IDC LINK
Real-time IDC Research® opinion on industry news, trends and events

It Was Only a Matter of Time — Digital Identity on Blockchain

March 24, 2017

By: Stewart Bond

IDC's Quick Take

This week, IBM and SecureKey Technologies announced an initiative that will enable digital identities of people to be shared across banks, telcos, healthcare providers, and government agencies — on a secure, shared blockchain network. The blockchain network will run on IBM Blockchain, an implementation of the Linux Foundation's Hyperledger Fabric v1.0, on the IBM Cloud and high security business network, also announced today on the IBM Cloud. It's no surprise or coincidence that these two announcements were made on the same day — digital identity on the blockchain is a match made in heaven, keeping our personal information secure and private but shareable on a trusted network, and made available only to those that need to know. One digital identity used for individuals across multiple systems shared on a blockchain will also remove the need to reconcile data differences, disrupting data integration and integrity more specifically — party master data management.

Product Announcement Highlights

SecureKey Technologies and IBM will be working together to enable a new digital identity and attribute sharing network based on IBM Blockchain. The solution is being developed and tested in Canada, where SecureKey Technologies has already deployed a secure credential sharing network between financial institutions and the Canada Revenue Agency to simplify the login process for citizens. Later this year, the plan is to have a blockchain network launched for Canadian consumers, providing the capability for financial services firms to immediately verify their identity when opening a new bank account, helping citizens that are renewing driver licenses, helping contract suppliers to provision utilities and communication services, and helping to submit income tax returns. A mobile application will allow consumers to opt in on the network and give consumers the ability to control what parts of their identity information they are willing to share using trusted credentials with organizations of their choice.

IDC's Point of View

As discussed in Blockchain – A Data Management, Integration, and Integrity Disruptor?, blockchain technology is at its core a shared, trusted and immutable data store, which has the potential to disrupt data management and integrity resources, processes, and technology. The study looks at blockchain technology from a horizontal data perspective rather than vertical industry applications and discusses the realization that the technology itself solves many problems that data integrity professionals and technology providers have been trying to do for many years. One of the challenges in computing is for users and organizations to manage multiple copies of digital assets, finding the most recent version of the truth and making that available for users that depend on it.

Blockchain doesn't propose to remove all copies of data. In fact, it promotes data distribution across a network. However, the data cannot be changed by one individual; that is, it can only be changed if consensus is gained among network participants that a proposed transaction is correct and valid. Once consensus is reached, a new state is created that represents the old state of the data modified by the proposed transaction, and a new block is added to the chain. Access to the updated data is made available for approved users on the distributed network. The chain is immutable because every new block in the data store also contains the contents of the previous block in the chain. The longer the chain, the more secure and harder it is to break.

Digital identity is a growing issue in the digital economy. Even though there is only "one" physical person, digital clones often exist in data stored across every institution and organization that people have a relationship with. Clones in the digital world are often not identical and in some instances, they may be different enough to be more like a distant cousin. Data about individuals not only differs across organizations but can also be different within multiple systems of entry, record, and reference inside of an IT environment. Data integration and master data management solutions have been deployed to help organizations find the most recent and accurate data representation of customers, partners, and entities across IT environments and increasingly, across business networks. When individuals want to interact with an organization (e.g., online or on the phone), it is important that the most recent version of data about the individual is being used to provide the appropriate access and provisioning of services. Another issue for consumers is the hassle of remembering different passwords on different systems. For example, the results of a 2016 Intel Security survey showed that an average person has 27 (different) digital identities and it has become almost impossible for users to remember all the rules for each of their digital identities and credentials. Therefore, as individuals revert to a few common passwords, they increase the risk of unwanted access across multiple accounts if the credentials for one account is compromised.

Unique digital identity for individuals is already a reality in some countries such as Estonia, Kazakhstan, and India. For example, each person's individual digital ID is used to file income taxes, register property, change mailing address, vote, get cash at an ATM, and even pay for parking. The ID is carried on the equivalent of a bank card with a chip or increasingly on smartphones. Digital IDs are managed by centralized government authorities and, while making life easier for the average citizen, can also be a source of risk. Centralizing identity creates a single point of failure and builds a repository of high value data that can attract hackers, and proper controls need to be in place to maintain integrity.

The SecureKey blockchain digital identity and attribute sharing network, built on the Hyperledger Fabric and deployed on the IBM Blockchain technology, will enable peer-to-peer sharing of protected personal identities and information. Without a central point of failure or data store, this solution provides "triple-blind privacy." Simply put, the sender doesn't know where the data is going, the receiver doesn't know where it came from, and the network cannot see the data itself while in motion or at rest. Therefore, users cannot be tracked across relying parties and data is never "in the open" while it is on the network. An example provided during the announcement call with SecureKey included applying for an apartment to rent, providing a digital ID to prove that you are who you say you are, including credit rating, background check, and employment attribute data to the prospective landlord or agent. This can save the landlord or agent service fees for credit and background checks. Once the landlord accepts the application, first and last month's rent can be paid from the individual's bank account, renters insurance can be applied for, and telecommunication and utilities can be provisioned. Part of the SecureKey solution will also use chaincode, alias smart contracts, to enforce privacy and contractual agreements among parties involved in peer-to-peer data sharing and transactions.

Introduction of biometric devices for authentication can offer the opportunity for users to connect their physical identification with digital identification. The SecureKey solution will be available on a mobile device, where fingerprint recognition can be used for authentication. SecureKey also discussed the future concept of using facial recognition to validate age of majority when purchasing alcohol or for standing in front of a bank teller to open a new account or apply for a loan.

SecureKey plans to monetize the network by providing billing services between the digital ID and attribute data consumers and the providers of that data, adding a premium for network and smart contract services. SecureKey has a demonstrable business case through its existing implementation, where for example, studies have shown that the government of Canada saved $800 million dollars using a single identity authentication mechanism compared to the cost of multiple identity stacks in front of every system they had for online and call center experiences. This network also allows banks to get re-intermediated into processes that they are currently not part of and reduces call center costs by improving the implementation of data exchange within a customer's network of service providers.

Digital ID, not unlike blockchain technology development, happens within an ecosystem. The same four forces IDC identified driving blockchain development are also part of digital ID solution development and innovations: vertical industry institutions, technology providers, regulators, and consortiums. For example, SecureKey has had to work with and gain acceptance from an ecosystem of financial, healthcare, telecommunications, and utilities — all highly regulated industries. Regulators themselves are also very interested in digital IDs for auditability and control reasons. Consortiums, including the Digital ID and Authentication Council of Canada (DIACC), the Command Control and Interoperability Center for Advanced Data Analytics (CCICADA), the National Institute of Standards and Technology (NIST), the FIDO Alliance, the Open Identity Exchange (OIX), the Kantara initiative, and the Linux Foundation, are interested in the use of blockchain technology for digital IDs too.

As an individual who just moved, I appreciate this announcement. If this solution was in place four weeks ago, I would have had to change my address once instead of 25 times. As a data integration and integrity professional, I appreciate how this could have an impact on master data management, specifically in the party domain. Digital identification can be applied to individuals, legal entities, and assets. In theory, digital identification solutions provide one true digital representation or "clone" of the physical or virtual entity, in this case a party (person, company, and legal entity). Blockchain aside, the more that a single digital identity is used in place of party data stored in multiple different schema in each location it exists, the less probability data about the party will differ across applications, thus reducing or removing the need to match and reconcile differences.

Enter blockchain and distributed ledgers – technologies that ensure the current data state of an entity is a valid representation of the entity, distributed across a network of applications, including an immutable record of data provenance. The current state of the entity in the blockchain, or in this case party, cannot change unless network consensus is reached that the change is valid. Blockchain can eliminate the possibility of a party using a fake mailing address, social security number, insurance policy, or even phone number, which helps protect parties from identity theft. It also eliminates the risk that a digital identity for an individual could be different across each location where it is used.

The challenges for SecureKey and IBM will be scale and adoption. Digital identification and changes to personal information may not require millisecond transaction processing throughput but will require a reasonable response time, and the network will not be valuable to the institutions connected if consumers aren't willing to opt in. Adoption within the ecosystem will also be critical; the institutions being targeted for use of digital identity are some of the most regulated and some of the most riskaverse organizations when it comes to new technology, especially where personally identifiable information is involved.

There will be one digital representation of an individual, shared across institutions, service providers, and retailers; giving that individual the ability to control what personal data will be shared and with whom, protection from identity theft, all with validated, correct and immutable data integrity — it's about time.

Subscriptions Covered:
Data Integration and Integrity Software, Data Integration Software

Please contact the IDC Hotline at 800.343.4952, ext.7988 (or +1.508.988.7988) or sales@idc.com for information on applying the price of this document toward the purchase of an IDC or Industry Insights service or for information on additional copies or Web rights. Visit us on the Web at www.idc.com. To view a list of IDC offices worldwide, visit www.idc.com/offices. Copyright 2017 IDC. Reproduction is forbidden unless authorized. All rights reserved.