How blockchain could prevent future data breaches

January 22 2020, by Victoria Lemieux

Credit: Tara Winstead from Pexels

Just before the new year, approximately 15 million Canadians —about 40 percent of the entire population of Canada —learned that their sensitive personal data, collected by one of Canada's major lab

diagnostic and testing services, had been breached.

The data included name, address, email, login, passwords, date of birth, [health](link) card number and lab test results. This event would be distressing enough, but it came on the heel of reports that, over a nine-month period in 2019, [19 million Canadians had already had their data breached](link).

Consumers' burden

Unfortunately, it appears that there is not much individual consumers can do to protect themselves. The only way that consumers can protect themselves is to use strong passwords and authentication, regularly check credit card statements, credit applications and histories, insurance claims and the like. This passes a large portion of the burden onto individual consumers.

The cost of such data breaches is high for society as a whole, too. The result is an erosion of trust and a reluctance to use services that gather sensitive health information, even if consumers could greatly benefit from receiving a service that diagnoses [health risks](link) and supports the maintenance or improvement their overall health. This reluctance may stem from uncertainty about how health data services will store and use their data over time.

Recent revelations about how platforms like [Facebook](link) and [23andMe](link) use individuals' sensitive personal data validates concerns that data may be shared with third parties without informed consent, adding to consumer concerns about data theft.

Reluctance to share health data

This growing reluctance to share health data is worrisome, as it will hold

back research advancements in personalized and precision healthcare which rely upon access to large bodies of data for analysis.

Faced with the threat of ongoing data breaches and unauthorized secondary use of their data, some Canadians seem willing to try novel solutions, such as blockchain technology, to address the issue.

In recent focus groups run by my research team working within the University of British Columbia's blockchain research cluster, Blockchain@UBC, consumers expressed their willingness to give blockchain a try.

As one focus group participant put it: " … someone has to start, right? There would be falls and all that and there would be corrections, I'm willing to be on the beta."

Personal health wallets

Blockchain has moved on significantly from its early association with Bitcoin and other cryptocurrencies, and is now envisioned for use in a wide variety of applications, including health care. In the case of sharing personal health data with consent, blockchains allow each individual consumer to manage their own data and how it is shared.

Consumers manage their health data as encoded credentials in their personal health wallets, similar to the Apple Pay wallet. They can then share only as much data as needed, using cryptographically encoded and distributed peer-to-peer networks, to fulfill the purpose of the data collection.

Using their wallets, consumers can provide their personal health data to labs, research partners, health-care practitioners and others, along with consent that describes how the recipient of their data is allowed to use

the data and for what time period. Recipients can be assured that the data they receive is shared with the consumer's consent, and consumers can be assured that their data will be treated appropriately by the recipient.

In some cases, such as in the context of health-care research, consumers may even receive a reward for contributing their data for the advancement of science. The use of a personal health wallet keeps data in the custody and control of consumers, while the use of encryption for data in transit over a distributed peer-to-peer connection between consumers and those with whom they share their data improves privacy and security.

Barriers to consumer adoption

There's no question that there are challenges to using blockchains for health data management, as Blockchain@UBC's early research results reveal. For one thing, consumers find it difficult to manage their private cryptographic keys—the digital key used to encrypt and decrypt data. These can be long, difficult to memorize and easy to lose.

In a truly decentralized blockchain, if consumers lose their keys they could lose access to their health data and not be able to recover it, in the same way that [loss of private keys has denied consumers access to their cryptocurrency](link).

Our research indicates that a hybrid approach that gives [consumers](link) control over their health data wallets but provides them with a service to recover their private keys in the event of loss may be the best way to ease into the use of blockchains. Ensuring that this approach does not compromise privacy and security is paramount, however.

Some participants identified the risk of exclusion of certain groups, [such](link)

[as of the non-tech savvy or older populations](#). Yet a participant in an older age demographic said, " … actually today older people have more access to smartphones then they have had in the last five or 10 years. Now it is a one- or two-step procedure."

Another older user said, "I think it will come to a stage that it will be much easier to use for older people." These early research results indicate that Canadians are open minded about [blockchain](#) as a novel way to address secure and privacy-preserving data sharing.

There is still much work and research to be done before blockchains would be ready to roll out widely for consumer health data management, but with the recent announcement of a [major new project on blockchain-based health data management to be funded by Canada's Digital Technology Supercluster](#), there is hope that Canadians will soon have new ways to protect their privacy while improving their health.

This article is republished from [The Conversation](#) under a Creative Commons license. Read the [original article](#).

Provided by The Conversation