Bloomberg Law Tech & Telecom

Blockchain – The Future of Digital Identity?

*By **Laura E. Jehl**,*
Partner,
Baker & Hostetler LLP

This article, the second in a series, explores the use of blockchain technology to create digital identities.

A New Paradigm for Proof of Identity

Government agencies, prominent tech companies, startups and newly-created foundations are all working to develop a new paradigm for proof of identity based on blockchain technology. Known as "digital identity," "decentralized identity," or "self-sovereign identity," it would allow individuals to control their own digital identities, limit access to personal data, and provide a much-needed, secure replacement to the current username and password system for access to websites. Digital identity also holds promise for the more than one billion people worldwide who lack officially recognized proof of their existence and, as a result, are deprived of protection, access to banking, education and basic rights.

What is Digital, or Self-Sovereign, Identity?

Digital identity is, essentially, a means of decentralizing identifying information so that individuals have control over their own data. For digital identity to meet the needs of governments, individuals, and businesses, it must be *personal*, *persistent*, *portable*, and *private*:

- ***personal:*** unique to only one person;
- ***persistent:*** remaining with the individual from birth to death;
- ***portable:*** accessible from anywhere; and
- ***private:*** only the individual can grant permission to use or view this data.

Blockchain's distributed ledger technology, combined with encryption, offers the possibility of creating immutable digital identity records that can only be linked to transactions or other data with the explicit authorization of the user. Most blockchain-based ID systems rely on decentralized identifiers ("DIDs"), which hold unique metadata that proves ownership of a particular identity. This distributed, decentralized architecture—with data spread across millions of devices rather than centralized in valuable "honeypots" that attract hackers—provides far greater security against cyberattacks, data breaches, and data corruption than the current system of centralized data repositories.

In addition, because the individual controls access to the data, the individual can share only the "minimum necessary" data for each transaction, and prevent the collection and storage of vast amounts of personal information by each business or organization with which the individual interacts. As a simple example, when an individual walks into a bar and orders a drink, the individual can provide access only to confirmation of legal drinking age, instead of handing over a driver's license containing name, address, birthdate, height, weight, vision and other information. The bartender receives only the information needed to comply with legal age restrictions, and the individual can enjoy a drink without revealing sensitive personal information.

Why Do We Need Digital Identity?

Digital identity has the potential to solve a wide range of pressing problems in both the developed and the developing world.

In the developed world, the current username-and-password identity scheme used to conduct transactions over the internet is becoming more insecure and may not be tenable long-term. The internet's address system is based on identifying and validating communications between endpoints—computers—on a network. Because that architecture has no way to verify the identification of the people behind those endpoints, each website or application must develop its own system of identifying users, leading to a proliferation of usernames and passwords that is inherently insecure. Each app or website also collects its own trove of personal data, creating huge and redundant volumes of user data. These inefficiencies result in huge costs—arising from identity assurance processes, expensive and ongoing data security efforts, regulatory compliance and potential liability—for the organizations who hold personal data. For individuals, the costs are measured in time spent entering and re-entering the same data, and choosing—and forgetting—multiple usernames and passwords. And, after a seemingly endless series of data breaches, it's clear that the current system is inadequate to protect the security of sensitive personal information, including traditional forms of identity such as Social Security numbers.

The developing world, on the other hand, faces a different kind of identity crisis. Approximately one-sixth of the world's population lacks any form of officially recognized identification. Without proof of identity, individuals are often unable to vote, gain access to healthcare, buy a mobile phone, open a bank account, or enroll in school, and are at greater risk of trafficking. Persons without official identity also cannot obtain passports, register for refugee status, or register the births of their own children. Without accurate population records, public and private organizations struggle to deliver aid and services, and to verify the identities of millions of refugees and displaced persons worldwide. Recognizing these costs, a United Nations-led global partnership of governments, non-governmental organizations, and technology companies has undertaken an effort, known as ID2020, to accelerate access to digital identity.

Self-sovereign identity also promises to eliminate middlemen and streamline bureaucratic processes such as background checks, passport controls and immigration systems. When an identity is verified on a blockchain network, the verifying party can see other trusted sources—like banks, universities, or government agencies—who have verified the same data. The validation itself can be shared without revealing any of the underlying data.

What's Next?

Self-sovereign identity has the potential to reconfigure the relationship between governments and individuals, placing control of identity data in the hands of citizens and raising many new questions:

- Will governments and organizations who currently serve as “identity providers” become “identity verifiers,” since identities will still have to be originally proven in some form, such as a birth certificate?
- Despite the reduced risk of loss or theft of digital identities, will there still be a need for “identity-proofing”—checks to ensure that individuals are who they say they are, whether online or in the real world?
- Since there are multiple digital identity projects and proofs-of-concept underway, will DIDs be standardized so that the systems are interoperable and identities portable from one system to another?
- And how will existing regulations—such as the EU's new General Data Protection Regulation—interact with this new technological approach to data privacy and security?

Despite these and other unresolved issues, widespread adoption of digital identity appears inevitable. Stay tuned for developments in this fast-moving area.

