

Conducting a Usability Evaluation of Decentralized Identity Management Solutions

Alina Khayretdinova, Michael Kubach , Rachele Sellung and Heiko Roßnagel

Abstract

New approaches to identity management based on technologies such as block-chain and distributed ledgers are promoted as a chance to give users full control over their own identity data. Despite being often called the future of digital identity management, Decentralized Identity Management (DIdM) and Self-sovereign Identities (SSI) are still facing a number of challenges, usability being a major one: their concepts are too sophisticated for users and do not fit their mental models. We address this by conducting a study that analyses and evaluates the usability and practical applicability of some of the most advanced DIdM solutions. The results of the user tests reveal existing usability issues and outline the way they deprive end users of experiencing the entire range of claimed privacy and security benefits of these identity solutions.

A. Khayretdinova
University of Stuttgart IAT, Institute of Human Factors and Technology Management,
Stuttgart, Germany
E-Mail: alina.khayretdinova@iat.uni-stuttgart.de

M. Kubach (✉) · R. Sellung · H. Roßnagel
Fraunhofer IAO, Fraunhofer Institute for Industrial Engineering, Stuttgart, Germany
E-Mail: michael.kubach@iao.fraunhofer.de

R. Sellung
E-Mail: rachele.sellung@iao.fraunhofer.de

H. Roßnagel
E-Mail: heiko.rossnagel@iao.fraunhofer.de

Keywords

Decentralized identity management • Blockchain • UX • Usability • SSI • Self-sovereign identity

1 Introduction

Despite of numerous state-sponsored efforts over the last twenty years to provide European citizens with high assurance electronic identities, today's digital identity market is heavily dominated by single-sign-on solutions that are offered by big international corporations. Nevertheless, the market for digital identities is not saturated yet. Many use cases still wait for a suitable, e.g. interoperable, easy-to-use, widely adopted, secure, privacy friendly ID-solution. This is why market researchers still see a high potential in this sector [1, 2]. New approaches, initially based on Blockchain and distributed ledger technologies (DLT) have been getting a lot of attention in the past 3–4 years and are promising to disrupt the digital identity market [3]. Such approaches, often also called Decentralized Identity Management (DIdM) and Self-sovereign Identities (SSI), are often marketed as the future of digital identity management [4, 5]. In the following, we will use the term Decentralized Identity Management solutions (DIdM) for these approaches.

Numerous companies and projects (Sovrin, Jolocom, W3C Decentralized Identifier Working Group, Decentralized Identity Foundation, Hyperledger of the Linux Foundation etc.) are currently working on technologies that make it possible to use decentralized identities for trustworthy and privacy-friendly identification in digital interactions. The European Commission supports such approaches, for example through the European Self-Sovereign Identity Framework (ESSIF) as part of the European Blockchain Service Infrastructure (EBSI) [6] and the SSI eIDAS bridge [7]. Those actors see security and privacy as the main challenges in the currently available approaches to digital identities and promise to give the user the power to reclaim control over their own identity data in digital interactions [8, 9].

Nevertheless, experience shows that technical functionality even together with high levels of security and privacy protection are not sufficient for the diffusion of new information technologies [10]. Many technologies in the identity management sector that were previously regarded as disruptive, such as CardSpace,

Uprove, and Attribute Based Credentials, have failed to find adoption by a significant share of the market [11, 12]. Hence, it has been argued that the consideration of multidisciplinary aspects, such as security, usability, and socioeconomics, is crucial for the success of a software product on the market [13]. However, it is a common issue that developers tend to focus on the former aspects while neglecting the latter [14].

We agree that there remains a growing need for identity management solutions to replace username/password and the solutions provided by the mighty GAFA platform-corporations (Google, Apple, Facebook, Amazon) — as has been countlessly discussed in information (security/privacy) science as well as in the public. New approaches entering the market for alternative identity management solutions still struggle with its multi-sided structure, leading to a “chicken or the egg” dilemma. Uptake with end-users and services providers and the sustainable as well as balanced trust relationship among the relevant stakeholders is a big challenge [15]. Therefore, we think that is important to critically assess the current promises, intentions and practices of DIDM solutions, in order to avoid mistakes that could, again, lead to the failure of a promising technology on the market. This is what we aim for with this paper. Our analysis is focused on the usability aspects of DIDM solutions, and studies them empirically with end users. Our research approach addresses the challenge of usability in DIDM solutions by conducting a user study that analyses and evaluates currently available DIDM solutions towards their practical applicability for end users. This paper presents the results of the usability tests with end-users that will be later used to build a user-friendly prototype and to give design guidelines to DIDM solution developers aiming to increase the adoption potential of their products. Other important aspects, such as the perspectives and requirements of service providers (relying parties) [16], will have to be kept aside for future work.

Our paper is structured in the following way. In section two we give an overview of the background and current state of Decentralized and Self-sovereign Identities. We briefly introduce the approach and terms, principles being followed, market overview and related research. Next, in section three, we present our user test of three DIDM solutions, describing methods, results, and analysis. Continuing, in section four we discuss the key results of the study and what we regard as its main outcomes. Lastly, section five presents the limitations and section six briefly concludes our paper.

2 Overview: Decentralized and Self-sovereign Identities

Decentralized and Self-sovereign Identities (SSI) are currently being marketed as the future of digital identity management as opposed to traditional approaches that are often simply called “legacy systems” [17–19]. The promise of these approaches is that they are able to empower users to take back control over their data [20, 21], and to overcome the dominance of the GAFA platforms [22, 23].

When it comes to new, alternative, decentralized approaches towards identities, the term Self-sovereign Identity has become more and more prominent. Although it is not always being used consistently, Mühle et al. [24] summarize the key properties of the concept as that a Self-sovereign identity management system would allow users to fully own and manage their identity without having to rely on a third party. The origin of the concept under this name can be traced back to 2016, when Allen published his so called “Ten Principles of Self-sovereign Identity” [20]. There, he also refers to the earlier proclaimed “Laws of identity” by Cameron [25], which illustrates that the basic approach is not entirely new. Following the taxonomy by Lesavre et al. [26], Self-sovereign Identity can be seen as a bottom-up approach, where no single entity acts as central authority that has control over identifier origination and/or credential issuance. Identifiers and credentials are solely managed by the users, without requiring any permissions. On the other side of the spectrum would be top-down approaches relying on central authorities as identity providers and federated approaches somewhere in between.

However, it is important to recognize that the reasoning provided for the DIDM approach and the SSI principles or laws are not founded on empirical studies of the requirements of users (and neither service providers). In addition, there are still some open questions on whether the users actually desire so much control and whether the solutions not only provide users with the theoretical opportunity to exercise this control through their technical architecture, but also empower them in practice and not confuse and overburden them. For users to be able to fully manage and own their identity without having to rely on a third party, they are required to somehow understand the concept and be assisted with usable tools that do not frustrate them. After all, typical users do not use identity management because it is such great fun, but rather to access services they want to use. Being in theoretical control of their identity could become a similar experience as the current total control users have over trackers and cookies when visiting a website. Having to manage those detailed settings manually through annoying dialogues might simply frustrate them. The lack of usability could then lead average users to

simply use privacy unfriendly, but convenient solutions—a pattern we frequently observe.

One of the potential usability issues of Blockchain-based DIdM solutions is the fact that the private key that ensures the access to user's personal data is in total responsibility of the user [27]. While this is often marketed as one of the most significant benefits of DLT-based and DIdM solutions, it also comes with significant challenges such as how to securely store and manage those keys to avoid irretrievable loss of key and connected accounts [28]. If such issues are not properly explained and handled, end users will have troubles understanding and using the new technology. This makes the solutions less attractive to average users and leads to lower levels of adoption. Especially, if it may seem that they require more and complex user involvement while not offering other benefits except for being more privacy friendly (something the average user cannot even personally assess as we are clearly in some kind of “market for lemons” here [29, 30]). Moreover, if such solutions are not widely supported by service providers and thus not integrated into a sufficient variety of services, their value for end users is even lower.

The issue of usability in privacy and security tools has already been subject of research efforts for quite some time [31, 32]. Nevertheless, there seem to be only few attempts to explicit fix user experience challenges for security tools and so also for DIdM. Following [33–35], the major problems that go beyond the mere graphical user interface are:

- The concepts and interface presentations do not fit the underlying mental models of the users.
- Tools offer actions, such as e.g. obtaining, managing, and securing private keys, passwords, credentials, etc. that are either too complicated to be carried out, or not presented clearly enough and therefore executed wrongly.

This seems particularly important when it comes to a technology like DIdM that puts as much power into the hands of the individual user and builds on concepts such as public and private keys that are not trivial to the average online-shopper. We see this lack of consideration of the usability and mental models in current approaches to DIdM as an important potential weakness that needs to be studied empirically with explicit user involvement. Therefore, we want to address it through our work.

For our user study, we are dependent on publicly available and testable DIdM solutions. In their public presentations, proponents of DIdM give the impression, that the technology is ready to replace legacy IdM systems. On their website,

for example, uPort writes of “easy-to-use data management and control to your business and customer” [36], Evernym of “The fastest, most efficient way for organizations to offer an SSI-enabled solution for their users” [37]. That of course raises high expectations regarding their solutions technology readiness and current practical applicability.

However, another consideration that needs to be made is that DiDM technology is still under heavy development and different approaches are currently being pursued. For example, those can be differentiated according to organizational structure, models for identifier and credential management, presentation disclosure, general system architecture design and the use of public registries. A systematic overview and discussion can be found at Lesavre et al. [26]. First standards are currently being finalized, e.g. by the W3C [38] and the DID [39], but the work is still ongoing. This makes interoperability between the different approaches challenging.

At this time, a significant number of companies and projects are working on decentralized identity solutions. In a thorough survey of market of Blockchain-based Identity Management solutions and technologies, Kuperberg [27] analyses 43 approaches with different levels of maturity and availability. He concludes that only a couple of these approaches could compete with established solutions when it comes to end-user convenience, though it has to be noted that his analysis has to remain on a rather high level due to the high number of solutions considered. What he misses in particular, is a clear and sustainable business model. Dunphy and Petitcolas [33] analyse IdM schemes of three Blockchain-based products (uPort, ShoCard, Sovrin) according to the Cameron’s “laws of identity” [25]. Regarding usability, they conclude that all of those projects have an “unclear usability and user understanding of [...] (the) privacy implications.” None seems to actively address the issues in regard to fitting mental models and usability. All this apparently supports need for our research approach.

3 User Test of DiDM Solutions

In our research, we are addressing the challenge of usability in DiDM solution by conducting a user study that analyses and evaluates DiDM solutions that are currently (beginning of 2020) available on the market towards their practical applicability and acceptance for end users. For our study, we identified 23 DiDM solutions. In April 2020, those identified solutions were on a sufficient level of maturity (and/or transparency in public communication) to provide enough information for an analysis that would determine whether they would be suitable for

an end-user study. In order to identify which DIDM solutions would best fit a usability study with end users, we analyzed those 23 DIDM solutions by their differences in maturity, purpose and functionality. The suitability of solutions for the user test was evaluated according to the following set of requirements: DIDM as the core technology; minimal level of technology readiness (at least TRL 7); wide functionality (to be able to carry out at least 3 scenarios for user testing); availability of the wallet for both iOS and Android platforms; availability of a demo scenario or even real services to test the solution; interface language English and/or German. According to these conditions, three DIDM digital wallets qualified for then being evaluated in a systematic study including end-users in a usability test: Evernym ConnectMe, Jolocom SmartWallet, and uPort ID.

3.1 Method

In order to obtain a full understanding of the user's impression of each tested identity solution and the concept of DIDM solutions in general we employed a combination of usability and user experience evaluation methods (following the approach of Tomlin [20]).

In Summer 2020, the user tests were conducted remotely via individual video calls, each with a duration of 80 to 100 min. The tests consisted of a preliminary questionnaire, a block of 8 tasks to be completed each followed by questions, the User Experience Questionnaire (UEQ) [19], and a post-questionnaire. Participants carried out tasks with the smartphone app and the demo websites that were provided by the solutions.

3.1.1 Pre-questionnaire

The pre-questionnaire consisted of 8 questions to define demographics (gender and age) of participants and their experience with technologies similar to digital wallets they were about to test. Moreover, there were questions aimed to understand how participants create and store their passwords, which would give more information on their further decisions and opinions regarding the seed-phrase technique all three digital wallets were using to recover user accounts.

3.1.2 Tasks

There were 8 tasks during the test: create an account within a digital wallet (1), obtain two personal documents (2 and 3), make sure the digital wallet is ready for future use (4), back-up the digital wallet (5), delete one of the credentials (6), delete the wallet, re-install the app and restore the account (7), delete the account

(8). After each task, there were a set of questions to assess whether a participant managed to perform the task, how difficult it was to perform the task, how many attempts it took them to get a certain task done, etc.

3.1.3 User Experience Questionnaire (UEQ)

To cover a comprehensive impression of the user experience aspect of digital wallets, an established and tested questionnaire was needed. We opted for the User Experience Questionnaire (<https://www.ueq-online.org/>) that helps to measure both usability aspects such as efficiency, perspicuity, and dependability, and user experience aspects such as originality and stimulation. According to Schrepp et al., the main goal of the UEQ is to allow a fast and immediate measurement of user experience of a product, which also allows to compare it with its direct competitors to get information on the comparative position of the product [40]. The questionnaire has 26 pairs of terms with opposite meanings grouped into six scales: attractiveness, perspicuity, efficiency, dependability, stimulation, and novelty. The items need to be rated on a 7-point Likert scale from -3 (fully agree with negative term) to $+3$ (fully agree with positive term). In order to avoid automatic response to some terms, half of the items start with the positive term, the rest with the negative term in randomized order [41]. More information on the UEQ, its underlying methodology and reliability as well as validity of its scales can be found at [40–42].

3.1.4 Post-questionnaire

Post-questionnaire consisted of 7 questions and was aimed to find out whether participants liked the apps or not, what they especially they liked and disliked in them. Moreover, some of the questions helped to understand what participants think about the concept of such digital wallets in general and whether they would be ready to switch from their physical wallet to a digital one.

3.2 Results

This section presents the results of user tests conducted on DiDM solutions following each step of the test process.

18 persons took part in the evaluation of three applications (6 participants per app), among which were 9 male and 9 female participants with 78 % of them being under 30 years old and 22 % above 30. All participants were able to complete most of the tasks except a few cases when users experienced connectivity issues between the digital wallet and the demo website, which led to failing some

tasks. Further, we are presenting the results of each tasks that participants were asked to do during the test.

3.2.1 User Test Tasks

Task 1. Create an account within a digital wallet. All the users managed to create an account in all three digital wallets, with 16 % of them finding it a bit difficult to perform the task.

Task 2. Obtain first personal document. All the user of ConnectMe and uPort ID performed the task without the external help with half of them having no difficulties finding the function in the apps. However, a smaller percentage of SmartWallet testers managed to carry out the task completely on their own—83 %.

Task 3. Obtain second personal document. All of the users that were testing SmartWallet and uPort ID managed to obtain the second credential without any external help compared to 67 % of those who tested ConnectMe. However, a smaller number of participants managed to perform the task from the first try in comparison to obtaining the first credential and the task seemed more difficult to a bigger number of people.

Task 4. Make sure the digital wallet is ready for future use. The participants were asked the following questions: “Have you done everything that was necessary with your digital wallet? Is everything set up now for the use in future?” Not all the users were sure the digital wallet was all set for future use, with some doubts being connected to the security of their account and the general purpose of the digital wallet.

Task 5. Back-up the digital wallet. Almost all the participants managed to back-up their credentials without the external help, however, almost half of them found the task somewhat difficult to perform. Moreover, less than 50 % of participants had the confidence that their documents are indeed backed up: 83 % testers of SmartWallet, 50 % of ConnectMe users and 33 % of those who tested uPort ID answered negatively to the question whether they think their documents are well protected after the back-up process. The most common doubts were about the back-up choice that was given in the apps and the back-up being saved on the server of the digital wallet. Another issue appeared in this task was the use of the “seed” or “recovery” phrase: most of the test participants did not understand its purpose and had doubts on whether it would help them to restore their account in future in case of a lost or a compromised device.

Task 6. Delete one of the credentials. None of the SmartWallet users performed this task due to the absence of this function in the app. A bit more than a half of ConnectMe users managed to delete one of the credentials with most of them being confused that they had to delete a connection instead of the credential. On

the other hand, all of the participant that tested uPort ID performed the task and found it not difficult at all.

Task 7. Delete the wallet, re-install the app and restore the account. All of the ConnectMe and uPort ID users managed to perform the task without any external help and the majority did not find the task difficult. However, only 67 % of them were sure they would be able to restore their account in case they do not have the access to their current mobile device (due to the fact that they stored their “seed” or “recovery” phrase on the mobile device where they interacted with the digital wallet).

Task 8. Delete the account. The success rate of the task performance is clearly much lower compared to other tasks. Only half of participants that tested uPortID managed to carry out the task; 17 % of ConnectMe testers and none of the participants could delete their account in the SmartWallet app. 50 % to 100 % of participants found it highly difficult to carry out this task for each digital wallet with almost all of them not being sure that their personal information was deleted everywhere.

3.2.2 UEQ

As stated earlier in the paper, the User Experience Questionnaire consists of 26 different aspects of design, usability and different requirements that the users had to rate from -3 to 3 . Having subtracted the best and the worst scores for each digital wallet, we found the following results: ConnectMe received the highest average score of satisfaction with 1.8 , uPort ID followed with a rating of 0.9 and the SmartWallet had a rating of 0.4 . In addition, Users presented the following results in regards to understanding (3) and not understanding (-3), Smart.Wallet -0.5 , uPort 0.8 , and Connect.Me 1.0 . Regarding feeling secure (3) and not secure (-3), users averaged with Smart.Wallet, -1.0 , Connect.Me 1.0 , and uPort with a 1.3 .

3.2.3 Post-questionnaire

A little less than a half of all users found the digital wallets as “rather good”, however only SmartWallet received 50 % of negative overall evaluation of the app with none of the testers saying they really liked it. Two other digital wallets were rated more positively with 33 % and 17 % of them respectively being really liked by users. The biggest problem found by users of SmartWallet was the fact that it is not protected by a passcode and the overall interaction was sometimes confusing with the app not letting to delete the credentials and the recovery process being difficult. The testers of ConnectMe enjoyed the intuitiveness and the interface design of the wallet, however some of the users mentioned confusing terms used

in the app. The users of uPort ID also stated interface design being one of the advantages of the application and the biggest drawbacks was its functionality: difficulty to obtain the credentials (except the first one) and not being able to delete the account.

Overall, most of the test participants of all digital wallets shared the opinion that the security of their personal information and documents in this kind of apps is the most important part that needs improving. Some of them also stated that in case those security aspects are improved, they would consider switching to a digital wallet.

3.3 Analysis

After carefully analyzing the results of the user study, two main points can be highlighted. First, the results show the apparent need of improvements of the DIDM solutions regarding user mental models and user understanding. Second, there are serious usability problems found in some of the key functions (e.g. backup and restoration) that are essentially required in DIDM wallets. We elaborate on these two points in the following section.

3.3.1 User Mental Models and User Understanding

The existing identity solutions are not as intuitive and easy to use as they claim to be. It would be expected that a market-ready solution is able to compete with the simple interaction patterns provided by the traditional username-password approach and the approach provided by web-single-sign-on solutions by Facebook and Google. This is not the case even for the quite tech-savvy users in our study: many users experienced problems not only in setting up and launching the interaction but also in obtaining credentials. In addition, The UEQ results presented rather weak results for the wallets regarding on whether or not users thought the app was ‘understandable (3) or not understandable (−3), where Smartwallet had a −0.5 average score, uPort had 0.8, and Connect.Me had 1. The interaction paradigm of those DIDM solutions is different and does not fit the user’s established mental models and apparently the solutions are still in a relatively early phase of development.

Moreover, test subjects had a trouble understanding the necessity and importance of backing up their keys (“seed/recovery phrase”). Most of the participants did not write them down even if the app suggested to do so, which in real life would lead them to not being able to recover their personal data in case the device breaks, is lost, stolen, or compromised in any other way. In addition to

that, some of the tested solutions do not explicitly explain the difference between the concepts of “backing up” credentials and setting up a “recovery” of the account ID and the importance of both functions, which in some cases led participants to carry out only one function and not considering the other. Again, this shows that the mental models of the users do not fit to the user experience that the DiDM solutions provide — which can lead to frustration, security problems and finally adoption problems on the mass market (again, this is even the case for the relatively tech savvy participants of our study).

Problems with mental models become apparent as well from the finding that it was unclear to most of the test subjects how and where their data is actually saved. This is quite surprising, as those DiDM solutions claim that local storage under full control of the user would be their key feature and advantage. This gave some of the participants an insecure feeling when they wanted to delete their data “on the servers”—which of course was not possible. Again, a problem of the users’ mental models that is not being adequately addressed by the DiDM wallets.

Another problem that became obvious in our study is learnability or the ability for users to ‘learn as you go’ with completing similar tasks. For instance, in some applications users obtained the first credential and naturally were searching for the same way to obtain the second credential but were unable to do so.

3.3.2 Usability Regarding Vital Functions: Backup and Restoration

The backup and restoration functionality was either not fully implemented (Jolo-com — for credentials), not very convenient (manually saving a.zip-file, writing down the mnemonic key phrase), or relied on a server(s) under control of a single entity (“Evernym Cloud”) and thus contradicting the whole decentralized and user controlled aspect of the DiDM approach. That such an essential function of the digital identity lifecycle is not properly implemented in the current versions of the wallets that were studied came as quite a surprise — considering how the solutions claim to be “ready for use” and beyond mere Proof-of-concept stage.

Moreover, not all of the three wallets pointed out the importance of the backup function enough (even if it was implemented). After all, this is the only way that users can restore access to their important private accounts if they are managed through the DiDM solution. Push-notifications and other warning messages would be advisable to remind users of this important function.

4 Discussion

According to its advocates, the main benefit of SSI is to put the users in full control of their identities. This is supposed to help to protect their right of informational self-determination. However, with more control also comes the burden of more responsibility and more effort to manage and use these identities and credentials. To be able to manage them effectively, users need to form some sort of rough understanding of how the technology works (aka mental model). Though, our results show that the mental models of the users not necessarily align with those of the developers that are quite familiar with technologies like public key infrastructures and electronic signatures. Users quite often form a different understanding that is shaped by the traditional, hierarchical solutions they are currently using and therefore experience problems when trying to use and manage the credentials in a decentralized architecture. This is especially apparent when it comes beyond the simple use case of issuing and verifying credentials. Important aspects of the identity lifecycle like backup and recovery as well as deleting credentials or whole accounts, constitute huge challenges for the users of the DIdM solutions in our study.

These difficulties are further emphasized by the fact that the basic usability of current DIdM solutions leaves a lot to be desired. This leads to further frustration of the users. Another problem for the approach is that the development of the available solutions is often not as advanced as it is being advertised by their advocates. Essential features are often missing which can be observed by the fact that out of the 23 solutions we examined, only three could offer all the features that we required for our study. And even those three resembled more a work in progress than a mature market ready solution. As just one example, one wallet application (Evernym ConnectMe) in the Fall of 2020 completely removed the backup functionality. It had been available during the user tests, but an update of the application removed the function. Such a gap between promises and actual performance that can be delivered at this point could lead to exaggerated expectations that can only be disappointed if one wants to implement the immature technology right now. This might sustainably damage the reputation of DIdM solutions. The danger is that this could also be regarded as another example that privacy friendly solutions just do not work in practice.

Moreover, to be successful on the market, DIdM faces the same challenge as all other competing and often much more mature identity management solutions. It has to attract a high amount of users and relying parties to benefit from network effects in a two sided market [15]. To achieve this, the perceived benefit by users and relying parties or relative advantage of the DIdM solutions has to be

higher than the competition. The main question will be if — in the eyes of the end users and service providers — the perceived benefit of more user control and more privacy will outweigh the drawbacks such as increased effort to manage the credentials (potentially more annoying dialogues to answer), higher responsibility e.g. to secure the device that is used to control the identity, more complicated backup in case of lost credentials, and particularly at the current state, poor usability and lack of maturity. An empirical user study on web identity management raises some doubts in this regard [43]. Their results show that users do not value control over their identity data as much as many proponents of DIDM apparently expect. Therefore, we believe that it is essential for developers of DIDM to address the current drawbacks we pointed out in a multidisciplinary fashion to improve the likeness of their success on the market.

5 Limitations

Our empirical user study and the derived analysis have undoubtedly some limitations, particularly regarding the sample of end users that participated in the test, the testing setup and the development state of the digital products that were tested.

A sample of 18 participants certainly cannot be regarded as representative of the general population. Most of the test participants were young people around 30 years. In most of the cases they reported themselves as being tech-savvy and could speak a high level of English while living in a non-native English-speaking country, which points to a higher level of education. However, while this is certainly biased sample, we can reasonably assume the results of the user tests could have been even more negative for the case that a broader sample of participants would have been available for us. An example would be end-users who are not as confident with smart phones, scanning QR-Codes, and other relatively new technology.

Another fact that needs to be considered is that the participants tested the DIDM solutions at home having a good internet connection for their smartphone (and desktop computers if used as well). Thus, at least connectivity-wise the whole process (e.g. obtaining credentials) ran smoothly for most of them. However, even under such perfect conditions there were cases when the connection between the digital wallet and the demo website was broken for some time and there was no way of getting back seamlessly to the process. Some of the tested wallets did not offer any solution for such cases and users had to start the whole process from the beginning. It would be interesting to learn about how DIDM solutions relying on mobile smartphone wallets perform in practice when there is

actually still a significant number of situations when smartphone connectivity is limited (Sign on at a desktop computer with no WiFi available for the smartphone and no high speed mobile internet connection).

Also, the evaluation of wallets was conducted at a particular time (April to June 2020) and only the three selected DIDM digital wallets had the level of maturity that was necessary for our user tests. However, even at that time these products were constantly changing significant aspects of their functionality (e.g. backups), one became temporarily unusable.

Finally, we could test the available digital wallets only with demo scenarios provided by the solutions themselves. The use cases were chosen by solutions, thus might be selective to work particularly well, and this was of course not a productive environment. Still, even in this optimized environment, the issues were apparent.

6 Conclusion

After conducting an initial analysis of 23 Blockchain-based DIDM solutions and performing 18 user tests with three of the more advanced applications, the current usability problem of DIDM and SSI solutions can be defined as significant. Principally, we found the overall issue that the new concept of decentralized identity while apparently seeming self-evident to its developers is not explained well enough to the end users, which leads to substantial problems that encumber the practical use and purpose of the technology.

In addition, the major importance of easy-to-use functionalities to backup and recover the account as fundamental step in the identity lifecycle does not seem to be understood by the developers. Its importance is not prominently highlighted in the applications — maybe as the functions currently are too complex for the average user and their practicality is debatable.

We want to conclude by highlighting the concern that even though such solutions are marketed as ready to be practically used, their usability and current state of the technology stack might deprive end users of experiencing the entire range of claimed privacy and security benefits. DIDM solutions that exist nowadays need to provide a solidified explanatory basis and carefully guide the user with a good user experience, for example through the interface. This requires an explanation that is beyond providing basic instructions on how to use certain functions but also providing clarification of why certain functions need to be carried out in one way, while solutions that are more traditional and familiar to users have been offering similar functions in another way. To sum up the results of our study, to

our knowledge the existing market does not yet offer Blockchain-based DIdM solutions with usability mature enough to be accepted and securely used by end users.

Acknowledgements Project DECIDE was funded and supported by the Next Generation Internet Initiative and was selected by the open call for proposals from the Partnership for innovative technological solutions to ensure privacy and enhance trust for the human-centric Internet — NGI TRUST (<https://www.ngi.eu/ngi-projects/ngi-trust/>).

References

1. MarketsandMarkets: Digital Identity Solutions Market Size, Share and Global Market Forecast to 2024. <https://www.marketsandmarkets.com/Market-Reports/digital-identity-solutions-market-247527694.html>
2. White, O.: Digital Identification: A Key to Inclusive Growth. McKinsey Global Institute, Washington, D.C (2019)
3. Kubach, M., Schunck, C.H., Sellung, R., Roßnagel, H.: Self-sovereign and Decentralized identity as the future of identity management? In: Open Identity Summit 2020, (GI-Edition - Lecture Notes in Informatics (LNI). Proceedings P-305), S. 35–47 Bonn, Köllen, (2020)
4. Simons, A.: Decentralized Digital Identities and Blockchain: The Future as We See it. <https://www.microsoft.com/en-us/microsoft-365/blog/2018/02/12/decentralized-digital-identities-and-blockchain-the-future-as-we-see-it/>
5. Arun, J.S.: Reimagining the Future of Identity Management With Blockchain. <https://securityintelligence.com/reimagining-the-future-of-identity-management-with-blockchain/>
6. Introducing the European Blockchain Services Infrastructure (EBSI). <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/ebsi>
7. SSI eIDAS Bridge reference Implementation. <https://joinup.ec.europa.eu/solution/ssi-eidas-bridge-reference-implementation>
8. Haenen, A., Jessen, J.: Sustainable hybrid financial services models. <https://www.accenture.com/nl-en/blogs/insights>
9. Smolenski, N.: Identity and Digital Self-Sovereignty. <https://medium.com/learning-mac-hine-blog/identity-and-digital-self-sovereignty-1f3faab7d9e3>
10. Flechais, I., Mascolo, C., Sasse, M.A.: Integrating security and usability into the requirements and design process. *Int. J. Electron. Secur. Digit. Forensics*, **1**, 12–26 (2007)
11. U-Prove. <https://www.microsoft.com/en-us/research/project/u-prove/?from=https%3A%2F%2Fresearch.microsoft.com%2Fen-us%2Fprojects%2Fu-prove>
12. Zibuschka, J., Hinz, O., Roßnagel, H., Muntermann, J.: Zahlungsbereitschaft für Föderiertes Identitätsmanagement. In: Der digitale Bürger und seine Identität. Nomos Verlagsgesellschaft mbH & Co. KG. S. 225–246 (2016)
13. Koçak, S.A., Alptekin, G.I., Bener, A.B.: Integrating Environmental Sustainability in Software Product Quality. Presented at the RE4SuSy@ RE (2015)

14. Khayretdinova, A., Kubach, M.: A methodology for experimental evaluation of a software assistant for the development of safe and economically viable software. In: Presented at the 15th International Conference on Web Information Systems and Technologies (2019)
15. Zibuschka, J., Roßnagel, H.: Stakeholder economics of identity management infrastructures for the web. In: Proceedings of the 17th Nordic Workshop on Secure IT Systems (NordSec 2012). Karlskrona, Sweden (2012)
16. Kubach, M., Roßnagel, H., Sellung, R.: Service providers' requirements for eID solutions: empirical evidence from the leisure sector. In: Hühnlein, D., Roßnagel, H. (eds.) Open Identity Summit 2013—Lecture Notes in Informatics (LNI)—Proceedings. S. 69–81. Ges. für Informatik, Bonn (2013)
17. Simons, A., Management, V.P. of P., Division, M.I.: Decentralized digital identities and blockchain: The future as we see it. <https://www.microsoft.com/en-us/microsoft-365/blog/2018/02/12/decentralized-digital-identities-and-blockchain-the-future-as-we-see-it/>
18. Aitken, R.: Blockchain To The Rescue Creating A 'New Future' For Digital Identities. <https://www.forbes.com/sites/rogeraitken/2018/01/07/blockchain-to-the-rescue-creating-a-new-future-for-digital-identities/>
19. Use case spotlight: Quick SSI integration for identity and access management with IdRamp, Use case spotlight: Quick SSI integration for identity and access management with IdRamp
20. Allen, C.: The Path to Self-Sovereign Identity. <https://github.com/ChristopherA/self-sovereign-identity>
21. Jessen, J., McLeese, V., van de Weerd, M.: Identity management on blockchain: a new era of data privacy. <https://www.accenture-insights.nl/en-us/articles/identity-management-on-blockchain>
22. van Bokkem, D., Hageman, R., Koning, G., Nguyen, L., Zarin, N.: Self-Sovereign Identity Solutions: The Necessity of Blockchain Technology. ArXiv190412816 Cs. (2019)
23. Wang, F., De Filippi, P.: Self-sovereign identity in a globalized world: credentials-based identity systems as a driver for economic inclusion. *Front. Blockchain*, **2**, 1–22 (2020). <https://doi.org/10.3389/fbloc.2019.00028>
24. Mühle, A., Grüner, A., Gayvoronskaya, T., Meinel, C.: A survey on essential components of a self-sovereign identity. *Comput. Sci. Rev.* **30**, 80–86 (2018). <https://doi.org/10.1016/j.cosrev.2018.10.002>
25. Cameron, K.: The Laws of Identity. Microsoft Corporation (2005)
26. Lesavre, L., Varin, P., Mell, P., Davidson, M., Shook, J.: A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems. National Institute of Standards and Technology (2020)
27. Kuperberg, M.: Blockchain-based identity management: a survey from the enterprise and ecosystem perspective. *IEEE Trans. Eng. Manag.* (2019). <https://doi.org/10.1109/TEM.2019.2926471>
28. The Importance of User Experience for Blockchain Applications. <https://upvest.co/blog/the-importance-of-user-experience-for-blockchain-applications>
29. Anderson, R., Moore, T.: The economics of information security. *Science* **314**, 610–613 (2006). <https://doi.org/10.1126/science.1130992>
30. Akerlof, G.A.: The Market for “Lemons”: Quality Uncertainty and the Market Mechanism. *Q. J. Econ.* **488**, 235–251 (1970)

31. Kirlappos, I., Sasse, M.A.: What usable security really means : trusting and engaging users. *Hum Asp Inf Secur Priv Trust HAS Lect Notes Comput Sci.* **11** (2014)
32. Zurko, M.E., Simon, R.T., Street, S.: User-Center. *Secur.* **1**, 1–9 (1996)
33. Dunphy, P., Petitcolas, F.: A First Look at Identity Management Schemes on the Blockchain 2018 (2018)
34. Fischer-Hübner, S., Lacono, L., Möller, S.: Usable security und privacy. *Datenschutz Datensicherheit - DuD.* **34**, 773–782 (2010)
35. Prieto, L.P., Rodriguez-Triana, M.J., Kusmin, M., Laanpere, M.: Maybe poor Jhonny Really Cannot Encrypt—The Case for a Complexity Theory for Usa-ble Security. In: *CEUR Workshop Proc.* S. 53–59 (2017)
36. uPort—Tools for Decentralized Identity and Trusted Data. <https://www.uport.me/>
37. Products - Evernym's Verifiable Credential Platform. <https://www.evernym.com/products/>
38. W3C: Decentralized Identifiers (DIDs) v1.0. <https://www.w3.org/TR/did-core/>
39. Authentication. <https://identity.foundation/working-groups/authentication.html>
40. Schrepp, M., Hinderks, A., Thomaschewski, J.: Applying the User Experience Questionnaire (UEQ) in Different Evaluation Scenarios. In: Marcus, A. (ed.) *Design, User Experience, and Usability. Theories, Methods, and Tools for Designing the User Experience.* S. 383–392. Springer International Publishing, Cham (2014)
41. Schrepp, M., Hinderks, A., Thomaschewski, J.: Construction of a Benchmark for the User Experience Questionnaire (UEQ). *IJIMAI.* **4**, 40–44 (2017)
42. Laugwitz, B., Held, T., Schrepp, M.: Construction and evaluation of a user experience questionnaire. In: *Symposium of the Austrian HCI and usability engineering group.* S. 63–76. Springer (2008)
43. Roßnagel, H., Zibuschka, J., Hinz, O., Muntermann, J.: Users' willingness to pay for web identity management systems. *Eur. J. Inf. Syst.* **23**, 36–50 (2014). <https://doi.org/10.1057/ejis.2013.33>

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

