Privacy-Aware Blockchain-Based Self-Sovereign Identity

Remy Duijsens , Martijn de Vos , Johan Pouwelse
r.w.j.p.duijsens@student.tudelft.nl, m.a.devos-1@tudelft.nl
Delft University of Technology

Abstract

No abstract yet.

1 Introduction

The internet was invented to be a distributed and open system for everyone. Yet in the 21st century, the decay of its users' privacy is an ongoing problem [1]. This is because machines are the endpoints within the internet and not the users. To be able to track and store users, online services implement the authentication layers themselves, sometimes with the help of an Identity Provider, such as Facebook or Google. As such, they create user profiles that are strongly tied to the online behaviour of the users. That is problematic, as this encourages for example massive data mining which can be valuable to companies, governments, and even malicious parties [2].

By a survey of InnoValor, it became clear that (Dutch) citizens are feeling a lack of control and a desire to be in more control of their online identities [3]. This is where the notion of a self-sovereign identity is introduced. It gives people back their authority over their own digital identities. Christopher Allen has proposed 10 principles that should be satisfied by this self-sovereign identity (SSI) [4]. Several implementations for SSI have been proposed in academic literature, for example, several blockchain approaches of which one is a solution for Dutch digital passports [5]. However, not many critical reviews on the current SSI technology have been proposed. One of the biggest problems posed for blockchain-based implementations is guarantying privacy to its users [6].

This research aims at finding the technical limitations for privacy protection of the current blockchain-based SSI implementations. It also tries to propose solutions to these limitations supported by a Proof-of-Concept implementation and, where appropriate, mention the possible adoption issues of these proposals.

Our work focuses on the following overarching research question:

> *What are the technical limitations for privacy protection in current blockchain-based SSI implementations?*

The paper will be structured using a bottom-up approach, where the main research question is split up into the following sub-questions:

- What are the privacy issues that SSI tries to solve?
- How does blockchain technology address privacy and what are its limitations?
- What are the current blockchain-based SSI implementations and how do they perform?
- How can we create a privacy-aware blockchain-based SSI implementation?
- What practical adoption issues arise for the current and proposed blockchain-based SSI implementations?

First, we will examine the privacy-related issues that are present in the technology we use today and that SSI tries to solve. We then look at current SSI technology and in particular the blockchain-based SSI implementations. From here the research will continue to focus on blockchain technology and its issues regarding privacy. What follows next is an overview of blockchain-based SSI implementations in an attempt to show the current shortcomings related to privacy protection and how to resolve these. This section also provides an implementation flowchart based on the trade-offs related to privacy. At last, we regard a more practical view of the privacy problem and the adoption issues that the current implementations might have. These issues will be further demonstrated via a Proof-of-Concept implementation.

The Proof-of-Concept implementation supplements the literature study in a practical way that is required to completely answer the main research question. First, it will demonstrate how current technology works and how it encapsulates and protects privacy through all the layers of the currently existing implementations. This will be done on a particular implementation created here at TU Delft, the Trustchain-superapp[1]. Secondly, where applicable, it shows how to improve the current implementation to achieve better practical privacy protection. The combination of a theoretical review of the current technology and the Proof-of-Concept implementation will provide a clear and complete picture of the current state of privacy protection in blockchain-based SSI. This allows for conclusions to arise on, for example, the question of possible adoption issues. It also provides a good reference point for future research on the subject.

[1] https://github.com/Tribler/trustchain-superapp

2 Problem Description

The past five years there have been a rise in literature on blockchain technology [7]. The original use-case of this technology, Bitcoin, has enabled a technology to truly enable decentralized computer networks [8]. Now this area is explored to find other application domains. One prominent domain is digital identity management. Like the monetary system, identity management is currently a mainly centralized business. As presented in the introduction of this paper the motivation to decentralize identity management is clear. Self-sovereign identities provide a conceptual solution to decentralized identity management.

The original article by Christopher Allen provides a technology independent description of SSI. In the years after this publication several types of SSI implementations have been proposed in both white papers and academic articles. The current trend in SSI solutions is based on blockchain technology, a natural catalyst of decentralization. However, blockchain technology also has its shortcomings. A recent survey on blockchain technology regarding privacy shows that there are still problems to be discussed and improved [9].

This problems translates naturally to blockchain-based SSI implementations. A repository of identity related blockchain applications shows the amount of different initiatives [2]. These initiatives are not bound to a specific type of blockchain technology and thus use many different solutions in the broad spectrum of blockchain [10]. There is however a lack of research of blockchain-based SSI implementations regarding privacy.

This research compares current blockchain-based SSI implementations based on the underlying blockchain models. The pros and cons of each model will be explained and the trade-offs in terms of privacy will be discussed. Furthermore, the notion of privacy is not a static one. Privacy needs and expectations are as various as the different cultures and societies around the world [11]. This should be accounted for in the deployment of blockchain-based SSI and thus will be included in the discussion.

3 Evaluation

3.1 Privacy

3.2 Blockchain Technology

3.3 SSI Implementations

3.4 Privacy Evaluation

3.4.1 Flowchart

3.4.2 Deployment

4 Experimental work

No results yet.

5 Responsible Research

Reflect on the ethical aspects of your research and discuss the reproducibility of your methods.

[2] https://github.com/peacekeeper/blockchain-identity

6 Discussion

No discussion yet.

7 Conclusions and Future Work

No conclusion yet.

References

[1] Smit, A. (2020). Identity Reboot: Reimagining Data Privacy for the 21st Century (1st ed.). MintBit Ltd.

[2] Jiang, L., Ren, Y., Wang, J., Xu, L., Yuan, J. (2014). Information Security in Big Data: Privacy and Data Mining. IEEE Access. 2. 1-28. 10.1109/ACCESS.2014.2362522.

[3] InnoValor. (2016). Persoonlijke data, onder controle? url: https://innovalor.nl/personal-data-store/ (visited on 01/05/2021)

[4] Allen C. (2016). The Path to Self-Sovereign Identity. url: http://www.coindesk.com/path-self-sovereign-identity/ (visited on 01/05/2021)

[5] Stokkink, Q. and Pouwelse, J. (2018). Deployment of a blockchain-based self-sovereign identity. In 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pages 1336-1342.

[6] Baars, D. (2016). Towards self-sovereign identity using blockchain technology. Master's thesis, University of Twente.

[7] Hellwig. (2020). Build Your Own Blockchain: A Practical Guide to Distributed Ledger Technology (Management for Professionals) (1st ed.). Springer.

[8] Nakamoto, S. (2009). Bitcoin: A Peer-to-Peer Electronic Cash System.

[9] Wang, D., Wang, Y., Zhao, J. (2020). A Survey on Privacy Protection of Blockchain: The Technology and Application. IEEE Access. PP. 1-1. 10.1109/ACCESS.2020.2994294.

[10] Syed, T. A., Alzahrani, A., Jan, S., Siddiqui, M. S., Nadeem, A., Alghamdi, T. (2019). A comparative analysis of blockchain architecture and its applications: Problems and recommendations. IEEE access, 7, 176838-176869

[11] Cullen, R. (2009). Culture, identity and information privacy in the age of digital government. Online Information Review. 33. 405-421. 10.1108/14684520910969871.