A Blockchain Ecosystem for Digital Identity: Improving Service Delivery in Canada's Public and Private Sectors

Greg Wolfond

> *"Blockchain is more than just ICT innovation, but facilitates new types of economic organization and governance."*
>
> Sinclair Davidson, Primavera De Filippi, and Jason Potts
> In "Economics of Blockchain" (2016)

Blockchain-based solutions have the potential to make government operations more efficient and improve the delivery of services in the public and private sectors. Identity verification and authentication technologies, as one of the applications of blockchain-based solutions – and the focus of our own efforts at SecureKey Technologies – have been critical components in service delivery in both sectors due to their power to increase trust between citizens and the services they access. To convert trust into solid value added, identities must be validated through highly-reliable technologies, such as blockchain, that have the capacity to reduce cost and fraud and to simplify the experience for customers while also keeping out the bad actors. With identities migrating to digital platforms, organizations and citizens need to be able to transact with reduced friction even as more counter-bound services move to online delivery. In this article, drawing on our own experiences with an ecosystem approach to digital identity, we describe the potential value of using blockchain technology to address the present and future challenges of identity verification and authentication within a Canadian context.

Introduction

Identity verification and authentication has long been a critical component in service delivery for both the private and public sectors, but changing citizen demands in the digital age have stressed the need for new approaches to verify that an individual is who they say they are – with surety. At the same time, as more of our lives migrate online, "bad actors" such as hackers and fraudsters are always finding new ways to exploit our sensitive information for their own personal gain at the expense of legitimate users and online service organizations.

Governments, banks, telecommunications companies, healthcare providers, and businesses of all sizes are vocal in their commitment to becoming more digital – and that commitment hinges on digital identity. Digital identity is a critical, but underserved, layer of the digital era for the safety of citizens as they continue to do more online both domestically and globally. Today, every service is an island unto itself. There is no open mechanism for citizens to assert their own digital identities, for ways for citizens to have trusted third parties to add fragments or attributes ("X is a doctor", "Y's reported income from last year is", or "Z's background check has been verified") to those identities or for citizens to subsequently use their identities around the world and safely interact and authenticate themselves with online services they want to access.

Current identity tools do not support this modern approach, relying instead on physical identity documents, processes, and methods that require expensive and tedious counter visits. Username and password combinations are cumbersome and easily forgotten, while

A Blockchain Ecosystem for Digital Identity: Improving Service Delivery in Canada's Public and Private Sectors *Greg Wolfond*

patchwork solutions authenticating users with photos of driver's licenses are less secure, are often extremely difficult to validate, and are easy to spoof. The results of today's inefficient identity-verification methods are high registration costs coupled with fraud and breach risks for businesses, together with low-convenience processes for citizens.

In this article, we argue for an approach that combines the benefits of blockchain and digital ecosystems. As Gartner (2017) defines it, "A digital ecosystem is an interdependent group of enterprises, people and/or things that share standardized digital platforms for a mutually beneficial purpose (such as commercial gain, innovation or common interest). Digital ecosystems enable you to interact with customers, partners, adjacent industries – even your competition." We further argue that new digital identity standards and tools that are trusted across the economy are required to allow individuals to prove they are who they are – in a secure and privacy-enhancing way. Businesses, governments, and consumers need help to combat rising rates of cyber-fraud and cybercrime, reduce the risk and friction of transacting digitally, and increase trust and safety for citizens. As a potential enabler of such help, we look to an ecosystem approach to digital identity based on blockchain.

Blockchain – The Building Block for Better Digital Identity

A number of public and private sector organizations have implemented various identity management solutions to manage authentication and authorization privileges of their users within or across system and enterprise boundaries. Many of these current solutions rely on federated authentication and identity networks services provided by a centralized broker architecture. These solutions allow end users to authenticate or provide their identity data claims using third-party digital credentials they already have and trust, such as from their banks.

Although currently deployed identity-brokerage systems provide great utility to their participants, it has been noted that the principles upon which they are designed have several security and privacy limitations. Desirable improvements, described by the United States National Institute of Standards and Technology (NIST) (Grassi et al., 2015) and Brandão and colleagues (2015), include an architecture that reduces reliance on single point of trust and failure and prevents any single party from tracking a user's transaction, while maintaining an auditable trail that cannot be altered but also prevents data mining. The identity of the participant should also be protected using state-of-the-art cryptographic technologies and protocols.

To meet these privacy and data integrity goals, what is needed is a decentralized model based on blockchain that leverages well known technology platforms and standards, and that is available to an ecosystem of participants leveraging an easy-to-license open source codebase maintainable by an established group of developers. If designed to promote easy adoption and integration, and to comply with established security, network communication, and design requirements, this system can be implemented quickly while adhering to guiding principles that are designed to improve privacy, security and ease of access to digital services for both citizens and service providers.

These guiding principles, which have been developed in collaboration with the Digital ID & Authentication Council of Canada (DIACC, 2017), are as follows:

1. *No Centralized Authority:* Both users and consortium members interact directly with the marketplace ensuring that there are no middle-man servers acting as a single point of failure or having the ability to tamper with the transactions.

2. *Secured Blinded Infrastructure:* Participants' identities should be guaranteed and protected using state-of-the-art cryptographic technologies and protocols, while all parties involved in a transaction should remain anonymous to one another. Users' data should not be accessible to the central infrastructure at rest or in motion.

3. *Decentralized, Secured, and Private Data Architecture:* Data storage, transaction endorsement, and log and configuration rules should be available only to network participants, while the network owner maintains financial auditing events in a private ledger with the related proofs of existence stored in a distributed ledger shared with all network participants. Each digital asset should be encrypted with a split key, where the data custodian holds part of the key and the user holds the other.

4. *Privacy and Controls:* Users must always be in exclusive control. Data should be encrypted and consent should be signed with keys that are in the users' control, while data at rest must not be linkable. Data in transit must be viewed by the minimum number of

A Blockchain Ecosystem for Digital Identity: Improving Service Delivery in Canada's Public and Private Sectors *Greg Wolfond*

systems to satisfy the transaction endorsement policy (endorsement is where an organization has verified the validity of a transaction), while user transactions (such as consent) should be linkable to a user only during an authorized investigation (but not otherwise). Transactions should be endorsed by multiple organizations to be valid (to ensure that no single organization can create unauthorized transactions).

5. *Book Keeping, Audit, and Billing:* A transaction history must be kept and cannot be altered, and auditable and decentralized architecture where billing can occur without the network being live.

The application of these principles adds value to the Internet as a new, distributed platform that will help reshape the world of business and transform the order of human affairs for the better. As an indication of the potential benefits of this approach, Tapscott and Tapscott (2017) have summarized the views of 40 policymakers, entrepreneurs, and other experts in Canada on their collaborative approach to transform the country into a world leader in digital identity. This work provides valuable insight on the called "second generation of the digital revolution" that, according to the authors, is being powered by blockchain technology.

A Collaborative Approach to Identity

No single organization or industry can solve the identity challenge alone. It takes a village to make identity. This is how the world works in-person already – new service registrations require customers to show up with trusted documents from existing third parties. What is needed to expand in-person registrations so they work online and at the call centre, too. Adding integrity to the current counter processes is also required so that source documents can be verified and matched to the applicant. Expanding the identity ecosystem in this way allows companies to leverage the best and most reliable information available to validate a customer's identity. This technical implementation of the ecosystem architecture leverages blockchain and distributed ledger technology, which provides the ecosystem foundation. Blockchain facilitates the immutable, secure, and privacy-respecting sharing and validation of digital attributes for consumers and businesses.

The strengths of each company converge to create the standards needed to support a world-leading network model enabling privacy, security, and trust in digital identity authentication, verification, and attribute sharing. Standards drive consistent experiences across industries, reinforcing user behaviours, which increases security – in fact, the user experience is the security. Hiding the security model from users simplifies the experience and minimizes the attack surface that needs to be managed.

Collaboration is necessary to keep the user in the centre of their transactions across the economy. This to enable the secure digital identities needed for citizens to access services from governments and businesses alike. Neither authentication nor identity registration are a source of competitive advantage for anyone – in fact, lack of consistency is a source of risk business and a frustration for customers. We only need look at the payment system as proof here – the card-based payment system is standardized across the world, and across the payment brands. Digital identity needs the same capabilities and scope for global reach, universal acceptance, and simplified user experience.

We believe that secure, trusted digital identities will allow citizens to carry out high-value and day-to-day transactions online, in more economically efficient ways without increased risk; will reduce identity theft and improve public safety and confidence by making it more difficult to use identities fraudulently; and will improve healthcare and healthcare outcomes.

In Canada, we believe that secure digital identities will improve access to government services, regardless of a user's location, that would normally require them to appear in person, and are critical to achieving much of the federal government's innovation and economic vision – digital identification is inextricably tied to digital economy transformative innovations.

Identity Ecosystems in Action

Banks, telecommunications companies, sharing economy companies, and many others around the world stand to benefit greatly from a digital identity ecosystem based on blockchain, but in Canada, we have identified two areas that stand to benefit the greatest: government services and healthcare.

Government services

Immediate access to services has always presented a challenge to governments, where the utmost needed for fraud prevention and thorough physical identification verification has been in place. For instance, renewing a driver's license or passport most commonly requires a visit to a physical location, identity documents in hand, and wait times that frustrate citizens in the digital age.

A Blockchain Ecosystem for Digital Identity: Improving Service Delivery in Canada's Public and Private Sectors *Greg Wolfond*

With mass adoption, government services stand to reduce customer service overhead costs associated with physical office space, verification, call centres, and more, resulting in hundreds of millions of tax payer dollars saved each year, better information sharing across the country, with the additional benefit improved customer service and satisfaction.

Healthcare

Many adult Canadians manage healthcare needs for a spouse, children, or aging parents. Although they may undertake many day-to-day activities online, healthcare management often relies on phone and fax for communications with healthcare providers. Phone tag is common, with voicemail effectively unused due to privacy reasons. Appointments are only made and changed on the phone, in direct conversation. Referrals between providers "vanish" from a patient perspective, and all-too-often, a receptionist selects an inconvenient appointment for the patient, starting another round of phone tag.

Access to a patient's test results is cumbersome. Private labs provide online access to some test results because privacy laws prevent sharing results across providers. Hospitals offer online access to results, for only their tests, and not to information in other provider locations. Primary care physicians, generally, do not allow access to anything. In this digital age, fax machines continue as the gold standard for secure messaging between providers in the healthcare system – paper messaging.

With an inclusive, comprehensive, and secure method of identification Canadian healthcare could be transformed – significantly streamlining patient administration, engaging consumers in self-care and management at home, and supporting those who manage the wellness of their family. Patients and providers could securely identify during appointment bookings, access records and authorize a "circle of care" to share their patient history across multiple providers and family members.

Implicit or explicit consent by consumers to authorize access to their personal information is supported by this secure method of identification, including delegation from aging parents to a "child" who is acting as their healthcare manager, or rules delegating access to their children's records. Secure identification is critical for home-based monitoring devices such as glucometers, intelligent weigh scales, or exercise trackers as data streaming from these devices is consumed by medical record and "smart" monitoring systems. Secure digital identification also enables protection of health information for children under the care of social service agencies, or for a spouse under court order.

Although time savings for health providers and convenience for patients are significant, the transformative value to the health system is reducing the demand side of healthcare via patient engagement.

Digital Identity on Blockchain Will Benefit to the Bottom Line

Cost savings regarding password management alone range in the millions. In 2016, the average administrative cost at call centres to manage and administer a lost, forgotten, or stolen password was estimated to be $31 per incident (Martin, 2016). Assuming one incident per year per working Canadian, across 18.454 million working Canadians, $572 million are lost annually to just call centre password management services and lost productive hours (StatsCan, 2017).

But, improved password management is one of many benefits of a standardized ecosystem. With adequate funding to convene participants, the economic impact on Canada is nearly incalculable. Banks, telecommunications companies, and governments stand to save hundreds of millions per year through increased efficiencies. With application to healthcare and patient consent to view and share their records, billions can be saved annually.

There are multiple other examples of the benefits of blockchain. For instance, Tapscott and Tapscott (2016) highlight that blockchain could transform remittances – the largest flow of funds – into the developing world, and it could provide immutable land title registration for the estimated 5 billion people in the world who have only a tenuous right to their land.

Conclusion and Next Steps for Canada

Private and public sector organizations have many challenges to overcome in synchronizing and aligning their digital transformation efforts to enable the network effects to take hold. Canada's policymakers, civil society leaders, senior business leaders, and entrepreneurs, among other actors, are building strong clusters to help the country be the leader of the next era of the Internet as a platform that helps transform human affairs for the benefit of the citizens.

A Blockchain Ecosystem for Digital Identity: Improving Service Delivery in Canada's Public and Private Sectors *Greg Wolfond*

Executives can contribute to the digital ecosystem by creating open and collaborative cultures where knowledge and innovation are shared with the industry for the benefit of the masses and, more so, to establish quality and communication standards. They also can contribute by staying open to change, embracing digital adoption and transformation within their management models and infrastructure.

It is time for institutions to rethink their processes and governance structures to become more agile and innovative players. The success of an harmonious digital identity ecosystem relies on staying ahead of the organization's digital curve.

As a first step to provide better quality in the provision of public services, SecureKey Technologies' blockchain-based ecosystem (securekey.com) allows multiple partners to strengthen authentication and provide identity attribute validation, as a fabric of trust and as a solid foundation to embrace a new digital era.

SecureKey Technologies' vision for the future of digital identities redefines the ways both consumers and businesses approach identity verification and the sharing of key personal information. The ecosystem members' commitment to consumer rights and the secure evolution of digital identities has engaged more like-minded organizations to participate and create a standard of privacy and consumer empowerment across organizations and industries. This process continues to involve exceptional collaboration between SecureKey Technologies, the DIACC, Canada's leading financial institutions, government agencies, telecommunications providers and many, many more. It takes a village to make identity work.

Acknowledgements

This article is based on documents produced in collaboration with the Digital ID & Authentication Council of Canada (DIACC; diacc.ca). The DIACC is a non-profit coalition of public and private sector leaders committed to developing a Canadian digital identification and authentication framework to enable Canada's full and secure participation the global digital economy. DIACC members include representatives from both the federal and provincial levels of government as well as private sector leaders and organizations, including SecureKey Technologies.

About the Author

Greg Wolfond is the Founder of SecureKey Technologies and brings more than 30 years of experience in fintech, security, and mobile solutions to his role as Chief Executive Officer. Greg is a serial entrepreneur whose earlier ventures include Footprint Software Inc., a financial software company he sold to IBM, and 724 Solutions Inc., a wireless infrastructure software provider he took public. He sits on several boards and has been recognized as one of Canada's Top 40 Under 40, Entrepreneur of the Year, and one of the 100 Top Leaders in Identity. Greg holds a Bachelor of Arts in Computer Science from the University of Western Ontario, Canada, and a Bachelor of Science in Biochemistry and Life Sciences from the University of Toronto, Canada.

References

Brandão, L. T. A. N., Christin, N., & Danezis, G. 2015. Toward Mending Two Nation-Scale Brokered Identification Systems. *Proceedings on Privacy Enhancing Technologies,* 2015(2): 135–155. https://doi.org/10.1515/popets-2015-0022

Davidson, S., De Filippi, P., & Potts, J. 2016. Economics of Blockchain. *SSRN,* March 8, 2016. Accessed October 1, 2017: http://dx.doi.org/10.2139/ssrn.2744751

DIACC. 2017. Digital ID & Authentication Council of Canada (DIACC): Digital Identity Ecosystem Principles. *DIACC.ca.* Accessed October 26, 2017: https://diacc.ca/principles/

Gartner. 2017. Digital Ecosystems. *Gartner.com.* Accessed June 6, 2017: https://www.gartner.com/technology/topics/business-ecosystems.jsp

Grassi, P., Lefkovitz, N., & Mangold, K. 2015. *Privacy-Enhanced Identity Brokers.* Gaithersburg, MD: National Institute of Standards and Technology (NIST), U.S. Department of Commerce.

Martin, Z. 2016. Passwords the Bane of Enterprise Security. *SecureIDNews.com,* January 20, 2017. Accessed October 26, 2017: https://www.secureidnews.com/news-item/passwords-the-bane-of-enterprise-security/

StatsCan. 2017. Employment By Age, Sex, Type of Work, Class of Worker and Province (Monthly) (Canada). *Statistics Canada.* Accessed October 26, 2017: http://www.statcan.gc.ca/tables-tableaux/sum-som/l01/cst01/labr66a-eng.htm

Tapscott, D. & Tapscott, A. 2016. *Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World.* Toronto: Penguin Canada.

A Blockchain Ecosystem for Digital Identity: Improving Service Delivery in Canada's Public and Private Sectors *Greg Wolfond*

Tapscott, D., & Tapscott, A. 2017. *The Blockchain Corridor: Building an Innovation Economy in the 2nd Era of the Internet.* Toronto: The Tapscott Group. http://dontapscott.com/BlockchainCorridorReport.pdf

Citation: Wolfond, G. 2017. A Blockchain Ecosystem for Digital Identity: Improving Service Delivery in Canada's Public and Private Sectors. *Technology Innovation Management Review*, 7(10): 35–40. http://doi.org/10.22215/timreview/1112

Keywords: digital identity, online security, digital assets, identity verification, identity fraud, digital attributes, online privacy, consumer privacy, blockchain, cybersecurity

Technology Innovation Management Review

timreview.ca

Academic Affiliations and Funding Acknowledgements

Technology Innovation Management (TIM; timprogram.ca) is an international master's level program at Carleton University in Ottawa, Canada. It leads to a Master of Applied Science (M.A.Sc.) degree, a Master of Engineering (M.Eng.) degree, or a Master of Entrepreneurship (M.Ent.) degree. The objective of this program is to train aspiring entrepreneurs on creating wealth at the early stages of company or opportunity lifecycles.

- *The TIM Review is published in association with and receives partial funding from the TIM program.*

The Federal Economic Development Agency for Southern Ontario (FedDev Ontario; feddevontario.gc.ca) is part of the Innovation, Science and Economic Development portfolio and one of six regional development agencies, each of which helps to address key economic challenges by providing regionally-tailored programs, services, knowledge and expertise.

- *The TIM Review receives partial funding from FedDev Ontario's Investing in Regional Diversification initiative.*