GLINZ & COMPANY GMBH

Pilatusstrasse 7
8032 Zürich
CHE-193.569.920 MWST

Zürich, 22. February 2018

Recapturing personal data and identity – How a Swiss project may lead the way

This article shows that the web as we know it needs to and inevitably will transform itself embracing new theoretical and technological concepts. Among those are powerful innovations in the fields of identity and personal data management. Leveraging the Blockchain technology as the link that was missing so far, VALID, a new platform concept from Switzerland, is about to change the way we handle data and eventually to give control about identity and data back to the user.

We are all connected. Ever since the American social psychologist Stanley Milgram proved with his small-world experiments in the late Sixties that every human being is inevitably linked to each other by surprisingly short chains of connections, we know about the importance of social networks. We also know that networks not only play a significant role in social interaction, but rather all over our physical and mental world. They allow a virus or gossips to spread. They can be used to display protein-protein interaction networks as mathematical representations of the physical contacts between proteins in the cell. It is in the nature of things to position itself or allocate resources in networks. The typical network characteristics and effects can also be made accountable for the emergence and spread of the internet. Being connected is one of the most important qualities in today's world. In our understanding of digital business, network effects are key to success. But there is a second side to this coin. Network effects can also encourage unfortunate developments. Alike the unstoppable spreading a bad virus or cancer, networks such as the internet can also evolve along wrong paths.

Today, the leading revenue models of digital businesses are based on advertising. It is evident that the economic engine of the world wide web is privatized and monopolized to a great extent. Monopolistic companies have emerged as giants in their space. Facebook, Google, Tencent, Airbnb and numerous other leaders of the pack have created own, proprietary platforms in the form of digital ecosystems in their markets. They collect and analyze the wealth of data their users produce when accessing their websites, communicating on their platforms and in many more occasions. All these data points together create the user's ***digital identity***.

Most of the success stories in digital business have one thing in common; they are all enabled by data. The mechanism behind this phenomenon can be explained in only a few sentences. Constantly improving algorithms lead to digital products and services. When done right, these data products add value to the customer. This perceived value added will convince customers to provide even more data. The use of data products itself leads in this perfectly closed loop to an ever-increasing wealth of transactional and behavioral data. All that data can be monetarized which causes profits to surge. Unfortunately, there is a worrying imbalance between giving and taking. Customers more and more understand this issue and demand for more reciprocity. They recognize the value of their ***personal data***. Empowered with new technological means and knowledge, they start to better protect this data. An even bigger effect on existing data-driven business models is to be expected by interventions from regulators. The latter are also increasingly concerned at what they see as a growing imbalance between data-dependent companies and individuals (Nguyen et al., 2013). This is why the European Commission will finally introduce its "regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" in May 2018 (European Commission, 2012).

All this leads to the hypothesis that the area of living in a land of milk and honey is coming to an end for the large players in the digital economy. The newly emerging web is characterized by fundamentally different mechanisms, it's about multiple nodes sharing value across an open network. Companies like Facebook are already anticipating this change. They are restlessly on the search for other revenue models apart from data monetization through advertising. But this is another story. Before painting a picture of the future and outlining solutions, we need to ask ourselves; How did it come to this?

Absence of an identity layer

The answer to this question can be found in a simple fact: "The Internet was created without an identity layer". This increasingly popular quote from Kim Cameron, Chief Architect of Identity for Microsoft, leads to the root cause that can make network effects a counterproductive force. Although the triumphant progress of the internet brought the information age to a new level, it led digital business models towards the described impasse. Whereas the Hypertext Transfer Protocol (HTTP) as the underlying protocol used by the World Wide Web lead to unpanelled, successful growth of the internet, the web community missed to establish an adequate system to assign and verify identity. The way the internet works is fundamentally different than identity on the web works. The latter is a network of connected devise. Each of these devices connected to a network are centrally assigned a numerical label, the Internet Protocol address. Instead of identifying human beings as endpoints on the network, the system connects physical devices. That's why it is nearly impossible today to uniquely identify people and authenticate their messages. In addition, we currently define and authenticate accounts that are not necessarily tied to real people or organizations. We do this often separately for each service. For the sake of convenience, we even allow the giants like Facebook or Google to authenticate our identities on third party platforms. This all leads to the unfavorable side effect that online identities can dramatically differ from real world identities and that information spread in digital communication might not be true. To better describe this phenomenon, politics has established all new expressions such as "alternative facts" or "fake news".

A certain degree of ***anonymity*** in digital communication is not harmful by nature. Anonymity may lower barriers to engage in discussions and therefore to participate in a network. It can support the rapid growth of networks and with that it's positive externalities. This effect describes the fact that an additional node in a network has a positive effect on the value of this network to others. Anonymity is also what drives the success of many use cases on the blockchain. The Bitcoin is one of them. Due to inherent anonymity, the most prominent among the broad range of new cryptocurrencies is also used for shady transactions. Without anonymity, the rapid adoption of the Bitcoin would not have happened and its value would be much lower. Another aspect that sheds a bad light on anonymity is the popular assumption that online anonymity is one of the principle factors that promotes aggression. This must not necessarily be the case. Anonymity can produce the "stranger on a train" phenomenon, wherein people share intimate self-disclosures with strangers as they do not expect a reunion and hence do not fear any risks and constraints (Bargh et al., 2002). Recent studies in social norm theory show that in the context of online firestorms, non-anonymous individuals are more aggressive compared to anonymous individuals (Rost et al., 2016). When introducing an identity layer for the web the major focus should therefore not lay on making anonymity a thing of the past. It should rather lay on enabling and supporting ***authenticity*** and eventually data veracity. In this context authentication can be defined as the act of confirming the truth of an attribute. If we were able to more easily and reliably authenticate data on the web, the degree to which data we use to make decisions is accurate, precise and trusted will be much higher.

What's the matter with Personal Data

Another side effect of the missing identity layer on the world wide web is the fact that personal data is easily accessible for service provider and that this data can be monetized without a clear consent and without remuneration of the owner. Dealing with personal data is complicated and gets more and more toxic for companies of all industries. Here is why:

- The amount of data is growing at an astonishing rate. Users leave traces with every activity and generate countless data points along the customer journey

- Although cost of data storage is shrinking, the cost to acquire, manage, analyse and protect huge volumes of user data is increasing
- Digital identities bear the risk of correlation. If a user is to use one identifier in multiple places, those places might collude to correlate that identifier and amass significant data about the individual without its consent.
- Central data stores are honeypots for hackers. With new data regulations coming into force this year, storing personal data can become illegal. Together with the high risk and impact of data breaches, capturing data becomes toxic.
- Generally, the responsibility and complexity of the management of personal data cannot be outsourced to the user. They prefer easy to remember passwords compared to excessively safe passwords. Usability of authentication systems remains key.
- Low data quality and veracity can lead to wrong decision and damaged trust

There is a common understanding of the strategic thrust mandatory to further develop digital business models: "A new approach to personal data is needed that is flexible and adaptive to encourage innovation, but also protects the rights of individuals. Notice and consent need to be reconsidered to be equipped for this changing world." (WEF, 2013). Extracting insight from consumer data requires respectful and farsighted handling of personal data. A first step on this approach is to establish a new paradigm to manage digital identities. Alike the handling of personal data, the control about identity needs to be brought back to the individual. Individual identity shall have administrative autonomy regardless of its location in digital space.

The path towards the web of trust

The missing identity layer of the internet is a well known issue. That's why there have been countless attempts to close this gap. The task has been left to applications and services. While these apps do their job quite well for a clearly defined area, they can't hardly be applied across silos. Furthermore, they all rely on a central authority. These are all facts that make current identity systems imperfect and also vulnerable to abuse.
The first step towards a better solution is to establish a solid, mental layer that takes up the challenges described. Such a layer requires a common understanding of the problem, a common language (ontology) and a clear commitment of participants to support this idea and to obey to certain rules of the game (codex).
Many interesting attempts in this direction have been made in the last years. Among them are ***trust networks*** such as the Secure Access For Everyone (Safe) network (https://safenetwork.org) or the respect network. The latter globally launched its platform in 2014 with a line-up of around 50 founding partners, including Neustar, Swisscom, and NEC. In a nutshell, these trust frameworks provide a set of guidelines, rules and tools together with an assessment and enforcement infrastructure that operationalizes them. In addition, trust networks

usually rely on decentralized concepts for data storage. The individual itself shall own its data using Personal Data Services or ***Personal Data Stores*** (PDS). These are services that let the individual store, manage and deploy their key personal data in a highly secure and structured way.

However, despite all efforts and well-intentioned ideas, it is a cumbersome endeavor to establish such a new type of contract that may legally bind the members of the trust community to the policies. It is therefore, not a big surprise, that many attempts have failed so far to get traction and eventually to establish a well anticipated industry standard.

Why the timing is right now

Great ideas often fail because they are ahead of their time. But the wind is about to change. Two forces can set the timing to stablish a reliable identity layer just right: The implementation of the General Data Protection Regulation (GDPR) in Europe and the increasing importance and anticipation of the blockchain technology.

With the upcoming introduction of new ***data regulation standards in Europe*** the discussion about the necessity of a resilient identity layer for the web and the demanded empowerment of individuals gains momentum.

The regulation demands that the control about personal data is given back to the individual. This implies that the identity should again belong to the individual. It must never be possible for a centralized authority to alter an identity or to take it away. Such a ***self-sovereign identity*** can only exist in a decentralized system.

A stringent requirement to establish self-sovereign identity is a web of trust with its decentralized trust model - a valid alternative to the centralized trust model of a public key infrastructure, which relies exclusively on a certificate authority.

The impressive global popularity of cryptocurrencies brings a much better understanding of the principles of decentralized systems. The ***Blockchain technology*** could be the missing link for a successful implementation of a decentralized trust network. Countless projects demonstrate that the Blockchain technology is tremendously powerful in overcoming the trust barrier. It's trust-less systems might be the answer. The Blockchain with its distributed ledger is the ideal backbone of a resilient web of trust. It reliably connects the described prerequisites such as policies trough smart contacts and with personal data stores in the form of decentralized applications (dApps). Now that the timing seems to be right, it's no surprise that a high number of projects enter the game. They have learned from the previous failures and often anticipate the culture of open source and open data. They know that they can only succeed, if their solution is open if they seamlessly integrate into the bigger picture that draws the self-sovereign identity.

The question arises if the Blockchain technology is the ideal vehicle to handle personal data? Given its decentralized mechanisms and with that its robustness against manipulation, it is an adequate solution for an identity layer. But there are also drawbacks of the technology that need to be considered:

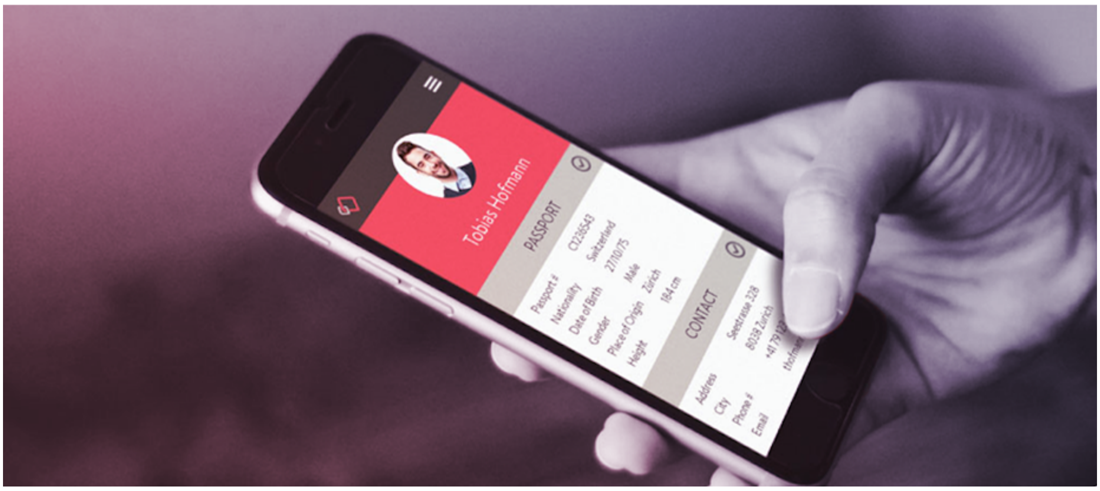
- The distributed ledger is forged by consensus. Therefore, it misses by design a strong governance. In order to improve the codebase or just fix an issue, the community around the Blockchain may decide to change the protocol. Such a hard fork would dramatically impair identity schemes.
- Personal data could be stored on the ledger. This would result quickly in a breach of the new data protection regulations.
- Transferring information across Blockchains can be difficult. Portability and interoperability may be impaired.
- The fact that a unique identifier would have to be defined and stored on the ledger would again trigger an immediate correlation risk
- Identity information on the Blockchain cannot easily be revoked. This is a critical requirement in order to manage claims and entitlements.

Following this argumentation, it stands to reason that the complexity of an identity layer can only be solved by drawing on multiple concepts and technologies. While a robust trust framework in terms of binding commitments to rules of the game remains important, the mechanisms of the blockchain can be leveraged to access personal data stores and handle value transfers in particular. There will not be a single, centrally owned solution or architecture, but rather a consortium of different, autonomous solution providers with their interoperable components.

How a Swiss project may lead the way

Companies like to leverage Switzerland as a brand that stands for quality and security. Conversely, authorities and local businesses are strongly motivated to life up to high standards. It is therefore not a surprise that, Switzerland plays a leading role in shaping new data protection regulations and developing new standards in digital identity. The Swiss government is keen to provide an electronical identity (E-ID) in the near future. How a final solution will look like remains open. It will however rely on private innovators as identity solutions provides. Over the last year, a few forward-looking projects have been implemented. Among them is an Ethereum based digital identity leveraging the Consensuses web-based wallet and identity management system called uPort. The solution has been implemented in Swiss City of Zug. It ties personal information to an Ethereum address and allows citizen to establish a self-sovereign identity, collect badges and credentials, login to decentralized apps, and digitally sign transactions. Another groundbreaking identity solution has been rolled-out for Canton of Schaffhausen by e-government as a service provider Procivis. The creators of this eID+

solution are aware of the fact, that such a project can only succeed if it is built based on the principle of an open architecture. The pilot project is only a first step towards an integrated e-Government solution. The system is inherently open to adjustments and to integrate seamlessly additional identity solutions such as the planned SwissID.



Tobias Hofmann

PASSPORT

Passport # C1236543
Nationality Switzerland
Date of Birth 27/10/75
Gender Male
Place of Origin Zürich
Height 184 cm

CONTACT

Address Seestrasse 328
City 8038 Zurich
Phone # +41 79 12
Email thofmann

The creators of the self-sovereign eID are about to go one step further. By end of February 2018 they are going to launch their blockchain based ***VALID ecosystem*** with an initial token offering. The team that is based in Zurich intends to expand the digital identity sphere beyond personal attributes by encompassing the individual user's entire personal data space. To achieve this, they will provide two key components.

1. The VALID ***wallet*** for personal data management. The wallet is the central user interface to access the VALID ecosystem. It features a personal data store that stores most sensitive data locally on the device. The encrypted data is therefore not stored on the ledger itself and the user is in full control of all his data at any time.
2. The VALID ***marketplace*** for data monetization. Users can decide to share their data by granting interested parties access to clearly defined data points. As a reward, users will be remunerated in VALID tokens (ERC20) based on the desirability of the shared data.

Obviously, the idea to establish a marketplace for personal data that is provided from personal data stores with the informed consent of the owner is not new. Many attempts in this direction have been made and all of the ambitious project have failed so far to get traction. VALID however, seems not only to have the right blueprint at hand. Also, the timing to roll-out the solution seems to be just right. With the new European privacy regulation coming into force in May 2018, users will pay much more attention to personal data management. Companies that used to tab into their user's data often without clear consent and any intention for remuneration are now forced to ensure transparency and data portability. The latter will allow users to conveniently collect personal data and store is in their vaults.

Another success factor will remain the openness of the solution architecture. VALID is aware of the fact, that it will coexist with numerous other solutions for personal data stores and marketplaces. The seamless integration with other platforms will be critical for the acceptance as well as for the usability of this product. An important step in this direction is already made. Procivis has established a partnership with the Lucerne University of Applied Sciences and Arts and the Crypto Valley Association with the intention to implement the Sovrin Blockchain ID protocol. The Sovrin Foundation incorporated the principles of the respect network and governs the world's first open public self-sovereign identity network.

Disclaimer:

The author is a member of VALID's ambassador program and owns VALID tokens. The writer's opinion is his own. This article is for educational purposes only and does not provide financial or investment advice. Please conduct your own thorough research before investing in any cryptocurrency.

Learn more about the importance and mechanism of trust in the digital space. Visit: www.iceberg.digital

About the author:

Daniel Glinz is an experienced management consultant and digital strategist. With broad academic background from leading management and design universities and a strong link to investors and start-ups, Daniel combines groundbreaking conceptual work with the ability to shape and eventually transform businesses. Find out more about digital strategy consulting on www.glinz.co.

Literature:

Nguyen, C. M.-H., Haynes, P., Maguire, S., Friedberg, J., 2013. A User-Centred Approach to the Data Dilemma: Context, Architecture, and Policy, in: Digital Enlightenment Yearbook 2013, Hildebandt M. et al. (Eds.), Amsterdam, IOS Press BV, 227-242

WEF, 2013. Unlocking the Value of Personal Data: From Collection to Usage, World Economic Forum, Industry Agenda

European Commission, 2012. General Data Protection Regulation (GDPR), Brussels

Bargh J.A., McKenna K.Y.A., Fitzsimons G.M., 2002. Can you see the real me? Activation and expression of the "true self" on the internet. Journal of Social Issues. 58(1), 33–48

Rost, K., Stahel, L., Frey, B. S., 2016. Digital Social Norm Enforcement: Online Firestorms in Social Media. PLOS ONE 11(6)