Research Plan for A Privacy-Aware Blockchain-Based SSI Implementation

Remy Duijsens

April 29, 2021

Background of the research

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. This is because machines are the endpoints within the internet and not its 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. 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 [6]. 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) [1]. 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 [11]. 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 [2]. 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 via a Proof-of-Concept implementation and, where appropriate, mention the possible adoption issues of these proposals.

Research Question

This research of the current blockchain-based SSI implementations and the privacy protection problem will be constructed using a bottom-up approach. First, it 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 a Proof-of-Concept implementation in an attempt to show the current shortcomings related to privacy protection and how to resolve these. At last, we regard a more practical view of the privacy problem and the adoption issues that the current and Proof-of-Concept implementations might have. We conclude this research by answering the main question of this research project:

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

Regarding the previously mentioned bottom-up approach, we can split this main question 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?

Method

The aims that have been set in the previous section will be mainly accomplished by literature studies on the currently known blockchain-based SSI implementations. Since most of the implementations are yet only defined as academic blueprints, the practical evaluation is limited. However, the project supervisors offer a hands-on experience with the trustchain-superapp which is available as open-source software on https://github.com/Tribler/trustchain-superapp. Several implementation details from the literature can be evaluated or improved with the use of this repository. This can be done in the form of a Proof-of-Concept implementation. The engineering contribution that is achieved by this Proof-of-Concept comprises several showcases. First, it will demonstrate how current technology works and how it encapsulates and protects privacy through all the layers of the currently existing implementations. Secondly, where applicable, it shows how to improve the current implementations to achieve better practical privacy protection. And at last, it will demonstrate the technical limitations for privacy protection of the implementations and at which point privacy must be warranted by an extra (non-technical) layer of legislation. The combination of a theoretical review of the used 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.

Planning of the research project

Week 1

1. Readings (10 hours):
   (a) A survey on essential components of a self-sovereign identity [8]
   (b) The Inevitable Rise of Self-Sovereign Identity [12]
   (c) Self-sovereign Identity - Opportunitie and Challenges for the Digital Revolution [4]
   (d) Towards Self-Sovereign Identity using Blockchain Technology [2]
   (e) Deployment of a Blockchain-Based Self-Sovereign Identity [11]
   (f) A Truly Self-Sovereign Identity System [10]
2. Research Activities:
   (a) Find more literature that relates to the research question that fits my interests and categorize these works for later usage (4 hours).
   (b) Taking a look at and exploring the trustchain-superapp repository and compile the project locally (2 hours).
3. Meetings:

(a) Internal group meeting April 19th at 14:00: discussing possible research questions (1 hour).

(b) Group meeting with supervisors April 20th at 10:00: Discussing the research questions and the research plan for week 1 (1 hour).

4. Other Activities:

(a) Deadline research planning week 1 (2 hours) at Monday April 19th 23:59.

(b) Deadline Information Literacy 2 course (2 hours) at Tuesday April 20th at 22:00.

(c) Deadline complete research plan (4 hours) at Sunday April 25th at 23:59.

Week 2

1. Readings:

(a) Read articles on current privacy issues and how SSI technology addresses these issues.

(b) Read (parts of) the book Identity Reboot: Reimagining Data Privacy for the 21st Century [9].

2. Research Activities:

(a) Finish first sub-question: research and draft text.

3. Meetings:

(a) Group meeting with supervisors Monday at 14:00: Discussing the submitted research plans (1 hour).

4. Other Activities:

(a) Research plan presentations

(b) Deadline Research plan presentation at May 2nd at 23:59

Week 3

1. Readings:

(a) Get comfortable with blockchain (and its history) and read introductory articles/books.

(b) Read (parts of) the book Mastering Blockchain: Unlocking the Power of Cryptocurrencies, Smart Contracts, and Decentralized Applications [7].

(c) Read (parts of) the book Mastering Blockchain: A deep dive into distributed ledgers, consensus protocols, smart contracts, DApps, cryptocurrencies, Ethereum, and more [3].

2. Research Activities:

(a) Finish second sub-question: research and draft text

3. Meetings:

(a) Group meeting with supervisors Tuesday at 10:00 (1 hour).

4. Other Activities:

(a) Deadline ACS Assignment 1 May 6th at 23:59

(b) Scientific Writing May 7th at 09:00

Week 4

1. Readings:
   (a) Read blockchain articles/papers related to SSI technology and privacy.
   (b) Gather and read about several blockchain-based SSI implementations and research their solutions and problems regarding privacy.
2. Research Activities:
   (a) Finish third sub-question: research and draft text.
   (b) Get familiar with the trustchain-superapp repository and if available other current implementations.
3. Meetings:
   (a) Group meeting with supervisors Tuesday at 10:00 (1 hour).
4. Other Activities:
   (a) Session responsible research May 10th at 10:45
   (b) Deadline ACS Assignment 2 May 16th at 23:59

Week 5

1. Readings:
   (a) Found a book that might be useful: Build Your Own Blockchain: A Practical Guide to Distributed Ledger Technology (Management for Professionals) [5].
2. Research Activities:
   (a) Work on fourth sub-question: research and Proof-of-Concept implementation.
3. Meetings:
   (a) Group meeting with supervisors Tuesday at 10:00 (1 hour).
4. Other Activities:
   (a) Deadline Midterm Poster May 19th at 23:59
   (b) Midterm Presentation May 19th
   (c) Scientific Writing May 17th at 15:45

Week 6

1. Readings:
   (a) .
2. Research Activities:
   (a) Work on fourth sub-question: research and Proof-of-Concept implementation.
3. Meetings:
   (a) Group meeting with supervisors Tuesday at 10:00 (1 hour).
4. Other Activities:
   (a) Deadline ACS Assignment 3 May 27th at 23:59
   (b) Scientific Writing May 28th at 08:45

Week 7

1. Readings:
   (a) .
2. Research Activities:
   (a) Finish fourth sub-question: research and Proof-of-Concept implementation, start draft text
3. Meetings:
   (a) Group meeting with supervisors Tuesday at 10:00 (1 hour).
4. Other Activities:
   (a) Scientific Writing Coaching Session June 4th

Week 8

1. Readings:
   (a) .
2. Research Activities:
   (a) Finish fifth sub-question and conclusion: research and draft text.
   (b) Reserved time for work on the Proof-of-Concept implementation.
3. Meetings:
   (a) Group meeting with supervisors Tuesday at 10:00 (1 hour).
4. Other Activities:
   (a) Deadline Paper draft v1 June 7th at 23:59
   (b) Deadline Draft peer review June 10th at 23:59
   (c) Scientific Writing Coaching Session June 11th

Week 9

1. Readings:
   (a) .
2. Research Activities:
   (a) Finish Proof-of-Concept implementation, deliverable state.
   (b) Critical view on all draft sub-sections and prepare for final draft deadline.
3. Meetings:
   (a) Group meeting with supervisors Tuesday at 10:00 (1 hour).
4. Other Activities:
   (a) Deadline Paper draft v2 June 16th at 23:59
   (b) Scientific Writing Coaching Session June 18th

Week 10

1. Readings:
   (a) –
2. Research Activities:
   (a) Finish the final paper and incorporate all final feedback from supervisors and peers.
3. Meetings:
   (a) Group meeting with supervisors Tuesday at 10:00 (1 hour).
4. Other Activities:
   (a) Scientific Writing Coaching Session June 25th
   (b) Deadline ACS Assignment 4 June 27th at 23:59
   (c) Deadline Final paper June 27th at 23:59

Week 11

1. Readings:
   (a) –
2. Research Activities:
   (a) Working on final poster and practice final presentation.
3. Meetings:
   (a) Group meeting with supervisors Tuesday at 10:00 (1 hour).
4. Other Activities:
   (a) Deadline Final poster June 29th at 23:59
   (b) Presentation Session 1 July 1st
   (c) Presentation Session 2 July 2nd

References

[1] Allen C. (2016). The Path to Self-Sovereign Identity. url: http://www.coindesk.com/path- self-sovereign- identity/ (visited on 07/05/2016)

[2] Baars, D. (2016). Towards self-sovereign identity using blockchain technology. Masterâs thesis, University of Twente.

[3] Bashir, I. (2020). Mastering Blockchain: A deep dive into distributed ledgers, consensus protocols, smart contracts, DApps, cryptocurrencies, Ethereum, and more (3rd ed.). Packt Publishing.

[4] Der, U., Jähnichen, S., and Sürmeli, J. (2017). Self-sovereign Identity − Opportunities and Challenges for the Digital Revolution.

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

[6] InnoValor. (2016). Persoonlijke data, onder controle? url: https://innovalor.nl/personal-data-store/ (visited on 05/23/2016)

[7] Lantz, L. (2020). Mastering Blockchain: Unlocking the Power of Cryptocurrencies, Smart Contracts, and Decentralized Applications (1st ed.). O'Reilly UK Ltd.

[8] Mühle, A., Grüner, A., Gayvoronskaya, T., and Meinel, C.(2018). A survey on essential components of a self-sovereign identity. Computer Science Review, 30:80â86.

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

[10] Stokkink, Q., Epema, D., and Pouwelse, J.. (2020). A Truly Self-Sovereign Identity System.

[11] 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.

[12] Tobin, A. and Reed, D. (2016). The inevitable rise of self-sovereign identity, Sovrin Found. accessed: 08/10/18. [Online]. Available: https://sovrin.org/wp-content/uploads/2018/03/The-Inevitable-Rise-of-SelfSovereign-Identity.pdf.