Towards a Disaster Resilient Self-Sovereign Identity Research Plan

Kalin Kostadinov

April 28, 2021

Background of the Research

Every person on the Internet uses at least one digital identity and Service providers rely on them for building trust with their users. Unfortunately, the creators of the Internet have not designed a unified identity layer. Thus, service providers need to handle authentication and authorization themselves [1] which explains why every service has at least one identity management system. But, those systems are in control of users' identities, so identity owners cannot administer their data.

In recent years, identity management has become a big concern for governments which has led to a large amount of research and regulations in the field [2]. There is a need for a novel identity management system, and its formal description stands in the middle of all the work [3]. It promises to not take control over an identity from its rightful owner and achieves this by satisfying the requirements for Self-Sovereign Identity [4]. SSI allows every identity holder to store and manage their data. For that, they need to use resources under their jurisdiction.

There are already several implementations that cover part of SSI's properties [5], and they have matured over the past couple of years. However, the biggest obstacle which prevents them all from going mainstream is the problem of adoption. Self-Sovereign Identity management systems have one of two problems in this regard. Part of them relies on global blockchains that contain the entire transaction history of all users. In this case, global consensus is a must that prevents such systems from operating in several situations. For example, in an offline setting or when transaction times need to be as low as possible. Other SSI managers either use local blockchains or do not use a blockchain at all. Such systems are fully distributed and need no global consensus, thus solving the problem of the former group. But, they do not employ any mechanism for disaster resilience, and in case users lose access to their digital identity, they cannot recover it. All in all, availability suffers.

Research Question

There is a need for a solution to the problem of fully distributed SSI management systems. It will allow those systems to outweigh the other SSI managers when it comes to service availability. Thus, the problem of availability as a sub-problem of adoption is a research area that is worthwhile exploring.

The following research question will be laid at the center of this work: How to make fully distributed Self-Sovereign Identity management systems disaster resilient?

It is clear that to make a system resilient to data loss, a protocol adding redundancy is in need because identities have to be in at least two separate locations. Redundancy, however, adds some complexity and overhead to the system. Also, it calls for a caching mechanism that, in an offline setting, allows temporary storage of transactions before synchronizing them with other system deployments. And if there are multiple nodes having control over the same identity, there needs to be a mechanism for access revocation. Two ideas emerge from these observations.

The first one is to keep the SSI management system on a master remote server, controlled by the identity holder. A central node that is under the jurisdiction of the identity owner will add some unwanted overhead. However, the benefit is that users will easily revoke remote access, quickly transfer control to other devices and reliably restore lost identity access. But, there needs to be a caching mechanism in the case of offline transactions.

The second idea is to reproduce the blockchain from the knowledge of other users about the lost identity. Blockchain recreation, however, increases complexity because there might be some offline users during the rebuilding process. Also, some might not be honest about previous transactions, and others might not even exist anymore. The benefit here is that there is no need for a caching mechanism, but the revocation will only be possible through peers, which ignore the revoked node. Privacy is also a concern in this instance. It is not desirable to keep identity information, even if it is encrypted, on untrusted nodes.

Method

The Delft Blockchain Lab develops one of the Self-Sovereign Identity management systems, called IPv8 [6]. It is arguably the most sophisticated SSI management system. However, the issue with IPv8 is that it does not offer long-term data resilience, thus not offering a mechanism for recovery from identity loss. Every user has its blockchain, called TrustChain [7], for managing their identity. And Trustchain allows IPv8 to work as a fully distributed system. The idea behind this design decision is that users have more control over their own identity if they are the only ones physically possessing their data blocks. Also, IPv8 functions in situations that SSI managers with global blockchains cannot work.

Mobile applications are the most effective way of hosting an identity management system like IPv8. However, it is not clear how users are supposed to recover their identities when access to them is lost. That is why I plan on using IPv8 as a platform to develop a solution for my research question.

My research will begin with a literature search for systems in other fields which have already solved the problem of availability for self-contained applications. If I can discover more ideas, I will use them during the later parts of the research. Furthermore, both solutions will be designed and evaluated. The one which adds less complexity and overhead to the usage of IPv8 will be picked and later implemented and integrated with IPv8. The research will conclude with a paper that will explain the problem in more detail and describe the solution of choice. Furthermore, it will include implementation details and a conclusion on whether it solves the disaster resilience problem.

Since I am going to use IPv8 as a base for improvements, I have the task of exploring its implementation in Kotlin for the super app [8], which the Delft Blockchain Lab is currently working on. My goal is to assess the application and find a suitable approach for integrating my implementation.

I was previously involved in the development of another application that also uses IPv8 for storing COVID-19 immunity certificates [9]. The main objective of that project was to create a user-friendly GUI. If I implement the remote server solution, I can use the COVID-19 project as an experimental environment for my findings since it already uses REST API to communicate with the IPv8 deployment. It also relies on React Native [10] for its GUI. That means IPv8 can get an easy implementation for iOS, which the lab is lacking.

Depending on the protocol's design, it might be helpful to keep the core back-end that is going to run on the mobile device in Python, as is the implementation of IPv8 [11] itself. There is still no publicly available tool that efficiently builds Python applications for Android, iOS, and other mobile or embedded operating systems. Therefore, I might make use of my development, called Porthon. Its goal is to make Python applications portable and resource-efficient. Currently, there is a working version of the IPv8 implementation in Python for Android, and one for iOS is underway.

A further development that goes beyond the goals of this research project will be the creation of emergency access "terminals" that will be available at border control, for instance. They will allow someone access to their identity manager with restricted controls if their other SSI managers are not available. Those emergency "terminals" should only allow for verification of attestations.

Planning of the Research Project

For week 1 of the research project, I have to submit a project plan. To achieve this, I aim to read through the following research from Uwe Der, Stefan Jähnichen, and Jan Sürmeli [12], Alexander Mühle, Andreas Grüner, Tatiana Gayvoronskaya, and Christoph Meine [13], Quinten Stokkink, Dick Epema, and Johan Pouwelse [6], Q. Stokkink and J. Pouwelse [14], A. Tobin and D. Reed [15], D.S. Baars [16]. I will also follow the citations from the papers mentioned above. And will try finding others that focus more on the issues of availability. Given my findings, I will write my research plan. Deadlines: April 19th - Planning Week 1, April 20th - Information Literacy, April 25th - Research Plan.

During week 2, I will search for best practices in solving availability issues in the mobile applications field. Any such ideas will be helpful in week 3. I will spend some time deciding which of the two proposed solutions is better feasible, given the time and technology constraints. In week 2, I have to also present my research plan to my supervisors and peers. Deadlines: May 2nd - Research Plan Presentation.

Week 3, I will work on formally defining a solution for the problem. This week is supposed to produce some parts of the final research paper as well. Deadlines: May 6th - Academic Communication Skills Assignment 1: First 300 Words.

Week 4 will set the beginning of the implementation process of the protocol. During it, I will work on adding a recovery mechanism for IPv8. Deadlines: May 16th - Academic Communication Skills Assignment 2: Midterm Poster for Feedback.

In Week 5, implementation of the recovery algorithm will continue. Since this is the halfway mark, I will have a midterm presentation as well. Deadlines: May 19th - Midterm Poster.

During week 6, access revocation will be at the center of most of my efforts. Deadlines: May 27th - Academic Communication Skills Assignment 3: Improve First 300 Words, and Add Section of 300 Words.

For week 7, I plan on working on the caching algorithm that will allow for offline transactions to be possible. There are no deadlines for week 7.

In week 8, integration of the protocol with IPv8 will start. Deadlines: June 7th - Paper Draft V1, June 10th - Peer Reviews.

Week 9 will consist of the integration and testing of the protocol. Deadlines: June 16th - Paper Draft V2.

During week 10, most of the work I will spend on finalizing the poster and the research paper. Deadlines: June 27th - Academic Communication Skills Assignment 4: Final Poster for Feedback, June 27th - Final Paper.

Week 11 is devoted to preparations for the final poster presentation. Deadlines: June 29th - Final Poster.

Meetings with my supervisors are scheduled every Tuesday at 10:00. During them, we discuss details around the progress of the project.

References

[1] Gergely Alpár, Jaap-Henk Hoepman, and Johanneke Siljee. The identity crisis. security, privacy and usability issues in identity management. 2011.

[2] European Commission. Regulation (eu) 2016/679 of the european parliament and of the council. 2016.

[3] Md Sadek Ferdous, Farida Chowdhury, and Madini O. Alassafi. In search of self-sovereign identity leveraging blockchain technology. *IEEE Access*, 7:103059–103079, 2019.

[4] Christopher Allen. The path to self-sovereign identity. 2016.

[5] Dirk van Bokkem, Rico Hageman, Gijs Koning, Tat Luat Nguyen, and Naqib Zarin. Self-sovereign identity solutions: The necessity of blockchain technology. 04 2019.

[6] Quinten Stokkink, Dick Epema, and Johan Pouwelse. A truly self-sovereign identity system. 2020.

[7] Pim Otte, Martijn de Vos, and Johan Pouwelse. Trustchain: A sybil-resistant scalable blockchain. *Future Generation Computer Systems: the international journal of grid computing: theory, methods and applications*, 107:770–780, June 2020.

[8] Tribler. Trustchain super app.

[9] Tribler. Immune: Building a critical infrastructure for the nation-wide identification of recovered covid-19 patients.

[10] Facebook. React native.

[11] Tribler. Ipv8.

[12] Uwe Der, Stefan Jähnichen, and Jan Sürmeli. Self-sovereign identity - opportunities and challenges for the digital revolution. *CoRR*, abs/1712.01767, 2017.

[13] Alexander Mühle, Andreas Grüner, Tatiana Gayvoronskaya, and Christoph Meinel. A survey on essential components of a self-sovereign identity. *Computer Science Review*, 30:80–86, 2018.

[14] Quinten Stokkink and Johan Pouwelse. Deployment of a blockchain-based self-sovereign identity. *CoRR*, abs/1806.01926, 2018.

[15] A. Tobin and D. Reed. The inevitable rise of self-sovereign identity. 2016.

[16] D.S. Baars. Towards self-sovereign identity using blockchain technology. October 2016.