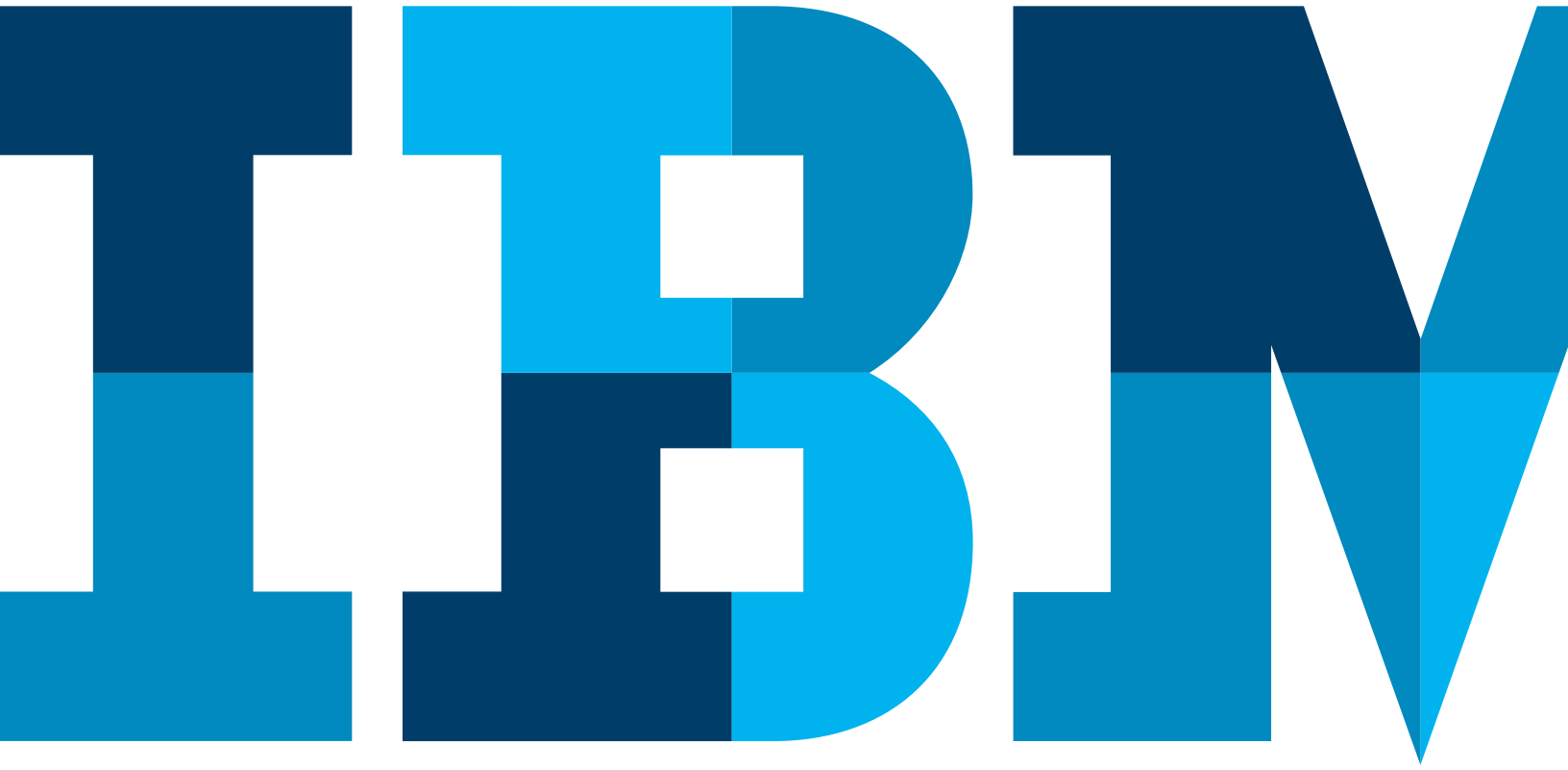
Identity Now

Building a Digital Identity Ecosystem on Blockchain with SecureKey in the Banking Industry



In 2016 the World Economic Forum recognized that identity is central to the financial services industry, enabling delivery of core financial products and services. It is also a critical pain point for FinTech innovators who are trying to deliver pure digital offerings, as the process of identifying users consistently forces them to use physical channels. Reliance on physical identity protocols introduces inefficiency and error to these processes.[1] Identity also opens up new markets. As of 2014, two billion individuals, primarily in emerging markets, were cut off from financial services, in part because they lacked identification or didn't have bank accounts.[2] Digital identity has great potential to improve core financial services processes and create new opportunities.

In Canada, the financial institutions saw this coming and decided to do something about it. Recognizing that the rules are changing, they decided that it was important to be relevant in customer authentication and ID validation. They recognized that it is essential that they deliver user experiences that **re-intermediate** them in their customer's lives.

They began in partnership with SecureKey Technologies by initially launching the SecureKey Concierge™ service, allowing citizens to authenticate to a variety of high value secure services utilizing their trusted bank credentials. Over seven million credentials have now been registered in the service, and hundreds of thousands are added per month. The service receives accolades for its privacy stance, in that the bank never knows the service a user is accessing and the government never knows the credential provider.

Royal Bank, TD Bank, Scotia Bank, CIBC, Bank of Montreal and Desjardins recently invested CAD $27 million into SecureKey to accelerate the journey, and help develop a true identity and attribute sharing ecosystem where the banks were relevant. The new service enables attribute sharing and consumption to and from other parties as well (e.g. telco and government), but it is the bank that is central in both creating the digital enablement and managing the nodes of the network. Each of the banks placed a senior executive on the SecureKey steering committee to manage governance and prioritization.

The banks felt strongly that while they needed to differentiate their own offerings, it was essential to work together in the development of a national standard, whereby the bank becomes relevant by providing value to customers in every experience—from renting an apartment, to opening a telco account, to accessing health and government services. Monetization of data was clearly a driver, but removing friction for customer onboarding with third party services, reducing risk for companies (with cross validation of attributes) and being present to improve the customer experience (with IDV, payment initiation, lending)—and doing all of this now before PSD2 regulation allows others to lead—were the main factors in banks deciding to move ahead with SecureKey.

A short video highlighting the service can be found here:

www.youtu.be/i9CxU1tghw0

The Technology

In order to achieve the goals of privacy and resiliency the service was implemented on a distributed ledger (Blockchain), where each of the banks runs a trusted peer node. Having run the Canadian ecosystem for many years, and having worked closely with both the U.S. Government on Connect.Gov and with National Institute of Standards and Technology on their new guidelines, SecureKey felt this was the only way to solve the problem at scale.

Specific goals in the implementation include:

- That no data is visible to the operator of the network
- That there is no central database or "honeypot" of data
- That there is no central point of failure
- That there is privacy so that an Identity Provider cannot tell where an identity claim is being used (imagine if the government knew every time a citizen went to the liquor store!)
- That there is no way to track an individual across relying parties

In fact, SecureKey recently won grants for its architecture and approach from both the U.S. Department of Homeland Security Science & Technology Directorate in the US and the Canadian Government.

The foundation of the technology is built on Hyperledger Fabric, which is a blockchain framework and one of the Hyperledger projects hosted by The Linux Foundation. SecureKey has been working closely with IBM on the development of the technology, ensuring that it will be able to scale to meet global demands while respecting the core security, privacy, integrity, and resiliency aspects needed for an identity network.

With the right set of partners, the benefits of a distributed ledger approach to identity management have the potential to outweigh the adoption risks perceived to be associated with a relatively new technology. The system's strong anonymity standards enable potential competitors to work together in the same ecosystem.

Its decentralized nature eliminates single points of failure, dramatically improving resilience. It also assures complete privacy for individual users while maintaining convenience and ease of access. SecureKey has implemented blockchain so that network participants require very little blockchain operations experience, and IBM Blockchain enables customers to quickly get on the high security business network with minimal operational effort. This will provide network participants with a strong customer proposition.

The Business Model

The business model of the service is quite straightforward. The providers of attributes get paid for each set they provide, and have no liability if they are wrong. The requestor of attributes pays for each set requested and generally will request more than one validator to be comfortable with the claims.

For example, a telco or a bank might request name, address and mobile number from a tier one bank (which requires a real-time bank login), but will also request that the mobile device being used by the user has been validated by the telco, and the SIM in the device matches the mobile number of record at the bank. They will also likely request a credit claim from a reputable agency, showing the credit score of the individual is over 700 and that there are no 90 day + delinquencies on file.

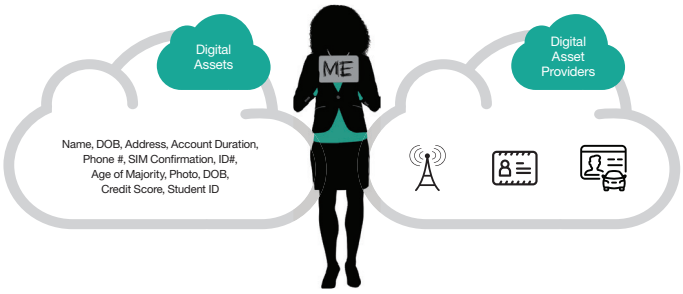
The requestor pays for each claim received and has no ability to go back to the provider if the claims have errors. The network manages the billing and provides the vast majority of funds back to the providers of claims.

Users are able to add a variety of attributes over time and share them when requested to a valid requestor.

The user provides explicit consent each time data is requested: e.g., Are you willing to share these attributes with this party for this purpose? Each action is recorded in the ledger and the user receives a secure notification on all actions.

Some sample attributes that we are enabling include:

So imagine a user experience such as renting an apartment. The prospective tenant can share identity validation (from the bank), credit score over 700 from an agency, and a background check in seconds. They can get adjudicated on the spot, then pay first and last month's rent, set up an internet service and add contents insurance in a few clicks more. The bank has made the consumer process much better, earned good revenue and perhaps sold more products. This is an example of **re-intermediation.**



Entering Other Geographies

We believe the model will replicate well in other select geographies. In Canada, we asked the banks for startup funds to get the network built and deployed. This was done through a one-time capital injection, and not ongoing operating funds. We have a contract with them that says a consumer cannot have an account unless it is linked to a bank.

The bank is the setup and recovery partner. When we share attributes we share the bank's first. Once we achieve operational funding at SecureKey (a base level of revenue), then the majority of the revenue earned with bank attributes will be shared back to the partner banks.

We believe that the model is like SWIFT, whereby each geography has a license and local team focused on successful implementation. Governance would be managed with a cross-bank team of executives. We are working with local businesses who are excited to be part of the network launch in other geographies. Please reach out and schedule some time with us.

As the banks came together in Canada, we are already working on Bank Account Open, Telco Account Open, Accessing Government Services, Accessing Medical Records and Test Results, A Social Buying Network, and Apartment Rentals - with more requests each day. There are lots of incremental advantages for banks in having a cross-border identity mechanism, but the focus initially will be local.

FAQs

Why hurry?

The banks recognize that the Silicon Valley companies are coming, creating new value propositions, slick user interfaces and compelling value propositions for customers. Apple recently demonstrated the beginning of the threat when they took over the authentication for transactions and charge the bank a fee to use their interface. This is just the beginning. If the telcos or Apple or someone else enables true identity and use cases in the phone before we do, it will be a lost opportunity. PSD regulation and FinTechs are coming quickly.

What is the business case for the bank?

Most of the banks in Canada believe this is a positive or break even business case with respect to monetization of attributes, because the bank will be buying attributes from others to improve onboarding and to reduce fraud (e.g. notifications when the SIM changes). So this is not a "move-the-needle" number. They see digital onboarding as vital in the coming age, with each percentage increase in online onboarding being worth over $100M annually. They see re-intermediation in other activities like social selling, apartment rental, phone account opening, government account access and health

services as vital to staying relevant. They see the opportunity to integrate their payment into all the ID validation use cases as another source of revenue as cash and cheques disappear.

Why was a blockchain architecture chosen?

Privacy is vitally important. The system was built from the ground up on Privacy by Design principals. The attribute sharing party must, in most cases, not know where an individual is sharing their data. A distributed architecture provides resilience against denial of service attacks that will be vital in a nationwide identity ecosystem.

There had to be no way the central broker could be honest but curious (per NIST new guidelines).

Having built both SecureKey Concierge™ in Canada and Connect.Gov in the U.S., it was determined that we couldn't solve these characteristics well without blockchain.

Why not lead as a single bank?

The banks in Canada tried this and realized that for relying parties to come on board the solution required ubiquity.

About SecureKey

SecureKey is a leading identity and authentication provider that simplifies consumer access to online services and applications. SecureKey's next generation privacy enhancing identity and authentication network enables consumers to conveniently assert identity information from trusted providers, like banks, telcos and governments, and help them connect to critical online services using a digital credential they already have and trust.

IBM Corporation
Route 100
Somers, NY 10589

Produced in the United States of America
April 2017

1 A Blueprint for Digital Identity: "The Role of Financial Institutions in Building Digital Identity" World Economic Forum report. 2016 (http://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf)

2 The Global Findex Database 2014: "Measuring Financial Inclusion around the World." The World Bank report. April15, 2015. (http://documents.worldbank.org/curated/en/187761468179367706/pdf/WPS7255.pdf)

Please Recycle

SECURE KEY

BKW03040-USEN-00