Why IT Matters to Higher Education
EDUCAUSEreview

Will Blockchains Revolutionize Education?

by **DaveMcA McArthur** Monday, May 21, 2018 Editors' Pick

Although most ideas for using blockchains in education are overhyped, carefully designed distributed ledgers show promise.

Credit: Foxy Burrow / Shutterstock © 2018

Blockchains, first introduced by Satoshi Nakamoto for use in **bitcoin**, are now being used across many industries. At their core, blockchains are trustworthy, distributed digital ledgers. Unlike databases maintained by a centralized authority that guarantees data integrity through its proven trustworthiness and practices, blockchains are records of transactions that are replicated across many systems (or nodes) and are cryptographically guaranteed to be immutable.

In the public blockchain that bitcoin uses, this immutability is guaranteed by cryptographic hash functions and a clever consensus algorithm that requires blockchain miners to solve puzzles; in doing so, they validate blocks of records, which are then accepted into the blockchain. Figure 1 outlines blockchain processes; more details are available elsewhere.[1]

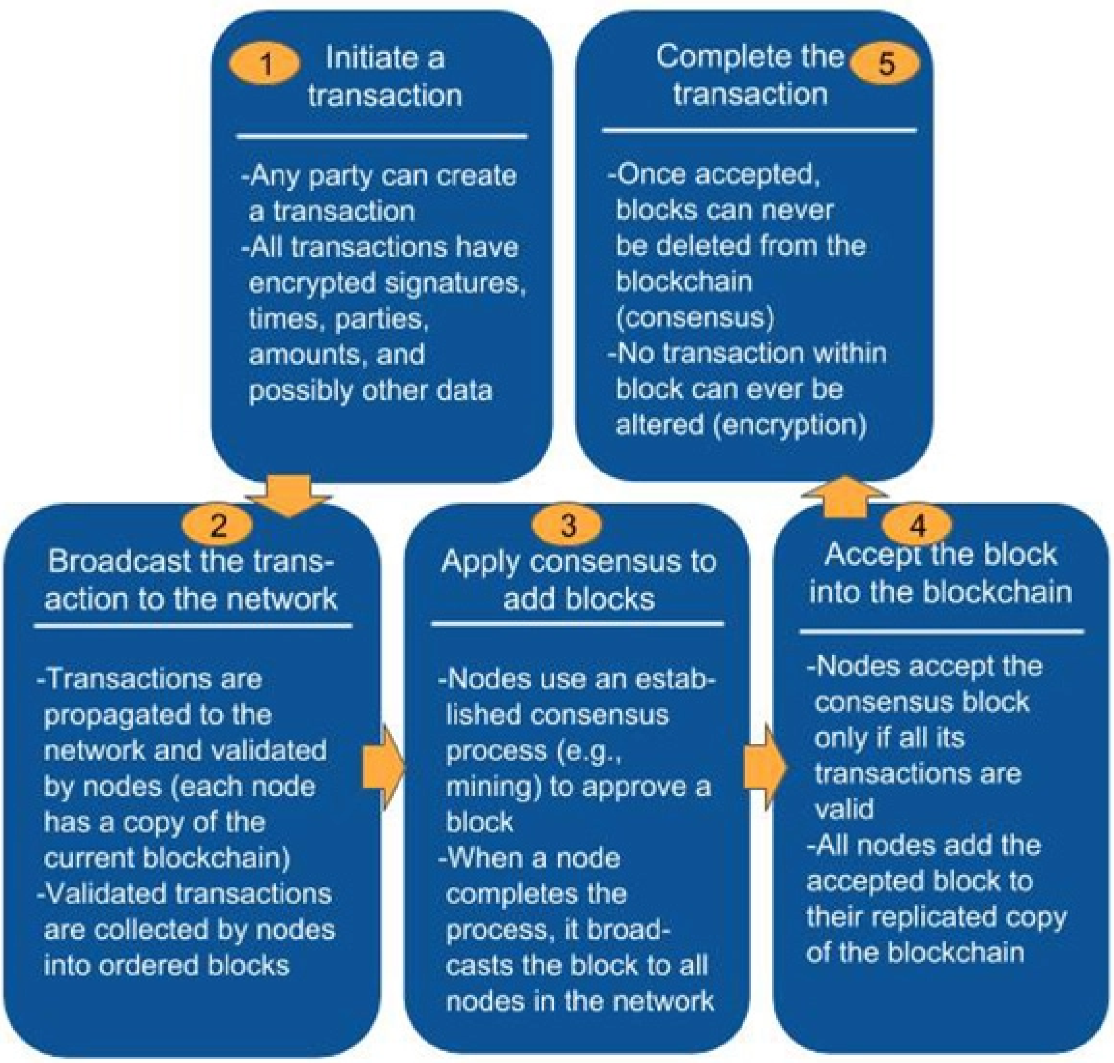

Figure 1. Steps in the blockchain approach

The benefit of the blockchain approach is that people who have no knowledge of one another can engage in business transactions. The blockchain is, in other words, "a machine for creating trust"[2] that potentially eliminates intermediaries in all sorts of exchanges. Researchers have devised blockchain applications in various areas, including smart contracts, intellectual-property registries, and storage of medical and educational records.

The public blockchain may be ideally suited to currency, but when it is applied to other areas, its benefits are offset by several limitations. One problem relates to the high cost of ensuring consensus when records — including potentially large ones — are accepted into the public ledger. A second problem is that acceptance into the public blockchain guarantees a record's immutability but not its value or quality. These and other limitations arise in relation to using the public blockchain to manage educational records. To address these issues, a blockchain alternative — permissioned distributed digital ledgers — shows great potential.

Blockchains in Education

Researchers, educators, and developers have envisioned various roles for blockchains in education and training, including their use for storing standards and issuing credentials. Several possibilities arise based on ideas from blockchains that provide trustworthy intellectual property records. For example, an educational standards committee might upload formal statements of their official competency hierarchies to a blockchain. Further, smart contracts managed in blockchain systems such as **Ethereum** could establish conditions under which a student would receive a certificate from a provider, and a series of those contracts could define a full degree program. As these students progress toward degree fulfillment, their blockchain records could be tracked automatically and shared in real time with potential employers.

While some economists view smart contracts simply as a way to reduce the costs of secure payment,[3] other analysts see them as a first step toward an ecosystem in which traditional centralized control of education gives way to distributed local creation and delivery of learning content.

Credentials and Competencies

The possibilities for blockchain are intriguing, but by far their most popular use in education today is in providing authentic records of student credentials and competencies.[4]

A prime example of this type of use is **Blockcerts**,[5] a toolkit that lets users create, issue, view, and verify blockchain education credentials. Issuers, such as schools, create the certificates, which can contain a wide range of assertions about an individual's skills and achievements. Students who have earned a certificate send their identification to the issuer, who then signs the certificate once all of the requirements are met. Completed certificates are submitted to bitcoin's blockchain, where external agents can verify that they are authentic and tamper-proof without having to rely on the issuer.

Blockcerts is an example of an innovative system that makes use of blockchains for functions unrelated to its original applications in finance. Blockcerts puts *off-chain content* — that is, assets other than digital currency — on the public blockchain by attaching arbitrary data to new records. In such applications, the currency associated with records is unimportant; the applications are simply paying a small price to use the trustworthiness and immutability of blockchains.

Blockcerts records provide a high-tech way of managing educational credentials, but the certifications are often for semester-long courses. Other educators want to use blockchains to promote the use of badges, which are much smaller-scoped credentials. So, while a traditional course might provide a single credential for, say, introductory robotics programming, badges could be issued for mastering separate topics such as sensors, basic movement, flow control, and robot math, with a final badge for a robot performance challenge. Other badges might recognize achievements, such as being a student tutor, that formal credentials rarely record.

Open Badges: A Transformative Step?

Badges can benefit students by giving them credit for a variety of acquired competencies, rather than only the collection of skills that providers package up in single courses or degree programs.[6] Further, badges issued by different providers can be assembled into an **open badge passport** that students can share as they wish.

Some advocates claim that open badges could stimulate a new marketplace for digital learning resources and that blockchains can play several essential roles in this revolution. For example, badge issuers, which are often small groups, often cannot afford much marketing and could benefit from publishing records to a public blockchain at almost no cost. Distribution is also immediate and cheap. An open blockchain can be used directly to publish badges, avoiding intermediaries and gatekeepers and further reducing costs. Finally, publishing badges to a blockchain offers providers and consumers an instant guarantee that their product or credential always will be available and cannot be tampered with, which can confer trustworthiness on new badge producers.

Open badge proponents see blockchains as a big step toward disintermediating educational institutions.[7] Such a transformation would change not only who provides educational services but also what kinds of credentials are offered. As a result, badges and other granular learning credentials or nanodegrees could become as ubiquitous as traditional degrees are today.

Limitations of Blockchain in Education

Both large-scale credentials and small-scale badges could use a blockchain's impressive record-management functions in innovative ways. However, bitcoin's public blockchain also has several downsides compared with other digital ledgers. At the very least, these limitations should give pause to evangelists who envision a blockchain-inspired educational revolution.

For Starters: It Is *Not* Free

For most of its history, bitcoin's blockchain has been almost free to users, but it is not free to *providers*. Miners, who play the essential role in consensus processes, pay a high computational price to validate new blocks. By some estimates, to ensure that a decentralized ledger can't be monopolized by any one group, blockchain miners already burn as much energy as the nation of Cyprus on an ongoing basis.

Assuming miners continue to earn bitcoins as a reward for successfully adding a block, a pool of rational miners should be willing to spend almost a bitcoin of processing energy to make a bitcoin. As the price of a bitcoin rises — in 2009, it traded at $27, while in December 2017, it topped $19,000 — overall energy consumption will continue to increase. The exchange rate for bitcoins is clearly volatile, but however it changes, current consumers enjoy the use of bitcoin's blockchain largely thanks to miners' willingness to expand the bitcoin money supply at their own expense. This could easily change; if so, consumers will likely see their costs rise.

Miners are compensated both indirectly by their rewards for adding to the blockchain and directly, through the fee they charge consumers for accepting their transactions into blocks. These fees are not fixed; in effect, they are user bids on miners' processing power. Such fees, which were near zero for so long, started to rise in mid-2016 and now routinely exceed $2 per transaction. This rise relates to the energy that miners devote to adding blocks. As processing costs have grown, miners have begun prioritizing transactions that pay a higher fee. User costs thus will continue to rise as long as processing power remains scarce relative to demand. As mining algorithms improve and processors speed up, fees may stabilize, but the big picture is clear: bitcoin's blockchain is not free.

Given this, potential users will adopt the public blockchain only if it provides positive value after fees are subtracted. This may be the case for bitcoin transactions, but most of the transactions we reviewed use bitcoin's blockchain as an infrastructure to represent nonfinancial assets, taking advantage of its openness, security, and reliability. So, while the market value of a bitcoin on the blockchain is, at any given time, perfectly clear, the value of off-chain assets that piggyback on bitcoin's blockchain is much less so.

Users who put high-value financial assets, such as property titles, on the blockchain still might be willing to pay escalating fees. But many users whose off-chain assets are of modest value, such as diploma records and small-scale badges, are unlikely to find bitcoin's public blockchain a cost-effective infrastructure.

Other blockchains may be no more economical; as of late 2017, storing a small (1 KB) contract on Ethereum could cost almost $100.[8] This amount may not seem excessive, since ensuring immutability would require replicating the contract across thousands of nodes. Still, badge providers and badge users might prefer less-expensive ledgers to store and distribute their credentials, even if those ledgers are less trustworthy. After all, in many contexts, trust alone is insufficient.

The Limits of Trust

Simply establishing trust does not ensure a record's enforceability, quality, value, or accuracy. Parties wanting to use a public blockchain to record off-chain assets face another problem, this one related to real-world laws. That is, blockchain records of off-chain assets might be immutable but not enforceable, or they might be necessary but not sufficient conditions for ownership exchange. For example, a blockchain that records the transaction of a car deed could replace the role of a notary, but the DMV, local tax agencies, and private insurers would still be involved and could have reasons to deny or modify the sale, at least in the current regulatory environment.

Quality or value is a more serious issue, particularly for education. The public blockchain's openness is an attractive infrastructure for many users, but it also poses challenges. If, say, a public blockchain credential claims that Bob got a badge from Alice, it means that anyone can now be confident that Bob did indeed get a specific badge (at a specific time) from Alice. However, this immutable authenticity says nothing about the value or real competencies that Bob gained; the badge might be as valuable as an MIT credential or as worthless as a degree-mill diploma. Clearly, the trustworthiness of blockchain records should not be confused with the quality or value of their contents.

So, while the public blockchain's openness and low barriers to entry could lead to an explosion of new educational providers offering digital credentials for consumers, in the absence of regulation, it is unclear whether this will improve the available educational resources or simply produce a barrage of dubious badges and credentials. Using the public blockchain will not prevent the development of quality-control regulations in the future, but it is unclear how such regulation would square with blockchain's freedom from centralized authority.

An even more basic problem is that statements that are now true but could later prove false can be immutably placed on the public blockchain. This might not matter when the blockchain is used to record "enduring truths" such as patents or even medical protocols and educational standards. Many off-chain records, however, represent time-dependent events such as medical records, which establish facts (such as a patient's blood pressure) that are true today but are likely to be different at some point in the future. Similarly, educational credentials might authoritatively establish a student's skills after completing a course, but those skills could strengthen or degrade over time.

The primary approach to addressing this is to add information to the records that contextualizes their truth, such as timestamps for medical test results and expiration dates for assertions about competencies. Another possible solution is to add links to information outside the blockchain to verify the value or quality of, say, a credential or a badge issuer. The linked data would, in effect, bring relevant data on such a credential or issuer into the record, resulting in less need for an intermediary to interpret that record.

Although promising, this approach has two problems. First, adding the linked data could lead the public blockchain to grow to an unmanageable size. Second, while blockchain records are guaranteed to be immutable, no such guarantees apply to externally linked data. To preserve this immutability, **oracles** have been suggested as intermediaries. Blockchains can guarantee immutability because they cannot access content outside their records. Oracles are agents associated with a blockchain that would be trusted to verify external data for blockchain decisions under specific conditions. For example, if a blockchain contract required payment only if a specific stock reached a given value by a specific time, an oracle would be established to poll stock exchange data.

Improving on the Public Blockchain in Education

As the above discussion shows, applying bitcoin's public blockchain to education entails significant limitations. Some remedies to overcome these limitations may succeed; others, such as oracles, seem to be kludgy patches to the elegant ideas that spawned bitcoin. Given the range of challenges to blockchains — especially in the case of off-chain records — it is wise to consider alternative approaches to educational record management. One such alternative is the *permissioned distributed ledger*.

Permissioned Distributed Ledgers

Whereas public blockchains are open to all, permissioned ledgers impose membership requirements on users and may also confer different access rights to different classes of users. Permissioned ledgers have many of the public blockchain's impressive features. They are open systems that allow participants who do not know one another to trust one another; they avoid the need for centralized authority; and they are robust, persistent, and resistant to censorship. They also overcome some of blockchain's limitations.

In a permissioned system, credential issuers are vetted by members, so they are guaranteed to meet the community's formal or informal accrediting standards; this addresses the blockchain issues with quality in relation to off-chain asset management. Permissioned ledgers also address cost issues. When members in a permissioned ledger know and trust each other, there is less need for the inefficiencies and relatively high costs associated with public blockchain mining protocols. Proponents of permissioned ledgers suggest that, in place of mining, lower-cost algorithms such as round-robin consensus might be sufficient in education and other areas where community trust or external regulation is high.[9] In a public blockchain, trust comes from the infrastructure alone; in permissioned ledgers, it comes from the mutual knowledge of the participants as well as from the consensus protocols.

Several systems that initially used the bitcoin's blockchain because of its convenience are now planning to move to permissioned platforms. For example, the most well-known ledger for educational credentials, Blockcerts, still uses the public blockchain. Its developers, however, acknowledge that the current version is only a first step and that bitcoin's infrastructure cannot meet their long-term needs. The next version of Blockcerts will use Merkle trees and avoid expensive mining protocols.[10]

Also, the initial Blockcerts system sidestepped the quality problem because MIT was the sole credential issuer, so quality was a given. Thus, the first version of Blockcerts was essentially a tightly permissioned or private blockchain built on top of a public one. This took away the openness of public blockchains yet still exacted its high price for mining. A more general approach would use a permissioned ledger infrastructure that allows for many members, not just one, and would use a less costly but still highly trustworthy consensus protocol.

How Permissioned Ledgers Might Work

As an example, we'll use a permissioned ledger network for badges. We might begin with core Blockcerts services for creating, issuing, verifying, and sharing credentials (see figure 2). Issuers would have a collection of badges that they are accredited to award based on well-defined evidence. Student recipients could store these badges in digital wallets to share as they choose; other tools would enable third parties, such as auditors and employees, to verify the badges.

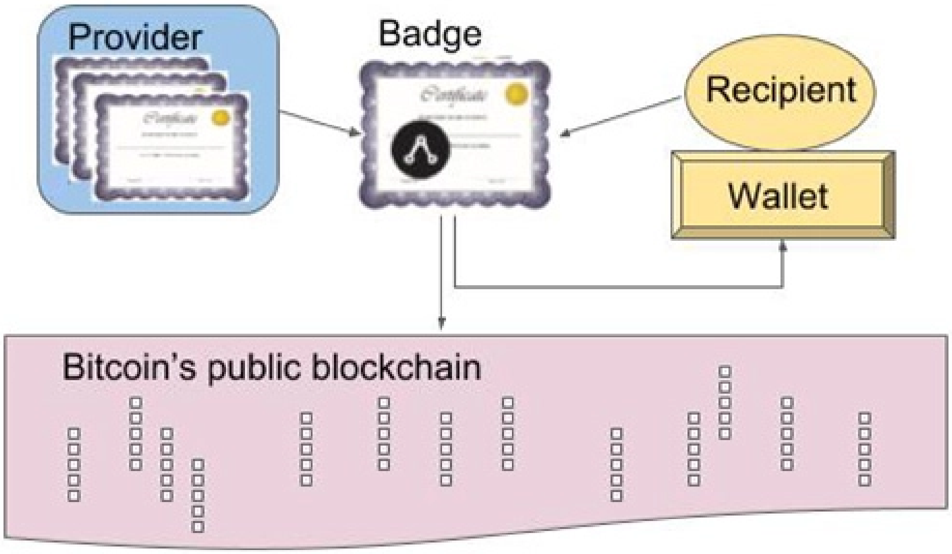

Figure 2. Outline of single-provider components of a permissioned ledger for educational badges

This permissioned ledger would differ from a simple Blockcerts system in the components that surround it, some of which could be borrowed from **Hyperledger** or other new blockchain platforms. Instead of a single issuer, the system would permit multiple members (see figure 3). Unlike an open blockchain, however, the permissioned ledger would establish policies on membership and permissions available to members. Badge providers would be central members and would have permissions to create and deploy badges and query the ledger. Other groups, such as auditors or researchers, could participate, but they would have more limited permissions to use ledger data.

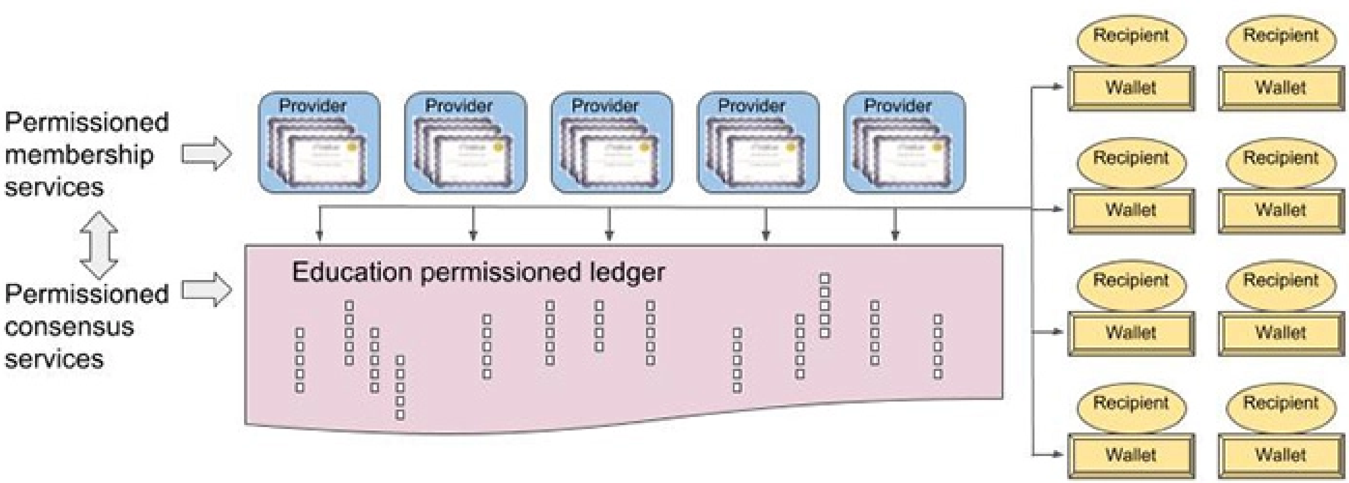

Figure 3. Outline of membership and consensus service components of a permissioned ledger for educational badges

The permissioned ledger would also use consensus protocols, rather than mining protocols, to guarantee immutability in a less costly way. A ledger's overall trustworthiness would be a function of both the technical strength of its chosen consensus protocols and the restrictiveness of its membership policies. Each permissioned ledger would need to make these two decisions in coordination.

Discussion: Issues and Opportunities

Although they have already shown promise in managing educational records, permissioned distributed ledgers have their own limitations. Thus, before they can be used successfully on a large scale, several challenges must be addressed.

The Openness Issue

Although well-designed permissioned ledgers can address some of the quality and cost shortcomings of a public blockchain, they sacrifice openness and anonymity. These issues may be critical for currency blockchains such as bitcoin, but they are less essential for communities using ledgers or blockchains to manage off-chain assets (such as educational credentials). Moreover, various options exist for keeping membership as open as possible while still ensuring ledger quality:

- **Accreditors:** Government-supported accrediting agencies could review all candidates and award membership only to providers who pass; specific badges could also be reviewed for inclusion.
- **Professional societies:** Subject-area experts could establish content standards and award membership based on provider compliance; standards would be revised as subject areas change.
- **Peer groups:** Groups of providers would arise dynamically and could use social networking platforms to establish policies for provider membership and badge quality. Policies would likely change rapidly as the distributed groups and their content foci evolve.
- **Fully open:** All providers would be accepted for membership, and all of their issued badges would be accepted into the ledger.

These and other approaches could be tested and refined in parallel experiments conducted by various education communities.

A Ledger Ecosystem

With new platforms such as Hyperledger, little time or money is required to assemble and change a permissioned ledger such as the one shown in figure 3. Members can be easily added, and new consensus protocols are plug-and-play. In a broad sense, permissioned ledger openness in education will be guaranteed not by every ledger including all providers but rather by blockchain technologies letting communities inexpensively establish their own distributed ledgers with varied membership and consensus policies. This will give students, trainees, and other learners a range of choices in education providers and badges.

Further, small badge providers could be members of many permissioned ledgers, perhaps even issuing different badges on each one. Students might seek out badges of specific providers wherever they are members, for example, or they might patronize a permissioned ledger that has developed a reputation for high-quality providers and badges in a specific subject area.

This dynamic ecosystem of permissioned ledgers, providers, and recipients could disrupt the traditional organization of education, but it is probably too soon to declare a revolution in learning. Just as traditional banks are now investigating how to use blockchains to streamline their transactions,[11] traditional higher-education institutions can use private permissioned ledgers simply as a way to reduce administrative costs for recording and conferring academic degrees. Such evolutionary uses of ledgers in education, at least in the near future, are likely to be more common than revolutionary ones.

Standards and Interoperability

Given the potential growth of ledgers, providers, badges, and other educational credentials and the records for each, permissioned ledgers for education could create a massive network of structured databases. This could make it difficult for students to find what they want, particularly if credentials lack a common language and fail to adhere to interoperable standards.

The importance of a common language for credentials has long been recognized. For example, the **Credential Engine**, built on work by the **Achievement Standards**

Network and the Credential Transparency Initiative,[12] established the **Credential Transparency Description Language** (CTDL). **The Open Badge initiative** is developing similar standardized terms, focusing primarily on granular learning resources rather than degrees and other large-scale credentials. Together, these efforts already provide a rich vocabulary for describing credentials and badges, the competencies they comprise, their issuers, how credentials align with educational standards, credential assessments, credential revocation conditions, and so on.

This work is relevant to blockchains and permissioned ledgers for education in two ways. First, it enables ledger developers and member providers to describe their credentials, badges, and competencies in common terms, making them easier to find and compare by students, workers, and employers who might be looking for web-based learning resources. Blockcerts certificates are already compliant with Open Badge standards.[13] Second, it provides the kind of information that should be added to credential records to articulate their quality and trustworthiness. For example, records that are compliant with Open Badge standards could provide extensive data on a badge issuer, the badge's associated competences, and the evidence used to verify that students possess these competences.

Blockchains in Education: Evolutionary, Not Revolutionary

Public blockchains and permissioned distributed ledgers could be applied successfully in many ways to education and learning. They offer several advantages over the traditional distributed database management systems (DDBMSs) that have been the backbone of earlier educational technology infrastructures.

The main difference between a distributed ledger and a DDBMS is the immutability of a permissioned ledger's records. This factor ensures that any credential that a ledger says a student obtained from an issuer was in fact awarded by it. This feature is significant: It means that no intermediary is needed to assure a credential's authenticity once it is issued. Ledgers and blockchains can also transform education more broadly by giving small badge providers an opportunity to publish their digital resources easily and thus compete with established educational institutions.

But these changes alone will not lead to a revolution in learning. By itself, the underlying technology of permissioned blockchains is not sufficient to guarantee the development of a top-quality educational content-management system. Distributed ledgers still will require a common language to describe their records and must provide a foundation for rich sets of services beyond just issuing and retrieving records.

All this means that as traditional intermediaries disappear, new ones will arise. In addition to offering courses and badges, they may assemble small credentials into large programs of study, assess the learning outcomes associated with courses and badges, help students assemble portfolios of competencies for students, and provide many other innovative services that leverage educational blockchain infrastructures. Moreover, traditional educational institutions may adapt rather than disappear; they could become as skilled as new providers at packaging credentials into blockchains or ledgers. In short, when it comes to educational innovation, blockchains and ledgers are likely to lead to evolutionary gains, rather than revolutionary reforms.

Acknowledgements

I thank **Eduworks** for its generous support on early drafts of this article, as well as Robby Robson, who was a source of educational technology ideas that helped shape this work.

Notes

1. "**Blockchains: The Great Chain of Being Sure about Things**," *The Economist*, October 31, 2015. ↩
2. "**The Promise of the Blockchain: The Trust Machine**," *The Economist*, October 31, 2015. ↩
3. Kenneth Rogoff, "**Crypto-Fool's Gold?**" *Project Syndicate*, October 9, 2017. ↩
4. Don Tapscott and Alex Tapscott, "**The Blockchain Revolution and Higher Education**," *EDUCAUSE Review*, March 13, 2017; and J. Philipp Schmidt, "**Credentials, Reputation, and the Blockchain**," *EDUCAUSE Review*, April 24, 2017. ↩
5. Chris Jagers, "**Why the Blockchain Will Revolutionize Academic Credentialing**," Learning Machine blog, *Medium*, October 29, 2016. ↩
6. Marnie Threapleton, "**Open Badges—A New Way to Recognise Expertise**," *Training Journal*, October 9, 2015. ↩

7. Donald Clark, "**10 Ways Blockchain Could Be Used in Education**," *OEB Insights*, September 12, 2016. ↩
8. Danny Ryan, "**Calculating Costs in Ethereum Contracts**," Hacker Noon blog, *Medium*, June 28, 2017. ↩
9. "**Permissioned Blockchains**," Monax. ↩
10. Juliana Nazaré, Kim Hamilton Duffy, and J. Philipp Schmidt, **What We Learned from Designing an Academic Certificates System on the Blockchain**, *Medium*, June 2, 2016. ↩
11. Tom Groenfeldt, "**Leading Banks in Using Ripple Blockchain Value Its Speed**," *Forbes*, November 1, 2017. ↩
12. "**Credential Transparency Initiative Debuts Groundbreaking Technology to Transform Credentialing Ecosystem**," *ANSI News and Publications*, September 19, 2016. ↩
13. MIT Media Lab Learning Initiative, "**Blockcerts—An Open Infrastructure for Academic Credentials on the Blockchain**," *Medium*, October 24, 2016. ↩

Dave McArthur is an educational technology consultant.

Badges and Credentialing, **Blockchain**, **Competency-based Education (CBE)**, **Data Security**, **Encryption**, **Openness**