use because it has guidance from the beginning

U1-25: I prefer to use prototypes because there was a guidance at the beginning

There are too many purely textual explanations, I don't want to read them. I need more visual guidance with pictures and text

U2-20: Create a user manual with graphics and text, as I may not know how to use it after a while

U4-13: I don't really want to read pure text guidance

U1-17: There are many explanations that I don't want to read

At first, I had no idea what to do, and the lack of guidance left me confused and even suspected whether this was a scam

U1-14: At first, there was no prompt, so I didn't know what to do (Lissi)

U1-13: The backup location is very confusing, I don't know why it needs to be backed up

U2-11: At first, I didn't understand what I was going to do (Lissi)

U1-11: I was confused from beginning to end when using the first one, thinking it was a scam

U5-01:As soon as I opened it, I didn't know what to do. He asked me to enter the password, and I didn't know it was set by myself

U5-23: Lack of user guidance

U1-03(2): At the beginning, I didn't know how to start the task

I am confused about scanning and connecting, I don't know why I need to do it twice, what tools to use, and what will happen next

I don't know how my connection was established, which makes me feel opaque and uneasy about the entire process

U2-08: How did I establish the connection and confirm the information inside?

I don't understand why it's necessary to scan the code twice for 'Establish Connection' and 'Apply for credentials'? They look the same, so I don't know the difference between them, nor what happens after each code scanning

U5-09: Scan the QR code to establish a connection in the application, and also scan the code to apply for credentials. These two steps are not distinguished, and it feels the same to me

U5-06(2): When sharing credentials, I will first go to the credential interface

U3-03: Isn't the certificate displayed in Connections?

U3-03(2): I can't distinguish between scanning the code twice

U3-02(2): I'm still a bit confused about finding the certificate

U4-02: I thought the credentials were stored in the connection

U2-02: Why didn't I find anything after scanning the code to open a bank?

User lack trust and feel insecure with the applications

I lack confidence in the security of the system and am worried about being hacked, lacking official endorsement, or having too simple verification

I don't believe I can truly control my data, I feel like all the data is being monitored.

U3-13: I prefer central storage, I don't believe I have autonomous control over data, it's definitely all monitored

U4-02(2): Now I am quite wary of QR codes, anti fraud. What if this is not official

The bank/institution issuing credentials too quickly and the process is too simple, which makes me feel insecure and unreal.

U3-20: This application is easy to apply and there aren't many steps in between. But in real world, some data cannot be downloaded directly, such as bank statements, and the actual operation process of the bank app is very complicated

U4-08: I don't think it's very safe. The bank gave the credentials too quickly

U4-07: The process is too simple, but in reality, banks require a lot of authentication, which gives me a greater sense of security

I need stronger security measures, such as double authentication for important operations.

U4-20: I hope more security measures can be provided, and some documents can be encrypted twice, especially when operations involving money

U2-15: There was no double check during sharing

U2-10: If the deletion operation involves biometric recognition, I think it's safer

I am worried about data security, afraid of being stolen by hackers, afraid of insufficient abilities of application developers, and afraid of not having official endorsement

U4-27: If there is an official endorsement, I would feel safer, otherwise what if the data is lost and cannot be found

U2-16: If I didn't remember the 12 words, it would be terrible. If I lost them, I wouldn't be able to find them back

U4-17: Having a password is enough, no need for facial recognition

U2-17: There is no fallback plan

U4-01:I don't really like using facial recognition because I'm afraid of information leakage

U4-18: Facial recognition will upload my personal information, and I think this step is about entering my personal information

U3-19: I'm worried about hackers stealing data. How can we ensure security?

U5-20: I am very concerned about the abilities of those who create such applications

Dual authentication (password+biometric) makes me more at ease

U5-12: Facial recognition is good, since passwords are often forgotten and there is a risk of being seen when entering them

U3-14: The combination of password and biometric information is a better way to log in

U1-16: I feel more at ease with dual authentication

Future Work

I feel some operations are easy and smooth to complete, and I am more familiar with them for the second time.

I feel like I am more familiar with the system

The process of deleting credentials was very smooth and a good experience.

U2-09: The operation of deleting credentials went smoothly

U5-03(2): All steps have become smoother

U2-07(2): Overall, it feels much smoother than the first time

U4-03(2): Overall, it feels smoother than before

U1-03(2): It feels smoother than the first time

U3-06(2): Backup and save files more smoothly

The process of scanning the code went smoothly, which gave me a great sense of achievement.

U3-10: Scan the code smoothly, with a strong sense of achievement

U4-06: Scan the QR code is smooth

If this application can connect to countless third-party services, then I won't have to carry many physical cards with me

U5-13: If the application can provide third-party services, I don't have to carry a bunch of cards

I believe this application is a good way to protect my personal privacy in the future

U2-24: I believe that such applications can better protect my privacy

I like that the system protects my privacy, but I worry that connecting different systems and getting all parties to cooperate could make it difficult to use in reality.

I'm worried that connecting different systems is a big project that will be difficult to implement.

U4-30: Although this type of application can better protect my privacy, I feel that it is not easy to promote in reality

U3-15: [illegible] cooperation [illegible] institutions [illegible]. Only when all institutions reach cooperation [illegible]

U5-21: It is difficult to connect many systems in various scenarios, which is a huge project

U4-15: I feel that this type of application is not very convenient to use in real-world, it needs a lot of cooperations

Protecting privacy is undoubtedly an advantage, but as long as the application is convenient enough, I don't really mind exposing a part of my privacy.

U1-26: [illegible] the advantage of this type of application is to protect [illegible], but I don't really mind exposing my privacy as long as it's easy to operate

[illegible]

[illegible]

It would be great if the application could provide photos of the front and back of the documents to [illegible] of submitting photo [illegible]

[illegible]

U2-04(2): Can you add some sharing attributes, such as showing off that I graduated and sharing them on social media

U2-05(2): They are all personal interactions with third parties, is it possible for there to be communication between individuals

I hope credentials can be managed and invoked more intelligently, supporting more scenarios.

I hope my digital credentials to be recognized and used offline, such as scanning the code directly during [illegible] verification, [illegible]

U2-18: Can only be done online? Can it be used as an offline credential

U5-17: We hope that third parties can recognize the documents in the wallet and have the same effect

U3-17: If I can't find my ID card while taking the train, it would be nice if I can just scan the code on the phone to verify it

I hope the types of digital credentials can expand infinitely to cover all life scenarios, like Disney tickets, hotel membership cards, etc.

U5-21: The types of cards that can be included can be broader, such as Disney cards and hotel membership cards

I want to swith to my monther language

U1-03: Why isn't there a Chinese option for language switching?

Exclude

After scanning the code, I was redirected to a webpage and didn't know what to do next. The process was interrupted

U1-05: How did I jump to this webpage after scanning the code? What should I do next? (Lissi)

U2-05: Why did it redirect to the webpage?

U3-12: How did I jump to the webpage after scanning the code (Lissi)

U4-05: How did you jump to a webpage after scanning the code (Lissi)

U5-06: Lissi will jump to the web page when using it, which is not very user-friendly

I feel like the system is slow and I don't really want to use it

U1-04: The loading speed is too slow

U1-19: The speed is too slow and I don't really want to use it

U4-23: It is inevitable to interact with third parties, and the speed is worrying

Terminology

We have different understandings and preferences for terminology

U2-14: I think using 'wallet' has more financial attributes and tends to use 'credential'

U5-14: Using wallet is too narrow and there are also degree certificates, but using credential is great. Wallet feels like an economic transaction that involves linking many bank cards and having a balance to deposit and spend money.

U3-22: Wallet is more like a bank card or transportation card with payment functions. I think using 'credential' is also abstract, so I would choose the word 'card'

U3-23: Credential is a bit abstract, I tend to prefer wallet

U5-04(2): In Contacts, it should be a single record, but now he gave it to me, and I gave him two records. I think the connection is more reasonable

U5-10: For these 12 recovery phrases, I may refer to them as keys