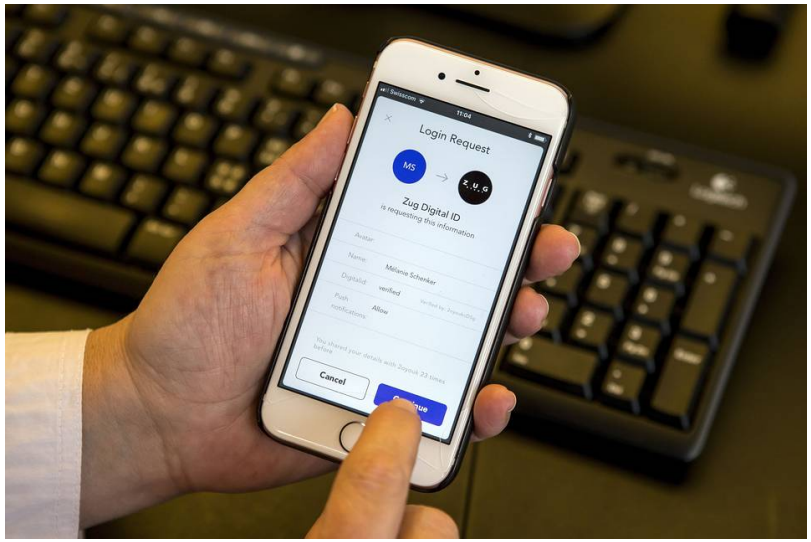
CIO JOURNAL. | COMMENTARY

Digital Identity Is Broken. Here's a Way to Fix It

The bedrock of trust is a human community with frequent positive interactions

By
Alex "Sandy" Pentland, Thomas Hardjono, MIT Connection Science

Apr 3, 2018 3:13 pm ET



A mobile phone is seen during the demonstration of a blockchain-based digital ID in Zug, Switzerland, Nov. 15, 2017.
PHOTO: EUROPEAN PRESSPHOTO AGENCY

Most people today suffer from a strange sort of psychosis: we are uncertain of our identity. For although we are (mostly) certain of who we are in our own minds, the identity we use to interact with the government, obtain services, and pay for goods is unreliable. In poor parts of the world people simply don't have trusted identity credentials that allow them to prove who they are, while in rich parts of the world we worry about identity theft, and crimes using fake or stolen identity credentials are rampant.

The core problem is that the identity credentials we use often are defined and certified by someone else, for instance, by the government or a company such as a bank.

This means that the certifying authority can unfairly coerce individuals needing to be credentialed, and it is difficult to escape "big brother" surveillance and protect individual privacy. The centralized nature of identity certification also means that fraud only requires altering a single database and that corruption stemming from inside the certifying authority is difficult to prevent.

How can we fix the current mess, where the basic building block of commerce and government...the identity of people and businesses....is so badly broken? The answer is we need a new generation identity mechanism where credentials are issued by communities of people and businesses that know each other. Here, your entire community vouches for you, not a single bureaucracy or a single commercial player.

Centuries ago they had 'letters of introduction' that would be signed by the local lord or the local priest, representing your standing in the community. Today military security credentials are backed by an FBI reference check of former employers, coworkers, friends, neighbors and landlord. The key point is that the community is the source of trust for assertions regarding its' individual members. It should be the community that certifies digital identity credentials, just as with military credentials.

How might this happen practically? A possible mechanism is through credit unions, which are already legally empowered to manage identity credentials and already boast

100 million people as members.

But what about self-sovereignty?

Some have taken today's problems with digital identity to move in the opposite direction. As a consequence, the notion of self-sovereignty has gained significant popularity among the digiterati. In a self-sovereign identity framework the individual uses tools such as cryptographic signing to create their own identity in order to allow others to authenticate their identity and properties. These identity credentials are said to be self-sovereign. The current hype cycle is backing blockchain ledgers to provide more trustworthy and more broadly available identity credentials, and many of the cryptocurrencies, such as bitcoin and Ethereum, function in this manner.

This idea is exciting but misleading. To have a system that is completely dependent only on assertions by the individual themselves – namely true self-sovereignty – is an invitation for mistakes, fraud, and systematic corruption. Most recently financial authorities around the world have been reacting to this problem in the world of cryptocurrencies and outlawing or severely restricting these digital currencies.

The mistake that both governments and tech pioneers are making is failing to realize that trustworthy identity depends on jointly-issued credentials, where credentials and certification must be based on trustworthy assertions by the community of people and institutions in which we live. Identity credentials are really mechanisms for collecting and documenting trusted relationships, not self-certifying systems. Trustworthy self-sovereign frameworks should really be called joint sovereignty or community sovereignty frameworks.

Simply collecting assertions from people in order to certify your identity is insufficient. Many fraud schemes depend on creating a network of false identities, reducing any identity mechanism based on joint sovereignty to a method of hiding fraud by spreading out the false information. For instance, many fraudulent financial schemes

and even terrorist organizations create fake Facebook identities and link them to many other fake identities in order to make the fake identity look like real people.

How to fix digital identity

Adam Smith wrote that "it is human nature to exchange not only goods but ideas, assistance, and favors...and it is these exchanges that create solutions for the good of the community." Similarly, Karl Marx wrote that "society is the sum total of social relations connecting its members." This suggests that it is networks of human-to-human interaction that define and are the basic authentication mechanism for the trust relationships that makes human society possible, and that trustworthy identities all ultimately depend on physical-world relationships as the basis of trust.

This is exactly what we find in our research on community trust where we analyze data from mobile phone, credit card, and similar digital breadcrumbs left behind by human-to-human interactions. Both subjective ratings of trust and objective demonstrations of trust are accurately predicted by the presence of frequent positive human-to-human interaction. The bedrock of trust is a human community with frequent positive interactions.

We should therefore be talking about identity credentials being issued by members of our community and certified by a set of people and institutions with whom we regularly interact. This does not have to be a physically co-located community, but it does have to be a connected, interacting community with a history of trust between people, and where people care about their reputation within the community. Mechanisms for identity within temporary virtual communities, or communities where violations of trust are frequent and have no bad consequences, are not likely to be trustworthy regardless of the sophistication of the cryptography or the robustness of the computing architecture.

We can characterize the trustworthiness of digital identities in terms of the following two properties of their community.

Digital representation of the community interaction network: Human beings operate within communities, both in physically co-located communities and in virtual (online) communities. Human communities include not only individuals, but also conglomerations such as companies, governments, churches, and clubs. The aggregate of data about community members' interactions provides a digital representation of community life as a network of relationships. As the internet expands and more aspects of a person's life are "digitized," the completeness of this representation will increase, and a data-driven society can increasingly rely on these "islands of community data" which will be distributed across the Internet.

Dense Interconnections and Trust: In human societies the reputation of a person within a community is a function of not only the network of community interactions, but it is also influenced by the degree and frequency of interactions. Networks that are "dense" – where everyone is connected – are the traditional source of *local trust* regarding an individual. For example, if Carol is close friends with Alice and with Bob independently, it will be less risky for Alice to trust Bob even though they may have only transacted infrequently. It is in Bob's self-interest to remain honest in dealing with Alice due to their respective strong connectivity with Carol.

A person's identity credentials become valuable for transacting within a human community because of the reputation of the person as attested by the members of the community. Consequently, a community with a dense, accurate digital network representation can be used to create a digital "Trust Network" consisting of assertions between community members, and this provides a secure and trustworthy foundation for digital identities. Digital identities cannot be trusted unless they are based on joint sovereignty among members of a community where false assertions have serious negative consequences and where there is sufficient data to make reliable inferences.

Professor Alex Pentland was named by Forbes as one of the "seven most powerful data scientists in the world", and is founder of MIT Connection Science and the MIT Trust Data Consortium.

Thomas Hardjono is CTO of MIT Connection Science and Trust Data Consortium, and was formerly Executive Director of the MIT Kerberos Consortium.

Share this:

BLOCKCHAIN IDENTITY MANAGEMENT PRIVACTY