Privacy, blockchain and the Internet of Things: Can we keep control of our own identities?

10 September 2020

Credit: Pixabay/CC0 Public Domain

New research from The University of South Australia indicates there are key privacy issues inherent to current blockchain platforms, suggesting greater effort should be made to refine the technology so it conforms to privacy rights and expectations.

Given how much we depend on it today, it's easy to forget that only 20 years ago, the Internet didn't really feature in most people's lives—in 2000, there were just 361 million web users globally, or about 6 percent of the world's population.

Now, in 2020, an estimated 4.57 billion people access the Net regularly, with almost 90 percent of Australians plugged into the online universe.

The rise of digital connectivity has brought profound benefits in some areas, but serious disruption has followed in others and, increasingly, people recognize the need to avoid techno-pitfalls in the future.

One of the biggest worries about our digital lives is privacy, and UniSA emerging technologies researcher, Dr. Kirsten Wahlstrom, believes the next generation of connected software and hardware could push the issue to breaking point.

"We're at a really delicate point with this because, increasingly, societies and economies are organized around data, and that has huge implications for privacy," Dr. Wahlstrom says.

"The main problem is, we're still struggling to understand what 'privacy' actually means in an online world—it's not the same as data security and protection, it's about how individuals control their whole online identity, and expectations around that change from person to person and situation to situation. By now we should have smarter technologies that recognize those changing contexts and preferences, but so far that hasn't been a priority, so, in fact, emerging technologies like blockchain and the Internet of Things have the potential to further compromise people's privacy."

A new paper from Dr. Wahlstrom and colleagues, Dr. Anwaar Ulhaq and Professor Oliver Burmeister (both from Charles Sturt University), suggests the exact features that make blockchain such a secure technology also make it a privacy minefield.

Blockchains use details of previous transactions, including participants identities and exchange values, to verify future transactions by embedding this information in the data chain, and the viability of the system depends on the uneditable nature of each block.

"The European Court of Justice ruled European citizens have the right to be forgotten," Dr.

Wahlstrom says, "but once someone's details are embedded in a blockchain, the system never forgets—yes, those details might be encrypted, but they are also part of an irreversible ledger, and one that's on the cloud.

"As long as a blockchain is in existence, it clashes with the European ruling that people have the right to retract data."

Recognizing there are also many benefits to the blockchain system, Dr. Wahlstrom suggests greater effort needs to concentrate on developing variations of the technology that retain its virtues while also taking the privacy consideration seriously.

"For example, our research has looked at the Holochain platform, which uses a distributed hash table to break the blockchain up, and then the chain, instead of sitting on the cloud, sits where end users want it to sit," Dr. Wahlstrom says.

"This allows individuals to verify data without disclosing all its details or permanently storing it in the cloud, but there are also still a lot of questions to answer about how this affects the long-term viability of the chain and how it obtains verifications."

With a number of recent incidents indicating blockchains are not the 'unhackable' technology they were once claimed to be, privacy concerns about the platform are mounting, and the same worries are now also surfacing among leading Internet of Things thinkers.

"Some years ago, I was at a presentation by Vint Cerf (Google's "Chief Internet Evangelist'), and I asked him about privacy, and at the time, he thought it was irrelevant, a view he was then well-known for," Dr. Wahlstrom says.

"Whereas in 2017, he and a co-author wrote that privacy is one of the biggest issues facing the Internet of Things and he called for regulation—if we have millions of devices collecting data about life on Earth: who controls it, how can we use it and how can we opt out when we want to?"

Dr. Wahlstrom believes we have reached a crucial point where these considerations must be anticipated and addressed as an integral part of developing new technologies, rather than just treated as a secondary issue that can be tackled reactively and retrospectively.

"We know that technologies disrupt society, and too often they do that in ways that we're not fully aware of when it is actually happening," she says.

"Researchers and technologists can apply ethical analysis approaches, like the one proposed by The Ethics Center at Sydney University, to see how their innovations might disrupt society, both the positive and negative, and then develop ethical, practical processes to deal with those impacts on society before they occur. In respect to privacy, I think the crucial first step is for the industry to develop a clear definition of what 'privacy' actually is—what we are trying to protect and why—and then agree standards to ensure those requirements are met across the board. It shouldn't be an afterthought anymore."

More information: Kirsten Wahlstrom et al. Privacy by design, *Australasian Journal of Information Systems* (2020). DOI: 10.3127/ajis.v24i0.2801

Provided by University of South Australia