Privacy-Aware Blockchain-Based Self-Sovereign Identity

Different main title? An Evaluation of Privacy Protection on Blockchain-Based Self-Sovereign Identity

Running title: Privacy-Aware Blockchain-Based SSI

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

Digital identity management has been established in a mainly centralized manner. In response to a lack of control, the concept of Self-Sovereign Identity (SSI) was defined to enable decentralization. Recently, this concept gained traction and several implementations have been proposed. The decentralized nature of blockchain technology was combined with the concept of SSI. However, no critical review on the privacy protection of this technology in combination with SSI currently exists. This research provides an overview of blockchain technology and current blockchain-based SSI implementations regarding privacy protection. It proposes a model for determining the privacy protection that specific solutions can offer. Furthermore, the practical adoption issues of current implementations in terms of privacy are considered. The result is a model for comparing different blockchain-based SSI solutions and the trade-offs that can be deduced. In the light of the practical adoption issues, arguments for a more localized deployment of blockchain-based SSI are given.

1 Introduction

The internet was invented to be a distributed and open system for everyone. However, 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 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 feel 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 ten 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 provides a clear overview of blockchain technology of several existing solutions regarding privacy trade-offs and, where appropriate, mention the possible adoption issues of these solutions.

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 preserve privacy?
- How can we create a privacy-aware blockchain-based SSI implementation?
- What practical adoption issues arise for the current blockchain-based SSI implementations regarding privacy protection?

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 to show the state of privacy protection. 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. This provides a good reference point for future research on the subject.

2 Problem Description

In the past decade, there has been a rise in the 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. As 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 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 problem translates naturally to blockchain-based SSI implementations. A repository of identity-related blockchain applications shows the amount of different initiatives [1]. These initiatives are not bound to a specific type of blockchain technology and use many different solutions in the broad spectrum of blockchain [10]. There is, however, a lack of research on 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 varied 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

+- 5 pages total

3.1 Privacy

In the 21st century, privacy awareness is more present than ever before [12]. Privacy is defined as ”someone’s right to keep their personal matters and relationships secret” by Cambridge Dictionary[2]. This isn’t just limited to this definition. The fact that privacy is a right is part of our legislation, and with the recent addition of the GDPR in Europe, it is present in all digital services. However, privacy protection is still not up to the expectations of a lot of people. This became apparent after a survey by InnoValor, stating that citizens feel a lack of control of their digital identity. [3].

The current digital environment is mainly maintained in a centralized manner. When an online service is used, digital identity management is implemented either by this service or by a Federated Identity Management (FIM) platform such as Facebook. The digital identity is stored, monitored, and owned by the service. Clearly, a lot of trust is necessary from the user of such a service. Yet, there is often not an alternative. This makes privacy abuse a real concern, take, for example, the controversy around Facebook’s real-name policy [13].

Solutions to provide anonymization already exist. Users can try to stay anonymous online by using VPN’s or more advanced solutions such as TOR [14]. However, this does not solve the problem around centralized identity management and the requirements that a service can pose upon a user. We need a decentralized solution that returns the control of the identity management to the identity owner. The notion of a Self-Sovereign Identity (SSI) is introduced to make this possible. It defines a solution where you are in control of your own identity. In ”The Path to Self-Sovereign Identity”, Christopher Allen motivates this concept, including ten principles that are still used today as a foundation for SSI technology [4].

The movement to a decentralized solution is not new. One of the most popular examples is the decentralization movement of money via Bitcoin [8]. This heavily influenced the SSI development. The underlying blockchain technology allows for decentralization by creating a peer-to-peer consensus protocol that no longer needs a centralized intermediary. Already there are a lot of initiatives for a blockchain-based SSI solution [15].

3.2 Blockchain Technology

Blockchain technology is characterized by a distributed ledger maintained in a decentralized way and secured by cryptography. By itself, the technology is not new. The first known blockchain started in 1995 and is still being published in the New York Times [16]. The technology took off after the Bitcoin white paper. It has since been seen as the catalyst of decentralization.

Soon after the decentralization of money via cryptocurrencies, other application domains were considered as well [17]. One of these domains is digital identity management, which fits naturally with the notion of SSI. However, SSI has more prerequisites than just decentralization. Privacy protection is the main concern. Data should only be disclosed to a party when consent is given. Moreover, the right to be forgotten that the European Union enforces should be complied with. This has strong implications on the underlying technology, and this is where problems start to arise.

Traditional blockchain solutions such as Bitcoin can be classified as permissionless blockchains. This means that there is no permission policy in place. All the users of the network can participate in any role they desire. It is based on zero trust, where the underlying technology maintains consensus and security. Anyone can view the data, and once data

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

[2] https://dictionary.cambridge.org/dictionary/english/privacy

has been processed into the blockchain, it is there to stay forever unless 51% of the users decide differently.

The open-access and immutable data structure contradict the necessities for SSI. Thus a trade-off between full decentralization and privacy is present. To counter these limitations, Decentralized Identifiers (DIDs) are introduced [18]. DIDs are globally unique identifiers designed to function in a decentralized environment. The goals are Decentralization, Control, Privacy, Security, Proof-based, Discoverability, Interoperability, Portability, Simplicity, and Extensibility. Consequently, there is an important overlap between the goals of DIDs and the principles that define SSI. Regarding privacy it promises to enable entities to control the privacy over their data and related attributes.

Aside from permissionless blockchain there is also a permissioned variant. It provides extra security by adding an access control layer to the blockchain. Users of the blockchain take on specific functions, determined by the authoritative party that regulates the blockchain.

2. How can blockchain contribute to SSI
3. Why is blockchain chosen by major implementations
4. What types of blockchain technology are there

3.3 Privacy Trade-Offs: Blockchain Technology

+- 1 page

1. What are the pro's and cons of each type in terms of privacy (Table ?)

2. Trade-offs -¿ when do you choose what regarding privacy, what purpose

3. flowchart, centralized, permissioned, permissionless to visualize.

3.4 Overview Blockchain-Based SSI

+- 1 page

1. What are the most prominent implementations
2. What technologies do they use?
3. What is there motivation in terms of privacy, if present?
4. Privacy evaluation per implementation

3.5 Privacy Trade-Offs: Blockchain-Based SSI

+- 1.5 page

0. Flowchart
1. Explanation of flowchart
2. Provide implementations in this flowchart
3. What are possible privacy-aware solutions that one can choose based on trade-offs from the evalution of technology and evalution of implementations.

3.6 Adoption Issues

+- 0.5 page

3. Practical limitations problems relating privacy
4. Localized / global solutions

4 Responsible Research

No results yet. +- 0.5 page

5 Discussion

No discussion yet. +- 0.5 page

6 Conclusions and Future Work

No conclusion yet. +- 0.5 page

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.

[12] Garfinkel, S. (2000). Database Nation: The Death of Privacy in the 21st Century.

[13] Gunthe, S. (2015). Facebook's "Real Name" Policy: A Violation of the Corporate Responsibility to Respect Human Rights. Columbia University.

[14] Dingledine, R., Mathewson, N., Syverson, P. (2004). Tor: The Second-Generation Onion Router.

[15] Liu, Y., He, D., Obaidat, M., Kumar, N., Khan, K., Choo, K.R. (2020). Blockchain-based identity management systems: A review. Journal of Network and Computer Applications. 166. 102731. 10.1016/j.jnca.2020.102731.

[16] Oberhaus, D. (2018). The World's Oldest Blockchain Has Been Hiding in the New York Times Since 1995. Vice. https://www.vice.com/en/article/j5nzx4/what-was-the-first-blockchain

[17] Jaoude, J. A., Saade, R. G. (2019). Blockchain Applications – Usage in Different Domains. In IEEE Access, vol. 7, pages 45360-45381

[18] Reed, D., Sporny, M., Longley, D., Allen, C., Grant, R., Sabadello, M. (2021). W3C. https://www.w3.org/TR/did-core/