Towards a Disaster Resilient Self-Sovereign Identity

Kalin Kostadinov , Martijn de Vos , Johan Pouwelse
k.k.kostadinov@student.tudelft.nl , m.a.devos-1@tudelft.nl
Delft University of Technology

Abstract

1 Introduction

2 Problem Description

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 [2] 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 [3]. There is a need for a novel identity management system, and its formal description stands in the middle of all the work [4]. It promises to not take control over an identity from its rightful owner and achieves this by satisfying the requirements for Self-Sovereign Identity [1]. 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.

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.

3 Method

4 Experimental Setup and Results

5 Responsible Research

6 Discussion

7 Conclusions and Future Work

References

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

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

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

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

[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.