Pre-Prototype Testing: Empirical Insights on the Expected Usefulness of Decentralized Identity Management Systems

Nadine Ostern
Frankfurt School of Finance & Management
n.ostern@fs.de

Johana Cabinakova
Goethe University Frankfurt
johana.cabinakova@stud.uni-frankfurt.de

Abstract

Decentralized identity management systems (IMSs) are envisaged to decrease fraud, enhance users' privacy and introduce transparency to the rather opaque business with personal data. Given these quite desirable features it is not surprising that many whitepapers discuss the technical feasibility of decentralized IMSs. What is missing, however, is the consideration of actual user requirements and their assessment of the decentralized IMS's ability to actually protect their privacy. We provide insights on the perceived usability of decentralized IMS features as well as on user concerns and requirements. The result of this study is a trigger for further and iterative usability testing that takes up the insights provided by this study. The result suggests that the usability of decentralized IMSs is not as straightforward as presumed by many companies and that a good deal of work is necessary to identify and implement actual user requirements into a functioning prototype.

1. Introduction

Since the introduction of Facebook in the year 2004, the social network has become one of the basic tools for and a mirror of online social interaction, personal identity, and networking. To offer these kind of services, social networks deeply penetrate their users' life by collecting and analyzing personal information, not only to know who their users are but also to sell 'truthful data' to advertisers [1], [2]. By revealing personal information on social networks, users, thus, accept significant risks to their privacy induced by the change of the relationship between public and private spheres [2].

Facebook and online social networks in general, favor the idea of people having transparent identities that are disclosed online, by releasing habitual behavioral data and personal information in the process of socializing [1]. However, these interest of owner may run counter to users' need to differentiate between various online identities, which is the attempt to self-manage and protect personal data through only partial or non-disclosure of personal information and associated characteristics [1].

Perennial privacy incidents fuel users' demand for increased protection of their privacy. Most recently, user data of Facebook were inadmissibly shared with the data analysis company Cambridge Analytica, leading to a wave of membership withdrawals and the claim for better privacy practices [3], [4]. Thereby, the answer to users' demand is probably not the design of better privacy practices and/or the introduction of new privacy protection mechanisms on yet centralized identity management systems (IMSs) such as Facebook or other online social networks [4]. This is because, using centralized IMSs, personal information is not under control of the individual and lives in repositories that are targets for hackers and identity theft [5], [6]. In 2017, the Identity Theft Resource Center recorded 1,339 breaches impacting over 170 million records on identity in the U.S. alone [7].

As an alternative, decentralized IMSs based on blockchain technology were recently proposed as a solution to privacy issues in centralized IMSs. Blockchain technology enables decentralized identity management, where credentials are cryptographically secured on personal digital wallets, with which an individual can securely prove its identity, while controlling how many and what kind of information is shared with whom [7]–[9]. Thus, several benefits are expected to emerge from a decentralized IMS, including increased security, enhance privacy as well as control over personal information and identifier through the identity owner [8], [10].

The following paper evaluates the expected usefulness of a decentralized IMS based on blockchain technology using a pre-prototype testing as proposed by [11]–[13]. Pre-prototyping is necessary since to date, no functioning prototype of a blockchain-based, decentralized IMS is existent and has shown feasibility of envisaged features, including privacy protection. However, several whitepapers exist that present the

URI: https://hdl.handle.net/10125/59623
ISBN: 978-0-9981331-2-6

planned development of a decentralized IMS, by describing among others the technical architecture, relevant functionalities, and potential user interfaces (e.g. [10], [14]). While the technical implementation is discussed controversially, a user perspective in terms of usability testing is frequently omitted in these whitepapers. Neither there is a concrete usability test assessing true user requirements nor is there any usability test envisaged for future research attempts. Overall, whitepapers rather describe a user perspective on decentralized IMSs, but do not assess real requirements. In order to close this gap and following the recommendations of [13], we state the following two research question:

RQ1: *Which features of a decentralized identity management system will be perceived as useful by target users?*

RQ2: *How do target users assess the ability of decentralized identity management systems to sufficiently protect their privacy?*

Using self-developed and guided animations that illustrate the features of a decentralized IMS as well as images of the endeavored user interface, a qualitative study is conducted to assess the expected usefulness of a decentralized IMS as well as users' expectations on decentralized IMS's ability to actually protect their on privacy. The results of this study lead to rather surprising insights that emphasize the necessity to identify and take care of discrepancies between specified and actual user requirements on decentralized IMSs.

The remainder is structured as follows: In the following section, the general functionalities of two different types of IMSs – centralized and decentralized IMSs- will be explained. Given the novelty and early stage development of decentralized IMSs, a qualitative, research approach is chosen to assess the expected system usability by conducting semi-structured interviews with 11 interview partners. The results are discussed subsequently and used to recommend improvements on the features of decentralized IMSs. Furthermore, we provide insights on the most preferred application scenarios of decentralized IMSs as well as concerns of interviewees towards the usability of and privacy issues within decentralized IMSs. Finally, a conclusion and outlook is provided that highlights further research opportunities.

2. Identity Management Systems

Internet continuously opens up new opportunities to use a number of different services involving all kind of actors (consumers, businesses and governments). Along with this development, there is a continuously increasing need for reliable online identity authentication [15]. Identity management systems (IMSs) are designed to help manage users identities across multiple systems and services by providing authentication, together with identification and authorization [16], [17]. Two larger classes of IMSs exist that are either centralized or decentralized. Broadly speaking, the two classes of IMSs differ with respect to the number of identity providers as well as in their relationship between the service provider and the relying party. Centralized IMS have a single identity provider and require a relationship between the provider and the relying party to be established in advance. In contrast, decentralized IMSs have more than one identity provider and need no shared protocols to exchange identities and assertions of authorization between the provider and the relying party [18].

Most recently, a new type of a decentralized IMS was proposed that is based on blockchain technology. Blockchain technology was initially introduced in the context of the cryptocurrency Bitcoin, which is a decentralized payment system, based on a peer-to-peer network and cryptographic proof. A blockchain is loosely speaking a distributed databased that is secured by cryptographic proof and a Merkle tree, which (under certain circumstances) enables immutability of all entries made on the blockchain [19]. Despite immutability, blockchains provide a considerable high level of transparency over entries made in the ledger, which allows traceability of pseudonymous nodes in the peer-to-peer network [20]. Application possibilities of blockchain technology go far beyond the initially supposed financial sector. Applied as foundational technology for the realization of decentralized IMSs, blockchains are expected to increase security of personal data and users privacy as well as to reduce fraud with digital identities [7], [9]. In the following, differences between centralized IMSs as well as a decentralized IMS based on blockchain technology (in the following: *decentralized IMS*) are briefly explained.

2.1 Centralized Identity Management

Using centralized identity management systems, service provider must itself understand, verify and accept user's credential [17]. Users are usually equipped with one or more credentials, which are for this purpose presented to the service provider. Currently most online service providers use for their identity management registrations a username and/or password-based system [15]. However, the usage of such systems might be upsetting for some users, as it requires to create and to remember a lot of different passwords each time he or she decides to use a new service [15].

Solutions for these problems provide so called federated IMSs [15]. Federated identity management allows individuals to use the same form of personal identification (e.g. user name, password or others) to sign on to the networks of more than one enterprise in order to conduct different transactions [21]. In a federated IMS, service providers depend on each other in order to successfully authenticate the respective users and vouch for their access to services. [21]. This enables companies to share applications without a need to adopt the same technologies for directory services, security and authentication [21]. Within companies, directory services allow companies to recognize their users through one single identity [21]. As for companies it is not easy to match up technologies or maintain full user accounts for their partners' employees, federated IMSs allow companies to keep their own directories and securely exchange information from them [21]. Especially in e-business scenarios, federated identity management is used to connect enterprises along the value chain and to enable a significant reduction of their transaction costs [17].

Single sign-on (SSO) is a specialized form of software authentication that enables a user to authenticate once and gain access to the resources of multiple software systems [21]. SSO is a session/user authentication process that permits a user to enter one name and password in order to access multiple applications. Thus, the SSO is one form of a centralized IMS [21]. The process authenticates the user for all the applications they have been given rights to and eliminates further prompts when they switch applications during a particular session [21].

Despite several advantages of centralized IMSs, problems of hitherto existing IMSs are also diverse. Despite security issues with single-sited identity silos, developers of centralized IMSs certainly struggle with many stakeholders and conflicting requirements between identity providers and users [18]. Moreover, the rapid increase in uptakes of digital services has led to serious negative effects on the user experience using IMSs that apply this rather traditional approach to identity management. The industry and, especially, startups have responded to these developments by proposing new identity management models [22].

2.1 Centralized Identity Management

In the following a decentralized IMS is introduced, which’s technical backbone constitutes a blockchain. Despite there are further types of decentralized IMSs, blockchain-based decentralized IMSs (in the following: decentralized IMS) gained growing public attention given several expected benefits compared to existing centralized and decentralized IMS solutions [7], [8].

One of the most obvious – and most emphasized – expected benefits of using a decentralized IMS is the ownership and control of data by the identity owner [9]. To this end, identity owners need to store their identifier on the blockchain along with a decentralized identifier (DID) document containing the public key for the DID, any other credentials the identity owner wants to disclose and a network address for interaction. The identity owner controls the DID document and the associated private key [10]. Because every DID has an associated public-private key pair, anyone with a DID should be able to digitally issue and sign verifiable claims and other documents. Thus, users are not required to trust any third-party and are always aware of the data that is being collected about them and how it is used by third parties [8]. In order to build trust in the users’ identity, identity owners probably need to work with other issuers of verifiable claims [10], [23].

Decentralized IMS are as well envisaged to enhance the identity owners’ privacy [8]. This is because decentralized IMSs are expected to provide so-called disclosure proofs. Disclosure proofs enable the owner of personal data to bundle claims and use it as DID, without disclosing unnecessary information about the subject [8], [10]. Certainly, a decentralized IMSs requires a permission-less blockchain architecture, meaning that everyone can participate on solving the consensus algorithm that serves as validation for personal information [10]. Consequently, the blockchain is envisaged to be user-owned and not governed by any central authority. Users should own and control their data without compromising security or limiting companies’ and authorities’ ability to provide personalized services [8]. Personal data, and sensitive data in general, are expected to be more prone to attacks and misuse if they are given to third parties [8], thus, decentralized IMSs are expected to be more secure than other and, especially, centralized IMSs.

It has to be said that these benefits are primary expectations: To the best knowledge of the authors – to date – no prototype of a decentralized IMS exists that proofs the feasibility of the envisaged functioning of the decentralized IMS as well as its advantageousness compared to other solutions. Several whitepapers and start-ups, however, document the vision and planned development of decentralized IMSs towards a functioning prototype [10], [24]–[26]. A revision of the corresponding whitepapers and technical papers revealed, however, that a lot of discussion is made up around the technical feasibility of certain features, while a user perspective on the envisaged decentralized IMS and especially usability testing, is continuously missing. Following [13], we suppose that for a successful development not only the implementation of particular features, but also the correctness of codes must be ensured: Diminishing the discrepancy between specified and actual user requirements is of particular importance for the successful development of a decentralized IMS. Thus, in the following an iterative process of several rounds of pre-prototype testing is triggered that aims at capturing actual users' (and future identity owners') requirements to ensure usability of the decentralized IMS and to guarantee a successful prototype development.

3. Methodology

Given the early stage of research on decentralized IMSs, we conducted a qualitative study in order to capture all information relevant to determine the usability and the users' assessment of the decentralized IMS's ability to ensure privacy. Interviews with potential users of decentralized IMSs were conducted to assess the expected usability of such systems and to test whether or not further features must be implemented to fulfill actual user requirements. The results of this study provide the basis for the first step of an iterative design process, inspired by the design science research methodology (e.g. [27], [28]).

3.1 Guidance through the Pre-Prototype

To date, no prototype of a decentralized IMS exists that can be used for a hands-on usability testing. Whitepapers that are concerned with decentralized IMSs, however, provide a rich source of information on how the technical architecture and functionalities of such an IMS are envisaged [10], [24], [26], [29]. Furthermore, some whitepapers also include an illustration of a proposed user interface of the decentralized IMS [10]. We used this rich source of information to develop a short animation that guides interview participants through relevant features of the decentralized IMS. Interview participants first received basic information about the general functioning, including technological background information. In the animation the participants we're then entrusted with the functionality of interactions of a decentralized IMS user named Alf with his bank, his local government and his potential employer. Figure 2 represents an excerpt of the animation showing Alf's view of his identity. The participants were also informed that Alf's identity doesn't really exist as depicted but that the view is mainly a virtual representation and Alf's identity represents the collection of all of his identifiers, claims, disclosures, and proofs stored on a ledger (blockchain).

Furthermore, a user interface was developed that shows how such a decentralized IMS could look and to explain how it can be used from a practical point of view (Figure 2). Our animation and the user interface were mainly inspired by a decentralized IMS proposed by the Sovrin foundation, which provides a whitepaper with an in-depth technological explanation of all features of the decentralized IMS [10] (Figure 1). The level of detail was the main reason to draw upon Sovrin's vision of the decentralized IMS.

Interview partners were led through the animation and the user interface in the presence of the respective interviewer. Subsequent questions on the features of the presented IMS were asked to ensure that participants understood the features and, thus, can assess the expected usability of the IMS adequately.

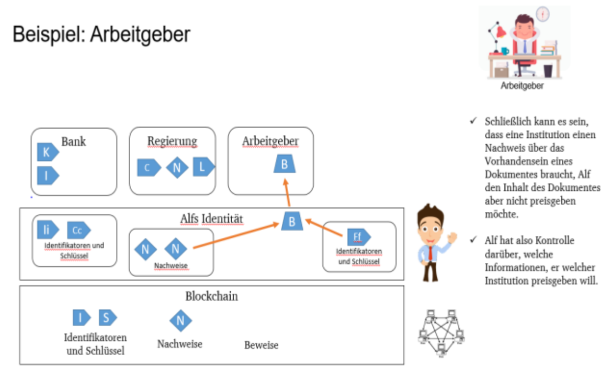

Figure 1. Screenshot of the guided animation through the decentralized IMS#

Figure 2. Mock-up of a decentralized IMS user interface

3.2 Data Collection and Theoretical Sampling

To assess the usefulness of the decentralized IMS, semi-structured interviews were conducted with 11 participants (4 males, 7 females). The average age was 31,8 years and participants were rather well educated, with more than the half of the sample having a master's degree or higher.

Given the fact that decentralized IMSs are envisaged to reach widespread user acceptance, we regard everyone, who was willing to participate in the study as an eligible interview partner. Nevertheless, we tried to select our participants purposefully regarding their age (the participants' age of this study range from 20 to 57 years), their gender, and their educational level (participants of study possess baccalaureate up to Ph.D.). This approach ensures that we will cover different perspectives on the usefulness the decentralized IMS.

Interviews were conducted following a coarse interview protocol as shown in the Appendix. Open questions were developed in the accordance with the Survey Design and Methodology (SDM) Guidelines for open questions proposed by the Leibniz Institute for Social Sciences [30] and discussed multiple times by the authors. All interviews were recorded and transcribed by the respective interviewer. During the interviews, all participants showed a general understanding of what an IMS does and indicated that they had already used a centralized IMS either for personal purposes (registering for a digital service) or because of work.

3.2 Data Analysis

For the analysis of the interviews, an open coding approach was used, which is recommended as method that is especially appropriate for analyzing early-stage qualitative data [31]. In particular, open coding allows the researcher to recognize similar patterns in the data and to analyze different meanings easily [31], [32]. Give the likewise early-stage research on the pre-prototype of a decentralized IMS, this approach seemed most appropriate to the authors.

The open coding process follows three distinct steps [31], [33]: In a first step, a database was created that contains the raw text data from the interviews and supplants the original text during the following analysis. Patterns in the data were identified in a second step by identifying more than once occurring combinations of conditions and outcomes [31], [32]. A powerful tool for pattern recognition is to define codes and identify distinct but qualitatively different states of these codes. Subsequently, these combinations of codes and states are labeled as themes [32]. Lastly, patterns that are not significantly different are integrated into another that finally allows contingent generalization [32], [34]. During that process, the authors frequently discussed open questions and feedback that led to new ideas and the adjustment of the interview protocol.

4. Results

The results of the qualitative study are presented in the following. Results are clustered in five thematic blocks covering different aspects of the usefulness of the decentralized IMS as well as needs for improvement that should be considered and implemented for further pre-prototype testing.

4.1 Evaluation of Decentralized IMS Features

Participants statements on questions regarding their assessment of the usefulness of the introduced features of the decentralized IMS are presented in Table 1. Moreover, exemplary statements of interviewees are shown. As obvious from the table, the majority of participants indicated that they perceive the control over data that is disclosed to other as the most useful feature provided by the decentralized IMS. Control over data was mentioned by 72% of all participants (P). Additionally, data ownership was a topic that was mentioned by 32% of participants. The ability to not pass actual information to institutions or companies was seen as a major advantage of decentralized IMS. Using a decentralized IMS, participants were thus aware that they are able to send disclosure proofs, without sending the actual data, like an ID or certified documents. Closely linked to data ownership is the feature of representation, as named by 9% of all participants. Actually, the ability that digital proofs are enough for representation and authentication of a person in an online environment is a prerequisite for ownership of personal data.

Lastly, participants emphasized that the transparency induced by the decentralized IMS is a feature that is seen as useful by 27% of the participants. The transparency introduced by the decentralized IMS was though interpreted in two different ways by the participants. On the one hand, participant understood transparency as a feature that enables the users of a decentralized IMS to see which and how many personal data is requested by any other party, e.g. a service provider or an institution (as stated in the table). On the other hand, some participants showed a more far-reaching understanding of transparency, emphasizing that they would like to see which and how many information a company already possess about oneself. Notably, this feature was not explicitly illustrated in the animation of the decentralized IMS, but could be suspected from the user interface, providing an overview on information shared with any other party.

Table 1. Evaluation of Functionalities

Feature	Exemplary Statements	%
Control over data	"*I think that especially the ability to control the disclosure of my personal data is an important function. Today, I don't know which data are passed on to other firms or which additional information exist about me as a person. Several times I used the Facebook Authentication mechanism, because it is fast, but actually, I don't know what kind of data and information are transferred*". [P5] "*Overall, I think, that control over my data is the most important feature*" [P8]	72
Data ownership	"*Very useful is that data remain by myself and when I understand it correctly, institutions or companies with whom I interact only receive the information that these data actually represent me."* [P11] *"I think it is very useful that data remain by myself, because then I can control them. It is good that data about my identity don't lie on a server of any third party that can be attacked*" [P5]	32
Transparency	"*I use regularly the IMS with which I can register with my Google or Facebook account. Often I don't care which information is passed to the other service from Google or Facebook. But generally, it would be interesting to see, how many and what kind of data is requested by services for registration and usage*". [P11]	27
Representa -tion	"*It is very useful that services or companies that want to have information about myself only receive a proof that data actually represent me, but do not get the actual data about me*". [P1]	9
Only-once Verification	"*I think that such a system is useful in particular if there is no need to proof the accuracy and correctness of documents every time that I use them. Information must be verified once on the blockchain and can used repeatedly*." [P2].	9

4.2 Benefits and Concerns

Practicability and the potential to save time when using a decentralized IMS were mentioned as very important benefits that are even pivotal when it comes to the decision whether or not to use a decentralize IMS [P4, P6, P10]. Especially, they rated the ability of the system to verify a document once and use it multiple times without further need of verification as very useful. However, participants also recognize that the ability to control the disclosure of data, might be a feature that hinders the practicability of the IMS. For instance, participant 2 stated: "*I think it is important to know how many work it needs to decide which data are disclosed to whom. Does I need to decide the disclosure of my data every single time or will there be general rules that I can set, such that it works automatically?*" [P2].

Less people were convinced that a decentralized IMS will help to prevent identity theft through increased security. Participant 4 mentioned that she is not sure how secure a decentralized IMS is and thus indicated that, "*I would probably only store information that are not too sensitive, something that – when it is misused – has not too big consequences.*" [P4]. Contrarily, some participants showed a certain level of frustration (9%). Participant 6 emphasized that: "*I don't have any concerns. I mean, I think my personal data were never really secure. Maybe data will be more secure in a decentralized system*" [P6]. Some participants also distinguished between the decentralized IMS itself and the application with which data disclosure can be controlled as depicted in Figure 2. In particular, some participants thought that the decentralized IMS might be more secure than currently existing IMSs, but that the application might be prone to attacks: "*If the app is hacked, than the hacker is able to pass all my personal data to a third party. He can use my proofs of identity. So, from my point of view the app is vulnerable, even if the decentralized IMSs as such is not open to attacks*" [P3].

Further concerns refer to legal aspects. Three participants stated that legal certainty must be ensured, before they use a decentralized IMS. It must be clear that verification of an identity through the decentralized IMS is legally watertight [P2, P5, P6,]. Moreover, liability was one concern as stated by participant 3: "*If there is a IMS that is controlled by the government I would definitively use it. This means that someone is liable in the case something went wrong. But I won't use it if the decentralized IMS would be provided by a private company, like Facebook (…)*" [P3]. Obviously, trust in the provider of a decentralized IMS plays an important role for the decision whether or not to use the proposed IMS.

4.3 Recommended Adjustments

Table 2 shows proposed adjustments for the pre-prototype features and security as proposed by the participants. Three main topics emerged that result either from concerns of participants towards using a decentralized IMS or general enhancements that are perceived as useful.

Table 2. Recommended Adjustments

Concern/ Enhancement	Proposed Adjustment
Security	"*The app must be additionally secured to prevent hacker attacks. One possibility might be that I receive a token with which I generate new numbers every time I use the decentralized IMS. I have a similar system if I want to log in to my office environment from home. This would make the application more secure and less vulnerable to attacks*." [P3] "*Maybe the app would be more secure if it would include a TAN-generator or if face recognition is used to prevent the use of the application by unauthorized third persons."* [P10]
Notifications and Rule Setting	*"I don't know if there is maybe such a function already but if I could retrace the flow of data, this would be very helpful. This could be like a type of notification feature, when and to whom my data are passed. I would also like to set some general rules to whom my data are allowed to be passed and to whom maybe not. Maybe sometimes it is okay for me, but potentially there are some firms with whom I don't want to share personal information." [P5]* *"It would be great to have a feature that notifies me when data are passed to a buyer of my data. This would allow more transparency. I know that my data are sold already, but I think it would be good to know to whom and when.*" [P7]
Sales of Data	"*Personal data are sold anyway. I want to participate on the profit made with the selling of my data. I think a feature that allows you to sell your data to particular firms or providers would be a useful and often used tool. At least, the sale of my data would be my personal decision and not done by some company that benefits from my data." [P2]*

Participants emphasized that the decentralized IMS, but especially the application that is used to control the flow of personal information, must be sufficiently secured. Several possible security mechanisms were proposed by the participants, including TAN-lists, face recognition, and/or random-number-generators that are used for authentication each time a user logs into the application. Additionally, interviewees indicate that a notification feature would be desirable. Particularly, they favor a feature that is able to track their personal information transferred to other parties throughout their whole life cycle. Probably, tracing personal information requires more than transparency and control of data that are disclosed. Companies and other institutions need to agree that personal information they acquire are identifiable and trackable. Moreover, participants stated that they would like to set general rules indicating whether or not certain firms or institutions should not receive particular personal data by default. One participant stated, for instance, "*I need to trust the company and/or institution to share my data. Considering some institutions, for example, I have certain concerns. My data must be protected against such institutions*" [P6]. Lastly, 9% of participants indicated that they would like a feature where they could sell personal data to firms like on a marketplace. This feature seems to be realizable, when the decentralized IMS is coupled with already existing platforms that allow sell data, such as [35].

4.4 Envisaged Application Scenarios

Asking participants to think about situations, in which they already used an IMS or are generally required to authenticate and verify information about themselves, we asked them if the decentralized IMS is perceived more useful in one situation or another. Generally, participants found it difficult to assess the usefulness of the decentralized IMS depending on the concrete situation - this is probably due to the fact that no hands-on experience through a prototype could be provided, leaving the participants with a rather theoretical concept of what comprises a decentralized IMS. However, 27% of participants indicated that they would not use a decentralized IMS for storing health data: "*In the case that I get ill, I want that my doctor has unrestricted access to all my personal data. I think the decentralized IMS is more important if there is a need to control the information flow of data that are not necessarily needed by certain companies or institutions to offer a service. (…) An example, where such an IMS is useful is probably for the control of data that are required by service provider like Spotify or Facebook*" [P6]. However, the latter point was discussed controversial by participants. In fact, the majority of participants indicated that they perceive control over data as the most useful tool of the presented decentralized IMS. However, thinking about application scenarios, they realized that this feature probably is not enforceable: "*I think it doesn't make sense to control the flow of data when I think about services like Spotify. I mean, if I don't give them my data, I won't be able to use their service. There will be no difference to existing IMS solutions. That is why I think transparency might be more important*" [P5]. Despite this might restricts the usefulness of the control features that is commonly envisaged for decentralized IMSs, some participants see nevertheless a certain advantage: "*Probably I won't be able to use the service, but at least I can make a decision based on the information about what data a service wants to have. I can decide to use another service that maybe doesn't want as many data as the other service*". Given these shortcomings, most participants indicated that they would either use the decentralize IMS, if they need to authenticate for communicating or receiving a service from a public authority or for banking transactions. Overall, these suggestions provide interesting insights that help to decide in which context a pilot of a decentralized IMS should be tested.

4.5 Overall Usefulness

Asking participants directly whether or not they think the introduced decentralize IMS is useful, all participants indicated that they think it would actually be useful. This results must be interpreted carefully, since they are potentially distorted due to informant bias. Particularly, we come to this conclusion based on the consideration of the severity of concerns and the feasibility of the control of data disclosure and flow of the participants in section 5.4, which was previously indicated as one of the most important features in terms of usefulness. Thus, we interpret the answers of the participants as a tendency towards a positive attitude of the participants towards the decentralized IMS. However, in order to check the validity of this statement, we need to, first, include the recommended adjustment and take care of concerns of participants to recheck the perceived overall usability.

5. Discussion

The results of the qualitative study on the usefulness of decentralized IMSs shows that several features envisaged for decentralized IMSs and especially the features proposed in the whitepaper of the Sovrin foundation [10] are perceived as useful by study participants and, thus, meet actual user requirements. Features that are implied by decentralization and the use of blockchain technology, like control over personal information, the ownership of data and transparency over the amount and kind of data required by services and institutions are emphasized as especially useful by the interviewees.

Despite this rather positive first impression, the questions after concerns and possible application scenarios revealed that participants also have doubts whether or not a decentralized IMS with its envisaged features is feasible. For instance, participants were skeptical about the feature of control: If a user of a decentralized IMS refuses the disclosure of certain personal data required by a service, he will probably not be able to use the service. Thus, the ability to exert control over the disclosure of data will actually led to the same situation as using existing IMSs. However, some participants stated that, even if this is the case, transparency over the data a service requires and receives might be useful, because at least one can decide to use an alternative service, based on the information available in the decentralized IMS.

Increasing transparency has actually more advantages than just providing more information to users of decentralized IMSs. Following the recommendations of participants, introducing transparency could facilitate the development of a marketplace for personal data. These findings are in line with the existing literature, which confirms, that transparency is an important precondition for the users' control over their privacy, which can increase users' trust in accurate and secure processing of their personal data [35]. Already existing attempts to develop such platforms are often restricted by the fact that companies do not reveal what and how many personal information they possess and with whom exactly information is shared [36]. Increased transparency could foster a free market in which users can participate and sell their personal data at will. Such a platform could be easily combined with an application that helps users to manage their personal data.

A further concern that must be attached great importance is security of personal data. Participants were less concerned about the security of data stored on a blockchain, but doubted whether the application, with which users are able to manage personal data is secure enough. Participants provided several proposals how to increase the security of the application. Each of them needs to be discussed and assessed for the further development of decentralized IMSs and the associated application. The fact that people care more about the security of data, when using the app than about the security of the decentralized IMS itself may stems from the fact that people are not familiar enough with the functioning of blockchain technology. Some participants stated that they cannot assess whether or not data are secure on the blockchain, however, the term blockchain is rather negatively connoted. One participants stated that in order to trust such an IMS, people must be educated about the functioning of blockchain and trained how to use such a system.

Surprisingly, some participants do not show any concerns with regard to security. Participants indicated a certain level of frustration, suspecting that their personal data is sold and used anyway. This considerable share of participants was more concerned about the practicability of a decentralized IMS.

Certainly, to be useful to a large user group, the IMS must be designed in such a way that it is easy to use and saves time, compared to existing IMS solutions. Thus, the user interface should be tested more carefully in further pre-prototype testing and finally should be assessed in hands-on prototype experiments.

6. Limitations and Further Research

The results of this study need to be viewed in the light of its limitations. First and foremost, the study shows a relatively small number of interview partners. Consequently, we can expect that further interviews will reveal more and potentially contradicting insights, since the criteria of saturation was not reached. Nevertheless, while analyzing the interviews we came to conclusion that the amount of concerns identified and recommendations that could enhance the usefulness of the decentralized IMS justify an interruption of the interviews, in order to implement already proposed features and to take care of participants' objections. In line with design science research methodology we thus propose the direct implementation of the proposed features and the consideration of their objections. Through this iterative and direct approach, we are convinced to create better prototypes in a faster way that actually fulfill user requirements. The pre-prototype testing presented in this paper is consequently a first step that triggers an iterative process of several interview rounds using adjusted pre-prototypes that increasingly obey user requirements. Having this process completed, a development of prototype of a decentralized IMS as well as its demonstration is envisaged.

7. Conclusion

Decentralized identity management systems (IMSs) are envisaged as the next big thing in identity management: They are expected to increase the security of personal information, to foster control over disclosure of personal data and to enhance transparency. Given this expected features, it is not surprising that there is a vast amount of companies that work on the development of decentralized IMSs. Several whitepapers document the state of the art in the development of decentralized IMSs. While there is a huge discussion about the technical feasibility of certain features, the assessment of the system from a user perspective is currently missing. In order to prevent huge losses that stem from the development of a prototype that is not accepted by users, simultaneous usability testing in the pre-prototype phase is needed.

This paper presents the results of a pre-prototype usability testing of a decentralized IMS. Participants of this study were guided through an animation of the pre-prototype, showing all relevant features of a decentralized IMS. The user interface of an application was provided to the participants of this study. The analysis of the interviews shows that a good deal of work is necessary to fulfil actual user requirements on decentralized IMSs. We will take up these concerns and implement interviewees recommendations in further pre-prototype developments. This study is a trigger for further usability tests, whereas an iterative process of pre-prototype development is suggested. At the end of this process, a pre-prototype should be developed that incorporates all user requirements and serves as foundation for the development of a prototype that allows hands on usability testing.

8. Appendix: Interview Protocol

1. Please provide us with some personal information (age, gender, education).
2. Please describe the function of an identity management system in your own words. Do you use such systems in your everyday life?
3. After you have seen the animation and the mock-up, did you understand everything you saw? Do you have additional comprehension questions?
4. Do you think the usage of such a decentralized IMS would be useful for you? Please provide an explanation.
5. If there would be decentralized IMS, would you use it?
6. Which features of the presented decentralized IMS do you think are especially useful? Please explain.
7. Please rank the stated features in accordance to their usefulness beginning with the most useful feature.
8. Which features are at least useful? Please provide an explanation.
9. Please rank these features beginning with the less useful functionality.
10. Do you have any concerns when thinking about using a decentralized IMS?
11. Now think about different situation, in which you need to manage information about your identity. Do you think a decentralized IMS could be more or less useful in any of these situations or does the situation has no influence on your assessment of the usefulness of the decentralized IMS?
12. Are there any features that you would implement in a decentralized IMS if you could?

9. References

[1] J. Van Dijck, "'You have only one identity': performing the self on Facebook and LinkedIn," *Media, Cult. Soc.*, vol. 35, no. 2, pp. 199–215, 2013.
[2] B. Debatin, J. P. Lovejoy, A. K. Horn, and B. N. Hughes, "Facebook and Online Privacy: Attitudes,

Behaviors, and Unintended Consequences," *J. Comput. Commun.*, vol. 15, pp. 83–108, 2009.
[3] D. Kugelmann, "Facebook in der Verantwortung," *Datenschutz und Datensicherheit*, vol. 42, no. 6, pp. 338–338, 2018.
[4] K. Young, "There's A Facebook Alternative, It's Called Self-Sovereign Identity," *Coindesk*, 06-Apr-2018.
[5] J. De Clercq, "Single Sign-On Architectures," in *Infrastructure Security - International Conference, InfraSec 2002 Bristol, UK, October 1–3, 2002 Proceedings*, 2002, pp. 40–58.
[6] R. Wang, S. Chen, and X. F. Wang, "Signing me onto your accounts through Facebook and Google: A traffic-guided security study of commercially deployed single-sign-on web services," in *Proceedings - IEEE Symposium on Security and Privacy*, 2012, pp. 365–379.
[7] IBM, "Collaboration: Unlocking decentralized, digital identity management through blockchain," *Blockchain Unleashed.* [Online]. Available: https://www.ibm.com/blogs/blockchain/2018/04/collaboration-unlocking-decentralized-digital-identity-management-through-blockchain/. [Accessed: 05-Jun-2018].
[8] G. Zyskind, O. Nathan, and A. S. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in *Proceedings - 2015 IEEE Security and Privacy Workshops, SPW 2015*, 2015, pp. 180–184.
[9] IBM, "Trust me: Digital identity on blockchain," 2017.
[10] Sovrin Foundation, "Sovrin: A Protocol and Token for Self-Sovereign Identity and Decentralized Trust," 2018. [Online]. Available: https://sovrin.org/wp-content/uploads/2018/03/Sovrin-Protocol-and-Token-White-Paper.pdf.
[11] A. C. Sonnenwirth, "Preprototype of an Automated Microbial Detection and Identification System: a Developmental Investigation," *J. Clin. Microbiol.*, vol. 6, no. 4, pp. 400–405, 1977.
[12] P. Niewczas, L. Dziuda, G. Fusiek, and J. R. McDonald, "Design and Evaluation of a Pre-Prototype Hybrid Fiber-optic Voltage Sensor for a Remotely Interrogated Condition Monitoring System," in *Instrumentation and Measurement Technology Conference*, 2004, pp. 2369–2374.
[13] F. D. Davis and V. Venkatesh, "Toward preprototype user acceptance testing of new information systems: implications for software project management," *Eng. Manag. IEEE Trans.*, vol. 51, no. 1, pp. 31–46, 2004.
[14] D. Foundation, "Decentralized ID."
[15] C. M. K. C. Cuijpers and J. Schroers, "eIDAS as guideline for the development of a pan European eID framework in FutureID," 2014.
[16] K. Tracy, "Identity management systems," *IEEE Potentials*, pp. 34–37, 2008.
[17] D. Hühnlein, H. Roßnagel, and J. Zibuschka, "Diffusion of Federated Identity Management," *Sicherheit*, pp. 25–36, 2010.
[18] R. Dhamija and L. Dusseault, "The Seven Flaws of Identity Management: Usability and Security Challenges," *IEEE Secur. Priv.*, vol. 6, no. 2, pp. 24–29, 2008.
[19] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," *Www.Bitcoin.Org*, p. 9, 2008.
[20] X. Xu *et al.*, "The blockchain as a software connector," in *Proceedings - 2016 13th Working IEEE/IFIP Conference on Software Architecture, WICSA 2016*, 2016, pp. 182–191.
[21] M. Gupta and R. Sharman, "Dimensions of Identity Federation: A Case Study in Financial Services," *J. Inf. Assur. Secur.*, vol. 3, pp. 244–256, 2008.
[22] A. Jøsang and S. Pope, "User centric identity management," in *Asia Pacific Information Technology Security Conference*, 2005, pp. 1–13.
[23] D. Shrier, W. Wu, and A. Pentland, "Blockchain & infrastructure (identity, data security)," 2016.
[24] UniquUD, "UniquID," *2018*. [Online]. Available: uniquid.com/. [Accessed: 15-Jun-2017].
[25] Blockstack, "Blockchain Identity," *2018*. [Online]. Available: https://blockstack.org/posts/blockchain-identity. [Accessed: 15-Jun-2018].
[26] ShoCard, "ShoCard," *2018*. [Online]. Available: https://shocard.com/. [Accessed: 15-Jun-2018].
[27] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, "A Design Science Research Methodology for Information Systems Research," *J. Manag. Inf. Syst.*, vol. 24, no. 3, pp. 45–77, 2008.
[28] A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design Science - Hevner," *Des. Sci. Inf. Syst. Res. Author MIS Q.*, vol. 28, no. 1, pp. 75–105, 2004.
[29] M. Ali, J. Nelson, R. Shea, and M. J. Freedman, "Blockstack: Design and Implementation of a Global Naming System with Blockchains," *Usenixatc*, no. February, 2016.
[30] C. Züll, "SDM Survey Guideline: Offene Fragen," Mannheim, 2015.
[31] H.-F. Hsieh and S. E. Shannon, "Three approaches to qualitative content analysis," *Qual. Health Res.*, vol. 15, no. 9, pp. 1277–1288, 2005.
[32] J. Gläser and G. Laudel, "Qualitative social life with and without coding: Two methods for early stage data analysis in qualitative research aiming at causal explanations," *Forum Qual. Sozialforsch. / Forum Qual. Soc. Res.*, vol. 14, no. 2, pp. 1–25, 2013.
[33] M. Schreier, "Varianten qualitativer Inhaltsanalyse: Ein Wegweiser im Dickicht der Begrifflichkeiten," *Forum Qual. Sozialforsch. / Forum Qual. Soc. Res.*, vol. 15, no. 1, p. 27, 2014.
[34] A. L. George and A. Bennett, *Case Studies and Theory Development in the Social Sciences*, vol. 82. 2005.
[35] Data Fairplay, "Data Fairplay: Der Marktplatz für deine Daten," *2018*. [Online]. Available: https://www.datafairplay.com/. [Accessed: 14-Jun-2018].