ExpertInsights@IBV

Trust me: Digital identity on blockchain

IBM Institute for Business Value

Digital identity – a market view

A popular cartoon once captured the zeitgeist of the digital age. The caption read, “On the Internet, nobody knows you’re a dog.” Now, businesses chase after digital footprints to determine precisely who you are. In the digital economy, “identity” is a vital security measure and, at the same time, the foundation for personalized engagement in customer-centric businesses. It’s based on an ever-expanding fog of data that defines a person. This includes attributes like name, address, credit score and net worth, as well as characteristics like taste in music, propensity to buy organic, health status and network of friends.

Tuned to trust

Many transactions, whether business or social, rely on understanding identity in context. As the number of these transactions pile up, so too do vulnerabilities. Can you trust the person is who they say they are – or are they impersonating someone else? Can you trust not just the person but also all of the data that characterizes them? Is the information you have accurate or has it been tampered with? Is it up to date? The current model for managing identity is quickly becoming unsustainable – costly, disjointed and all too fallible.

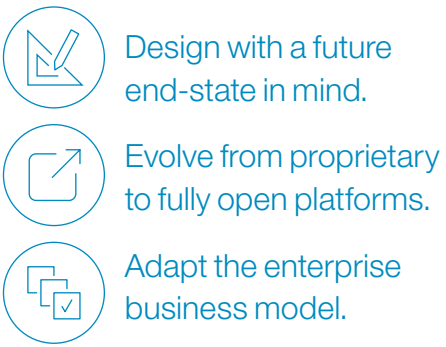
Blockchain, the technology underlying distributed ledgers shared across a scalable group of individuals and institutions, takes a new approach. Data associated with every event or transaction is time-stamped, appended to the record preceding it and available to authorized participants in real time. Individuals can't tamper with records after the fact; records can be amended only by agreement among participants. In this way, data becomes part of a reliable, unbreakable chain of trust.

Blockchain shifts the lens from disparate bits of information held by different owners to an always up-to-date lifetime history of data related to a person, place or thing. In effect, data tracked on a blockchain becomes a single source of truth. How should organizations approach this new opportunity? Our view encompasses three practices: to design, evolve and adapt (see Figure 1).

"Building trusted identity networks is a big step towards a whole new world, where companies are going to have to negotiate with individuals via smart contracts as to how they can manage and use their data."[1]

Don Tapscott, IBM InterConnect 2017 (Technology and innovation leader, author of "Blockchain Revolution")

Figure 1
Three principles can help organizations adopt blockchain for identity management



Design: The paradox of control

Empowering patients for improved outcomes

Self-sovereign identity management supports a patient-centric model for healthcare. Today, less than one-fifth of hospitals incorporate patient-provided health data into their clinical decisions.[3]

With self-sovereign identity management, data from wearables and other medical devices could be cost-effectively captured to create more personalized care plans, and to track medication adherence and healthcare outcomes. A self-sovereign cognitive identity advisor could help patients manage and understand their own health data and even choose among the healthcare providers best suited to their current needs.

In 2011 the World Economic Forum recognized that personal data had become an important new asset class.[2] This data, however, is at risk of remaining a surplus resource. Privacy and security concerns curb consumer trust and constrain the sharing of data. The result? While organizations spend money chasing down and trying to make sense of the digital breadcrumbs left by consumers, attributed personal data remains grossly underutilized.

Our view is that if users know that personally identifiable information is theirs to command, they will be more likely to share it. This user-centric model, also known as self-sovereign identity, is contingent on two principles – consent and control. Consent is the agreement (or permission) between individuals and institutions defining what personal information can be collected and used by whom and how. Control ensures that individuals have complete ownership of their personal data. The self-sovereign identity model puts privacy control in the hands of the consumer or intermediary identity broker, which consequently reduces the liability arising from identity breaches and fraud for businesses.

Blockchain technology is particularly well suited to managing both consent and control of personally identifiable information, because it can be self-managed without relying on a centralized control authority. On blockchains, smart contracts can embed rules that efficiently automate the opt-in process. They can define both who has the right to collect identity-related data as well as who has access to that data and to what level of detail. For example, blockchains can verify identity without revealing details behind that identity. In short, necessary data can be widely shared in a transparent manner and protected at the same time.

Ultimately, for a self-sovereign identity model to succeed it must be easy to use. Managing one's identity across dozens of disconnected platforms, organizations and even countries, is unlikely to satisfy anyone. Blockchain technology has the advantage here. Its distributed architecture assures that business applications can be fully interoperable, and span both industries and ecosystems. At the same time, the consent and control of personal data across a blockchain network could be managed from a single access point.

Evolve: Future-proof the platform

Because business rules and smart contracts can be built into a blockchain platform at any time, they can be extended beyond their original purpose across an end-to-end business process and a wide range of activities in a business network. Unlike a fixed, centralized database, blockchains are inherently flexible – not vulnerable to a single point of failure and easily expanded and adapted for future use.

Hyperledger – an open-source community project that is part of the Linux Foundation – brings together 127 companies and technology providers to develop blockchain technology that can flexibly evolve over time.[4] The Hyperledger approach is framed by three critical attributes: it's permissioned, secure and modular so that the blockchain platform is fully interoperable and can scale across a business network's participants.

Initially, many organizations are likely to prefer proprietary, centralized systems that are designed with consent mechanisms for personal data. This maximizes the organization's control over data integrity and its compliance with data protection regulations. Ultimately, these proprietary systems may not confer the full advantages to be gained from permissioned distributed platforms.

For banks complying with KYC regulations, for example, the processes to establish the initial authentication of identity will most likely remain as they are today. But once a verified identity is put on the blockchain, it could be made available to other banks. Canada's leading banks, which include Bank of Montreal, Canadian Imperial Bank of Commerce, Desjardins Group, Royal Bank of Canada, Scotiabank and TD Bank, recently took this approach. They came together with IBM and SecureKey to establish an identity verification network that, among other things, shares identity attributes and eliminates the need to check credit scores.[5]

As blockchain technology evolves, proprietary applications are likely to give way to more open, fully interoperable platforms. The lure of network effects and the advantages gained from data diversity are just too strong. As permissioned data is shared across institutions of every kind, context becomes richer, and new personalized products and services become possible. Moreover, identity and the data associated with it become more robustly verifiable. This well-rounded "market view" of a person's identity, actions, reputation and lifetime history establishes superior levels of trust for other individuals and businesses seeking interaction.

Building better blockchain standards

Not all blockchain implementations are equal. Ultimately, strong and trusted protocols for integrity of data will win. Industry consortia are likely to provide the best means for achieving these robust standards.

Adapt: A wider circle of trust

Making regulators trusted partners

Expanding regulatory requirements to protect personal data and privacy is often viewed as a burden. Compliance can be complex and costly; fines for violations can be onerous. Blockchain technology, however, is generally viewed with favor by regulators because, in part, it creates a trusted, real-time audit trail. By including regulators in their trusted business networks, organizations can detect potential problems before they occur.

Few attributes are more important to identity and trust than reputation. Data tracked on a blockchain could be used to measure an individual's or an institution's propensity to do what they promise, whether that's making a payment or delivering a shipment on time.

Access to data on past performance tracked on a blockchain becomes a new verifiable basis for reputation. Start-ups and smaller enterprises, whose identities and reputations have been established on a blockchain, could be more reliably accepted by trusted business networks, rather than relying on traditional measures such as brand recognition. Peer-to-peer business models, such as those for lending or insurance, could become more viable.

A recent Goldman Sachs report predicted that blockchain-enabled reputation management could accelerate the sharing economy. Using Airbnb as a case study, Goldman Sachs calculated that blockchain-based identity management, among other improvements, could potentially result in a 13–46 percent increase in worldwide booking fees by 2020.[6]

Educational blockchain initiatives are looking to tackle academic fraud, build trust and protect the reputations of educational institutions. In Kenya, the ministry of education is piloting blockchain as a single source of truth across its educational system.[7]

Blockchain-based business networks could leverage new approaches to reputation management to open up new markets. As of 2014, two billion individuals, primarily in the emerging markets, were cut off from financial services, in part because they lacked identification or didn't have bank accounts.[8] On blockchains, a combination of social, community and reputation identifiers could more quickly establish verifiable identity and creditworthiness.

Nascent markets, from community-based electronic grids to car sharing, could benefit from reputation-tracking through identity management. Reputations substantiated on a blockchain could strengthen the brand identities for those who market sustainable goods, and assure the safety of foods, medications, electronic goods and similar products.

Notes and sources

1 Clark, Jen. "Blockchain technology: the next generation of the internet." Watson IoT blog. March 22 2017. https://www.ibm.com/blogs/internet-of-things/keynote-don-tapscott-blockchain/

2 "Personal Data: The Emergence of a New Asset Class." World Economic Forum report. 2011. http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf

3 Bresnick, Jennifer. "Exploring the Use of Blockchain for EHRs, Healthcare Big Data." HealthITAnalytics website, accessed March 31, 2017. http://healthitanalytics.com/features/exploring-the-use-of-blockchain-for-ehrs-healthcare-big-data

4 Hyperledger website. Home and About pages, accessed March 27, 2017. https://www.hyperledger.org/

5 "IBM and SecureKey Technologies to Deliver Blockchain-Based Digital Identity Network for Consumers" IBM press release. March 20, 2017. http://www-03.ibm.com/press/us/en/pressrelease/51841.wss

6 "Profiles in Innovation." Goldman Sachs Global Investment Research report. May 24, 2016. http://www.the-blockchain.com/docs/Goldman-Sachs-report-Blockchain-Putting-Theory-into-Practice.pdf

7 Young, Joseph. "Kenyan Government Uses IBM Blockchain to Prevent Academic Certificate Fraud." The Cointelegraph. December 22, 2016. https://cointelegraph.com/news/kenyan-government-uses-ibm-blockchain-to-prevent-academic-certificate-fraud

8 "The Global Findex Database 2014: Measuring Financial Inclusion around the World." The World Bank report. April 15, 2015. http://documents.worldbank.org/curated/en/187761468179367706/The-Global-Findex-Database-2014-measuring-financial-inclusion-around-the-world

About ExpertInsights@IBV reports

ExpertInsights@IBV represents the opinions of thought leaders on newsworthy business and related technology topics. They are based upon conversations with leading subject matter experts from around the globe. For more information, contact the IBM Institute for Business Value at iibv@us.ibm.com.

Experts on this topic

Jai S. Arun

IBM Program Director,
Blockchain – Identity/ Security Solutions
https://www.linkedin.com/in/jsarun/
jsarun@us.ibm.com

Alexander Carmichael

Chief Operating Officer,
Promontory Financial Group Australasia LLP
https://www.linkedin.com/in/alexander-carmichael-8a90b443/
acarmichael@promontory.com

Route 100
Somers, NY 10589
Produced in the United States of America
April 2017

GBE03823USEN-00