ROUND TABLE REPORT

NOVEMBER 2018

BLOCKCHAIN, DIGITAL IDENTITY AND PERSONAL DATA: THE POTENTIAL OF SELF-SOVEREIGN IDENTITY FOR EUROPE

REPORT
ROUND TABLE

Blockchain, Digital Identity and Personal Data: The Potential of Self-Sovereign Identity for Europe

Brussels, 19 November 2018

European Parliament
Rue Wiertz 60, 1047 Ixelles

DISCLAIMER

This report is prepared by Dr. Alea Fairchild with help from the rapporteur, Sivan Pätsch, for OpenForum Europe ("OFE"). The summaries of the speakers' presentations and panel discussions in this report are based on the rapporteur's notes, and are not in any way binding or necessarily complete. All effort has been given to reflect and convey objectively the essence of the speakers' presentations and the discussion.
The views expressed in the report do not necessarily reflect those of the rapporteur or OFE. Neither the rapporteur nor OFE should be held accountable for any claimed deviation from the original speeches and panel discussions.

CREDITS

SPEAKERS

MEP Sorin Moisa
MEP EPP, International Trade Committee, Delegation for Relations with the United States of America

Arnaud Le Hors
Hyperledger Project, IBM Senior Technical Staff Member, Member of the European Blockchain Observatory and Forum

Peteris Zilgalvis
Head of Unit, European Commission, Digital Innovation & Blockchain, Co-Chair, FinTech Task Force

MODERATOR

JDr. Alea Fairchild
Director, The Constantia Institute and Professor, KU Leuven

FOREWORD

We are increasingly moving the focus away from the fin-tech applications of Blockchain technology to an application that is receiving increasing attention, one that holds significant potential in technologically and politically relevant fields: **self-sovereign identity ("SSI")**.

Self-sovereign identity is the next step in the evolution of digital identity management. It provides the user with individual control, security and full portability, by making the individual their own identity provider and storing the record of identity transactions in a distributed ledger. We could thus move beyond the insecure silos of directories, passwords and usernames to improve how the internet works. **By extension, the technology has the potential to revolutionise how individuals interact with public administration and business.**

ASTOR NUMMELIN CARLBERG

Astor Nummelin Carlberg, Senior Policy Adviser, OpenForum Europe opened the event by welcoming everyone to the event, and explaining the purpose of the OFE and its participation in the open standards community.

The four speakers invited to frame this discussion of self-sovereign identity (SSI) were:

- **MEP Sorin Moisa,** MEP EPP, International Trade Committee, Delegation for Relations with the United States of America
- **Arnaud Le Hors,** Hyperledger Project, IBM Senior Technical Staff Member, Member of the European Blockchain Observatory and Forum
- **Peteris Zilgalvis,** Head of Unit, European Commission, Digital Innovation & Blockchain, Co-Chair, FinTech Task Force

Moderator: **Dr. Alea Fairchild,** Director, The Constantia Institute and Professor, KU Leuven

Questions to be addressed included:

- Where are we today in terms of the technology and adoption of SSI?
- What actual examples of SSI application do we have currently?
- What are the sources of reluctance or opposition among business, public authorities and users?
- What is the current status of the standardisation process? What are the points of friction?
- Concerns have been raised about the consequences of the GDPR and personal data on the blockchain--what is the actual relationship?
- How does the development and implementation of SSI relate to the Commission's efforts with the adoption of eID and eIDAS Regulation and framework?

DR. ALEA FAIRCHILD

Dr. Alea Fairchild then introduced the concept of SSI and the panel members, making it clear that the Chatham House Rule would apply – i.e., that whilst the main named speakers could be quoted, no other participant in the debates should be quoted with reference to their contributions.

In her opening, Dr. Fairchild discussed how models for online identity have advanced through four broad stages since the advent of the Internet: centralised identity (administrative control by a single authority), federated identity (the power of centralized authority now being divided among more than one powerful entity), user-centric identity and self-sovereign identity.

The term user-centric identity suggests that users are placed in the middle of the identity process. Initial discussions of the topic focused on creating a better user experience, which underlined the need to put users front and centre in the quest for online identity. However, the definition of a user-centric identity soon expanded to include the desire for a user to have more control over his identity and for trust to be decentralised. Self-sovereign identity is the next step beyond user-centric identity, which means it begins at the same place – the user must be central to the administration of identity. That requires not just the interoperability of a user's identity across multiple locations, with the user's consent, but also true user control of that digital identity, creating user autonomy.

To accomplish this, a self-sovereign identity must be transportable; it can't be locked down to one site or locale. A self-sovereign identity must also allow ordinary users to make claims, which could include personally identifying information or facts about personal capability or group membership. It could even contain information about the user that was asserted by other persons or groups.

Several self-sovereign identity systems exist now in various stages of development, including Sovrin, uPort and Veres One. Whilst each of these supports decentralized, self-sovereign identity, they differ in how claims are issued and presented.

In this regard, today we are discussing the use of blockchain. Self-sovereign identity systems can use blockchains – distributed ledgers – so that decentralised identifiers can be looked up without involving a central directory. Blockchains don't solve the identity problem by themselves, but they do provide a missing link that allows things we've known about cryptography for decades suddenly to be used. That allows people to prove things about themselves using decentralised, verifiable credentials just as they do offline.

MEP SORIN MOISA

Sorin Moisa then opened his presentation with the statement that he hoped to learn answers to his questions on SSI and blockchain through this event. He believed that identity under the control of the identity owner is a beautiful idea, and hoped that it would been seen as more democratic. He felt that blockchain might make this possible. He stated that GDPR reacts to business models that monetise other people's data, sometimes without consent of the user, whereas GDPR is supposed to give citizens control over their data; it has, in this, similar ideas to SSI. One opportunity that SSI presents is the possibility for people to monetise their own data.

He also discussed that projects such as the Blockchain observatory (which the EC started in reaction to an EP request) show that there is a tension between SSI and GDPR. Immutability is one of the main issues which blockchain poses for GDPR (including the "right to be forgotten" - compliance with the obligation to delete unnecessary data would appear difficult in this respect). Moisa asked the question: "Can there be peace between these two strands of tension?" Because if yes, SSI would a great new beginning, which would disrupt bygone times.

ARNAUD LE HORS

Arnaud Le Hors introduced his work with the Hyperledger Project and the European Blockchain Observatory. He started with the background on how hyperledger can be used, stressing that it is a consortium, not a software product. As an example, he mentioned "Hyperledger Indy", a project for a distributed ledger, which is still in development.

He then discussed the evolution of what kinds of information elements are covered in identity services -- evolving from just a password to the whole spectrum of identity. Over time, one accrues different pieces of identity (ID; driver's licences, etc.) and individual people are not in control of these or their level of accuracy. With the newfound tension between GDPR and blockchain, the project found a solution in an identity issuer, e.g. a university could issue a diploma which would be cryptographically signed and put into your digital wallet on a blockchain. He noted that the information that is on the blockchain is linked not to the individual, but the issuer, as so would not be covered in the same way by GDPR. Even if the university were to disappear, the possibility to access the credential would be kept, allowing it still to be used by the individual.

However, the reality of Blockchain is that economic requirements cannot be denied, the system needs to sustain itself, therefore there must be a working business model. For example, banks are subject to costly regulatory requirements, such as "know your customer" (KYC), which Blockchain could solve at a lower cost. He also believes that selective disclosure could be possible, with an associated privacy advantage. For example, on a webshop, a Blockchain verification could verify that an individual customer was aged over 18 without their birthdate being shared. To be successful, however, governments will need to play a big role in this concept.

PETERIS ZILGALVIS

Peteris Zilgalvis began his presentation with a comment on decentralisation: A move from big platforms with centralised data to a decentralised system could possibly be done on blockchain. The concept of nodes of information can be helpful in dissemination. The use of Blockchain could be helpful in decentralised digital platforms, or at least to take control of data at platforms in general. He went on to discuss how the European Commission and Europe are active in developments in Blockchain, e.g.: Fintech taskforce, European blockchain partnership, etc. In order better to support Blockchain actions, the Connecting Europe facility could be a source for funding.

He went on to discuss eIDAS, i.e., Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market, which was adopted by the co-legislators on 23 July 2014. With eIDAS, the EU has managed to lay down the right foundations and a predictable legal framework for people, companies (in particular SMEs) and public administrations to have safe access to services and to implement transactions online and across borders in just "one click". Since the purpose of eIDAS is to create a European internal market for trust in electronic transactions, eIDAS could be implemented with Blockchain, as eIDAS is obligatory for the public sector, with interoperability.

He saw SSI as complementary to other government-issued ID methods. He also was positive about GDPR and SSI co-existing. The use of Blockchain can be beneficial, but needs to be evaluated sector by sector in terms of interoperability and implementation. Individual control of data also raises issues about the necessary control which government has over data. As a supranational body, the European Commission does not want to pick a winner product/technology, the consumer should instead rightfully choose.

As a final note, he pointed out that researchers should look at the "once-only principle" call, which is currently open under Horizon 2020.

PANEL DISCUSSION

Dr. Fairchild then opened the discussion to the whole panel. She started the discussion with a follow-up comment on GDPR and pointed out that right now, privacy management is extremely complicated if achieved through use of conventional technology. She asked whether implementations such as Blockchain could solve privacy issues by giving less information to businesses (e.g., profiling based on the address).

The response to this question was to focus on how we can make this technology easy to use. It was agreed that it was very complicated to have separate systems for each identity service: big platforms already provide single-sign-on, with privacy drawbacks. Any new system would need to be easy to use, in order fo it to be able to replace the big platforms. At present, different blockchains represent different wallets without interoperability. It is still very early in the development, but there is a huge business opportunity if we can find a way or a mechanism for collaboration.

It was stated that the Commission sees the potential for cost savings of 30% by transitioning to Blockchain for education technologies (diplomas). Also (although this is still although quite a bit off in the future) one can now imagine the possibility of a "digital euro".

The opposition of some people to sharing their data at present, especially in certain geographies and certain demographic groups, was highlighted. It was agreed that in central and eastern Europe extremely invasive State practices have been routinely observed, which has made people distrustful of sharing their data. Someone provided an example given to her by a millennial to show that sometimes people are less concerned when they understand the value of sharing their data (e.g., Google Maps takes your location data but offers personalised services in return).

There are differences in cultural backgrounds on how people approach identity. In the future, Blockchain might just be accepted as part of the lower layer of the technology stack, without people even being aware of the technology. One contributor suggested that it would be good for the technology to be less "hyped".

We then focused the discussion on trust, and what could be the basis for trust in this system such as this. We also discussed trust in terms of eIDAS. As GDPR has educated people about how data can be used and misused, it was asked how Blockchain can relate to this? The panel then discussed what can we do in terms of standardising Blockchain, but agreed as a panel that it is not yet the right time (too early) for any such standardisation. At the same time, the panel also agreed that standards are required to "make this work", i.e., for interoperability. We need standards, for data formats, and for protocols to exchange the data. Industry is making great progress on this and has understood that standards are necessary for this to work.

Q&A WITH AUDIENCE

Dr Fairchild then opened the discussion to the other attendees.

One gentleman wondered whether, although Blockchain has made progress, there might be an issue with Blockchain possibly destroying privacy. When people can pay with their personal data, it becomes a commodity. There was a reply that data has value and is a fundamental right, currently we essentially pay with data. Perhaps personal data will become a trade good and then be removed as a fundamental right. Someone felt that people were not conscious about giving away their data, even though from a legal perspective, they were informed. He saw that even if we could sell data in an anonymised way, it would then still have value. It was foreseen that we would never withdraw the fundamental right to privacy. Perhaps both awareness and incentives could be a solution. One person remarked that a good business model is necessary for success.

Another attendee remarked that this may create the need for a privacy tax (only people who can afford it will have privacy, others will pay with their data). To be successful, Blockchain has to go into the background. Standards build trust in the back-end, but FOSS phones would be required to be able to trust (e.g.) an app's usage of the data. Someone agreed that Open Source very important, and this should also be promoted through the standards unit.

A question from another attendee: What happens if you make a mistake? You cannot correct a mistake with Blockchain - what happens? There was a response that a wrongly issued credential is under users' control and can just be discarded. When talking about identity, we don't mean a single identifier, so it would not be possible to track this. It was then asked how, considering the immutability of data, one would control a piece of information on the ledger (i.e., disregard it)? Someone replied that the information you have is not related to you, it is related to the issuer. Governments need to be able to revoke (e.g). a driving licence; in this case, the original data is not being deleted; rather, information is added, to record that the original licence-related information has been revoked.

CONCLUDING STATEMENTS

The panel concluded its contribution, with each panellist providing a concluding statement, as follows:

PETERIS ZILGALVIS
The European Commission is committed to SSI and Blockchain, regulated technology creates efficiency increases and a flourishing private sector.

SORIN MOISA
He is now more convinced that idea of SSI (own control, slowly, maybe not monetised) is aligned with the European way of doing things, more so than any other possible solution.

ARNAUD LE HORS
Many applications of Blockchain exist, such as supply chain. But SSI is the most exciting one. SSI on Blockchain is a system where no one loses.

Alea thanked the panellists and concluded the event.

ABOUT

OpenForum Europe (OFE) is a not-for-profit, independent European based think tank which focuses on openness within the IT sector. We draw our support not only from some of the most influential global industry players, but most importantly from across European SMEs and consumer organisations and the open community. OFE also hosts a global network of ***OpenForum Academy Fellows***, each contributing significant innovative thought leadership on core topics. Views expressed by OFE do not necessarily reflect those held by all its supporters.

ROUND TABLE REPORT

NOVEMBER 2018

BLOCKCHAIN, DIGITAL IDENTITY AND PERSONAL DATA:
THE POTENTIAL OF SELF-SOVEREIGN IDENTITY FOR EUROPE