frontiers in Blockchain

EDITORIAL
published: 06 August 2021
doi: 10.3389/fbloc.2021.738862

Editorial: Identity and Privacy Governance

Andrej Zwitter and Oskar J. Gstrein *

University of Groningen, Campus Fryslân, Leeuwarden, Netherlands

Keywords: digital identity, governance, data protection and privacy, human dignity, blockchain for good

Editorial on the Research Topic

Identity and Privacy Governance

The design and management of digital identity is a complex challenge. On the one hand, it requires a clear understanding of the parameters that are involved in identity management. On the other hand, it requires the cooperation of many stakeholders. In particular, this involves those public authorities and private organisations that need to be aligned to define technical standards, develop identification infrastructures and maintain them. A shared understanding of fundamental concepts that define identity in the digital age is then a prerequisite. Such a complimentary reflection and evaluation of what the emergence of distributed-ledger technologies means from the perspectives of human rights, human dignity, as well as individual and collective autonomy are essential to ensure their use for good purposes. While technical capabilities are important, they are increasingly insufficient without guiding theoretical frameworks. Sound governance mechanisms which respect, protect and promote human rights such as privacy are equally essential. The COVID-19 pandemic has only further increased the desire to use data to understand and manage our societies (Zwitter and Gstrein, 2020), which also increases the degree to which we are defined through data and our access to digital services.

Certainly, we currently witness profound changes in the capabilities to define and manage identity. Established architectures to validate, certify, and manage credentials are usually based on centralized or federated top-down approaches. They rely on territorial sovereignty, trusted authorities and third-party operators which gain considerable power by being able to manage the systems. In recent years, distributed-ledger technologies such as Blockchain have been described as "trust mechanisms", which can operate independently of such trust-mediators and territorial restrictions. One might prefer to rather trust a technical system, as well as the parties that host the software and ensure proper functioning, than traditional institutions such as banks and states. This emerging opportunity to change the practice of identity management raises the questions of 1) how blockchain applications influence trust, and 2) how trust based requirements affect the design of applications based on distributed-ledger technology?

Some identity management architectures presented in this research topic go even further and design full-fledged identity management systems. Their users are not only independent from the gatekeepers mentioned above. They also do not need to maintain a single aggregated identity. This enhances privacy and autonomy, so the authors argue, since aggregated identities can potentially be constrained or reconstructed against the interests of individuals. Such a pattern change could also potentially mitigate information security issues. These security issues are becoming more and more pressing as conventional digital identity management based on passwords and e-mail addresses face enhanced cybersecurity threats, typically associated with identity theft. Nevertheless, private forms of digital identity governance can also create worrying consequences from a security perspective, as the case of "Silk Road"—a historically influential platform for trading on the "dark web"—demonstrates.

OPEN ACCESS

Edited and reviewed by:
Richard Adams,
Cranfield University, United Kingdom

****Correspondence:***
Oskar J. Gstrein
o.j.gstrein@rug.nl

Specialty section:
This article was submitted to Blockchain for Good, a section of the journal Frontiers in Blockchain

Received: *09 July 2021*
Accepted: *27 July 2021*
Published: *06 August 2021*

Citation:
Zwitter A and Gstrein OJ (2021) Editorial: Identity and Privacy Governance. Front. Blockchain 4:738862. doi: 10.3389/fbloc.2021.738862

A more hopeful perspective is offered by digital identity management systems that aim at leveraging the potential of "self-sovereign identities" to become a driver for economic inclusion in some regions of the world. These pilots could help to demonstrate the potential of "Blockchain for good", but only if concerns associated with the use of biometric data and autonomy are mitigated. Still, new business models might emerge, such as identity insurance schemes, along with the emergence of value-stable cryptocurrencies ("stablecoins") functioning as local currencies. It remains to be seen how public institutions react to the emergence of these new opportunities. The impact of innovative approaches to digital identity management is not missed by intergovernmental organisations such as the Financial Action Task Force (FATF), which is at the centre of global anti-money laundering and counter-the-financing of terrorism. While FATF is not directly involved in the actual coding of protocols it influences the location and type of centralized modes of control over digital identity governance. In highlighting both the influence of FATF on blockchain governance and blockchain governance on the FATF, it is possible to draw together research areas which have been considered separately. A combination of perspectives might be helpful to understand the future of global digital identity governance more holistically.

With the same objective of developing holistic approaches, some articles of this research topic outline the underlying fundamentals by exploring philosophical conceptualisations of digital identity management. While a naturalist world view establishes identity as a concept that hinges on the concept of uniqueness, it also evokes questions on the dependence and interaction of an individual with its environment and society. Proponents of a constructivist identity emphasize relationality while questions of identity as a complete individual entity remain. At the same time, when considering the legal domain, it can be observed that particularly in the human rights space, identity is determined by several individual rights that states are obliged to grant to individuals. Furthermore, aspects around the ownership of material and immaterial goods (e.g., intellectual property) ultimately highlight the issue of "data ownership" which could be essential to keep rights enforceable on a universal level in the digital domain. These arguments and insights might inspire the design of innovative governance frameworks. Nevertheless, it is also necessary to consider how traditional identity management systems such as citizenship engage and intersect with the emerging technological capabilities. It cannot be overlooked that the development and implementation of digital identity management systems using distributed-ledger technology raise multiple ethical and moral issues.

As editors of this research topic, we can only be grateful for the insights and ideas the authors have shared with us. We hope that the readers of the contributions to this edited volume share our excitement when exploring their content. To us it seems that the development of digital identity systems will continue to remain an important topic in the years to come. Currently, the development and implementation of "vaccine passports" and digital COVID-19 vaccination certificates might eventually morph into general purpose infrastructures that also receive broader tasks in identity management. These and similar developments result in a chorus of ethical, legal and social issues that need to be addressed (Gstrein et al., 2021), and for which the research presented in this research topic provides a rich basis.

AUTHOR CONTRIBUTIONS

OJ provided the first draft which was reviewed and edited by AZ.

REFERENCES

Gstrein, O. J., Kochenov, D. V., and Zwitter, A. (2021). A Terrible Great Idea? COVID-19 'Vaccination Passports' in the Spotlight. Centre on Migration,. *Pol. Soc. Working Pap.* 153, 28.

Zwitter, A., and Gstrein, O. J. (2020). Big Data, Privacy and COVID-19 - Learning from Humanitarian Expertise in Data protection. *Int. J. Humanitarian Action.* 5 (4), 00072–00076. doi:10.1186/s41018-020-00072-6

Conflict of Interest: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.