Why blockchain could mean fewer hassles for students and workers proving their credentials

October 4 2022, by Rory McGreal

Credit: Samet Dikmen from Pexels

Microcredentials—attestations of proficiency in a specific skill or knowledge base that are certified by an authority—can provide evidence

of a person's skills to employers.

While microcredentials are becoming more popular, the concept is hardly new: A driver's license or the [St. John Ambulance certificate](#) could be considered as microcredentials, attesting respectively to a person's driving skill or their competency in administering first aid.

Blockchain technology is [appropriate for microcredential implementation](#). Blockchain can best be described as a digital ledger that records information that can be shared among a community of users. Bitcoin and other crypto-currencies are the best-known examples of [blockchain](#), but blockchain has uses beyond financial transactions.

Student records stored in blockchain for security limit access only to legitimate users, such as institutional administrators and potential employers selected by [students](#) or job seekers. Traditionally, institutions own and control certifications like degrees, but that could shift with "digital degrees" and microcredentials that rely on blockchain.

Verifying accomplishments

Besides providing effective security and privacy for users, blockchain can also facilitate the maintenance and dissemination of the credentials, while ensuring that access is readily available for students under their control.

Because of its immutability, blockchain can be used to attest to and verify students' accomplishments. This is important for students seeking to [have their credits recognized](#) whether because they are studying to obtain new professional accreditation, studying in multiple institutions or because they are moving for study or employment.

Blockchain is distributed, meaning that multiple copies of the same

information are stored on different computers. So, blockchain is not controlled by any central authority and the "blocks" in the "chain," linked chronologically, are shared in a P2P (peer-to-peer) network, which can be accessed from any node or point on the network.

These blocks are immutable, as any change to the original leaves the first iteration intact and accessible.

When students or job seekers want to have credits transferred between institutions, gatekeepers—for example, post-secondary institutions or employers—typically insist on receiving copies of diplomas and degrees directly from each institution. As more students gain credentials from multiple institutions, this process becomes increasingly untenable.

Students need to control this process and blockchain can provide a solution.

Securely validates learning

In 2019, McMaster University announced it was awarding "digital degrees" using blockchain to Faculty of Engineering students after the university implemented microcredentials using blockchain to securely validate students' learning.

Some post-secondary institutions are implementing pilot projects with eCampus Ontario and industry partners to award microcredentials using blockchain.

Microcredentials are now offered by post-secondary institutions, sometimes in partnership with corporations to target labor market needs. These may come in the form of "digital badges." Digital badges are easily verifiable testaments to when, where and how skills have been mastered. Meta data in digital badges allows viewers to click on the

badge to [learn things like criteria for earning the badge, the date it was issued or when it expires](#).

Maintaining privacy of data

Certification by blockchain begins when a trusted institution issues the microcredential and creates a blockchain. The student then sends [a public key](#) password to the institution, requesting a transcript be sent to a potential employer.

The institution then adds a block onto the blockchain and sends the micro-credential, which is verified and forwarded to the potential employer. The learners can keep private keys to their credentials in [an offline digital wallet](#).

Maintaining the privacy of the data is essential. With blockchain, the ownership of the microcredential rests with the individual, not the [institution](#).

Blockchain supports more control for students and has the capability of further democratizing education. It empowers students to maintain control of their now-secure credentials and allows them to be confident their acquired skills and knowledge will be valued.

Potential concerns

However, there are [some ethical](#) and logistical concerns. Right now, when a person seeks to transfer credits through traditional channels, they can choose which documents or certifications to share with employers: mistakes, or aspects of one's past credentials and experience deemed less salient or undesirable can be addressed or ignored.

But blockchain is immutable and this immutability can cause its own problems when mistakes cannot be erased.

Students cannot omit blocks from the chain that they do not feel are appropriate or that could damage their reputation. So, how can they create different narratives for diverse purposes or highlight and/or hide different experiences? What happens if someone wants or needs to start anew? Is there a right to forget?

What if a student loses their key? *The New York Times* reports that lost passwords have locked millionaires out of their bitcoin fortunes. Will students and workers fare any better when it comes to academic and professional records? Who will respond to these problems within institutions?

These are questions post-secondary institutions and our society at large will increasingly need to navigate.

This article is republished from The Conversation under a Creative Commons license. Read the original article.

Provided by The Conversation