Why IT Matters to Higher Education
EDUCAUSE REVIEW

Credentials, Reputation, and the Blockchain

J. Philipp Schmidt Monday, April 24, 2017 Editors' Pick

18 min read

Using the blockchain and strong cryptography permits creating certifications that put us in control of the full record of our achievements. Recipients can share a digital degree with an employer while providing trustworthy proof that the degree was in fact issued to the person presenting it. This raises interesting questions about the nature of recognizing and accrediting achievements.

The trail of credentials and achievements that we generate throughout our lives says something about who we are, and it can open doors that allow us to become who we want to be. Some credentials, such as university degrees, count more than others. But all of these

credentials represent experiences that are part of our lives, signals of our achievements, and markers of communities we belong to.

Our current, mostly analog system for managing credentials is slow, complicated, and relatively unreliable. Creating a digital infrastructure for certificates has many advantages, and new technologies like the **blockchain** offer exciting opportunities. The stakes are high, however, because such a system could grow to represent our professional reputations as well, creating or limiting opportunities. We need to be thoughtful about its design and the type of institutions we trust to govern it.

Digital Credential Systems

My interest in the field of digital credentials began in 2010, when I realized that outdated credential systems limited our ability to create new pathways to education, in particular for those who lacked access and needed it most. One challenge for people without formal education is to translate their learning into jobs because they often lack credentials affirming their skills and experience. Existing credential systems vastly favor formal education over other learning experiences, making it harder to develop valuable after-school and after-work education programs.

This focus on credentialing only formal education affects learners at all ages. Kids who build robots in after-school programs, for example, but struggle in their algebra classes, will end up with poor grades. And adults, who might participate in open-source software communities in their free time but never studied computer science at college, will have a harder time translating their experience into a job. Furthermore, as the pace of technological development quickens, the need for all of us to remain lifelong learners increases, and we need new ways to recognize and organize a broad range of achievements so that they can help us advance toward our goals.

Together with colleagues Erin Knight and Mark Surman at Mozilla, I co-authored a **white paper on open badges** (another name for credentials) that describes an alternative vision for digital credentials: a system that would be more inclusive and recognize a wider variety of accomplishments. The open badges specification provides a standard vocabulary to describe academic achievements, such as the name of the recipient and institution, the date a badge was issued, etc. But despite the success of open badges, broader adoption has been limited by two challenges: (1) the lack of convenient tools for learners to easily store and share their open badges, and (2) the failure of universities to see the benefits of transitioning their diplomas to open badges, leading to a focus on *lower-stakes* badges such certificates for after-school programs.

With the emergence of **blockchain** technology, the interest in digital academic credentials has made another jump. Blockchain, the underlying infrastructure used by cryptocurrencies such as Bitcoin, gives us new ways to share and verify credentials, potentially offering the pieces missing in the earlier open badges ecosystem.

The combination of open badges and blockchain enables digital credential systems that could prevent fraud, open up new insights into the way credentials are used, and offer new

mechanisms for communities to share knowledge. The first examples of such blockchain-based systems have recently moved from prototypes to commercial products. University registrars at institutions like MIT, UT Austin, and the University of Nicosia are considering issuing digital diplomas to their students this way. Refugee organizations are interested in providing them to learners who are moving from country to country and might not have the ability to carry paper certificates with them. And earlier this year, the **government of Malta** announced its intention to support the deployment of **blockcerts**, an open standard for digital credentials on the Bitcoin blockchain, which grew out of prototypes developed by my research group at the MIT Media Lab.

A Short History of Credentialing Systems

Humans have used credentials for their academic and other achievements for thousands of years. We can learn from the design of these systems, in order to articulate a set of core values and features that all credentialing systems should have, including those created with new digital technologies.

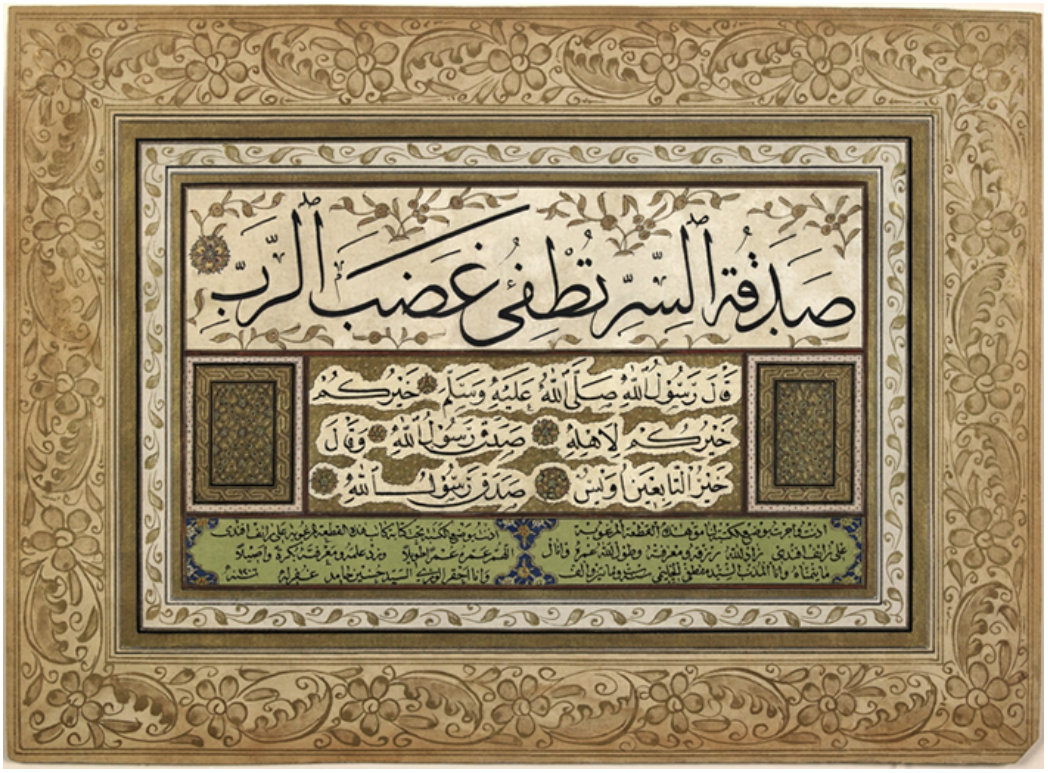
Ijâzah

Until very recently a quest for knowledge often required an actual quest — having to seek out, travel to, and spend time with the experts one wanted to learn and receive certification from. William A. Graham wrote about islamic religious scholars who, as early as the ninth century AD, would go on such a "journey in search of knowledge" in order to study the **hadîth** (reports of the life of the prophet Muhammed).[1]

To allow students to demonstrate to others what they had learned and from whom, they received a type of certificate called an *ijâzah*. Over time, these elaborate documents were used not just to recognize religious study but also for other forms of knowledge such as history, law, or philosophy. Once a teacher was satisfied with the student's mastery of a certain topic, he or she would issue an ijâzah as a form of license that would grant its holder permission to pass on the learned knowledge to others.

A unique characteristic of an ijâzah is that it typically describes not only the knowledge a student has gained but also the teacher's own "scholarly lineage of teachers."[2] Not only the journey of the student holding the ijâzah can be traced back, but also the historical path of the knowledge as described in the certificate itself. The ijâzah acts as a map of the journey the student has taken, and a license that allows the student to share it with others. It is a way to facilitate the spread of ideas and knowledge within a community of scholars.

Figure 1 shows an example of an ijâzah certifying competency in Arabic calligraphy. Written by 'Ali Ra'if Efendi in 1206 AH/1791 AD in thuluth and naskh script. From the **Wikipedia page**: "The top and middle panels contain a saying (Hadith) attributed to the Prophet Muhammad which reads: *Secret charity quenches the wrath of the Lord. / The best of you is the best for his family. / The best of the followers is Uways.*"



'Ali ra'if Efenda, Library of Congress; public domain
Figure 1. Ijâzah of competency in Arabic calligraphy (18th century)

Licentia Docendi — A License to Teach

The early European universities had no buildings or faculty. While there is an even older tradition of religious study, the concept of the medieval university emerged spontaneously from groups of young scholars who organized into guilds and hired tutors to advance their knowledge. Slowly these communities invented many of the structures and institutions that have shaped the university until today, including the diploma.

At some point during the 12th century AD, the medieval universities in Bologna and Paris started issuing a credential called a "licentia docendi" to its graduates. Literally a "license to teach," it represented a notion of knowledge transfer similar to the ijâzah. Crucially, at the time a number of **papal bulls** gave more autonomy to universities and established a system of recognizing licenses from one university in others, essentially formalizing a network of institutions for the spread of knowledge. Figure 2 shows an image of medieval instruction in philosophy, **via Wikimedia Commons**.

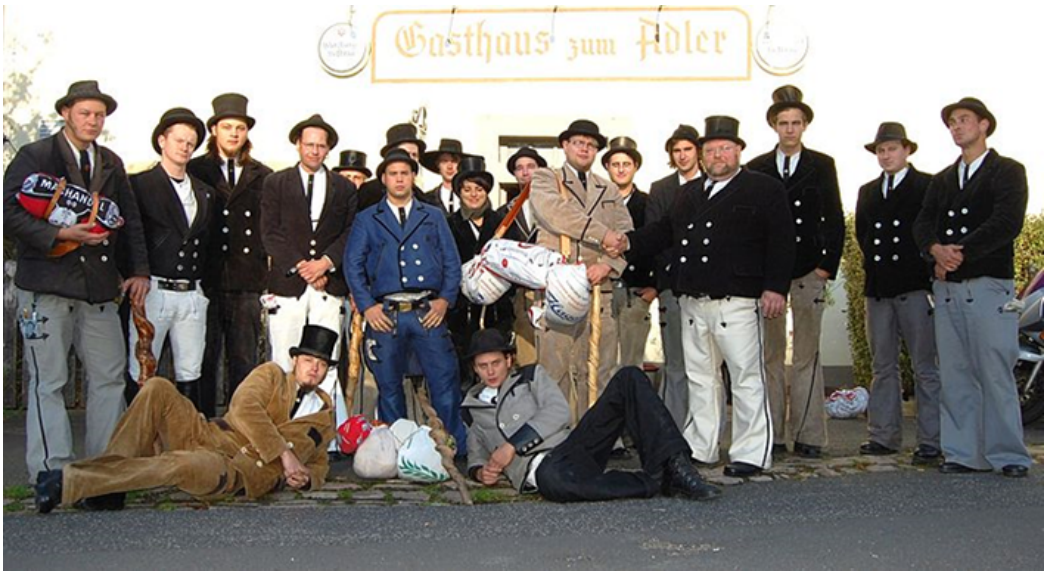
Cours de philosophie à Paris Grandes chroniques de France; public domain
Figure 2. Image of a medieval philosophy lesson

The licentia docendi not only marked individual accomplishment — the role we focus on today — they also acted as mechanisms to distribute knowledge in a consistent way over large distances and many generations. Aspects of the modern doctoral degree can be traced back to these early credentials in the same way that aspects of the modern research university can be traced back to the institutions of higher education that created them.

Journeyman Certificates

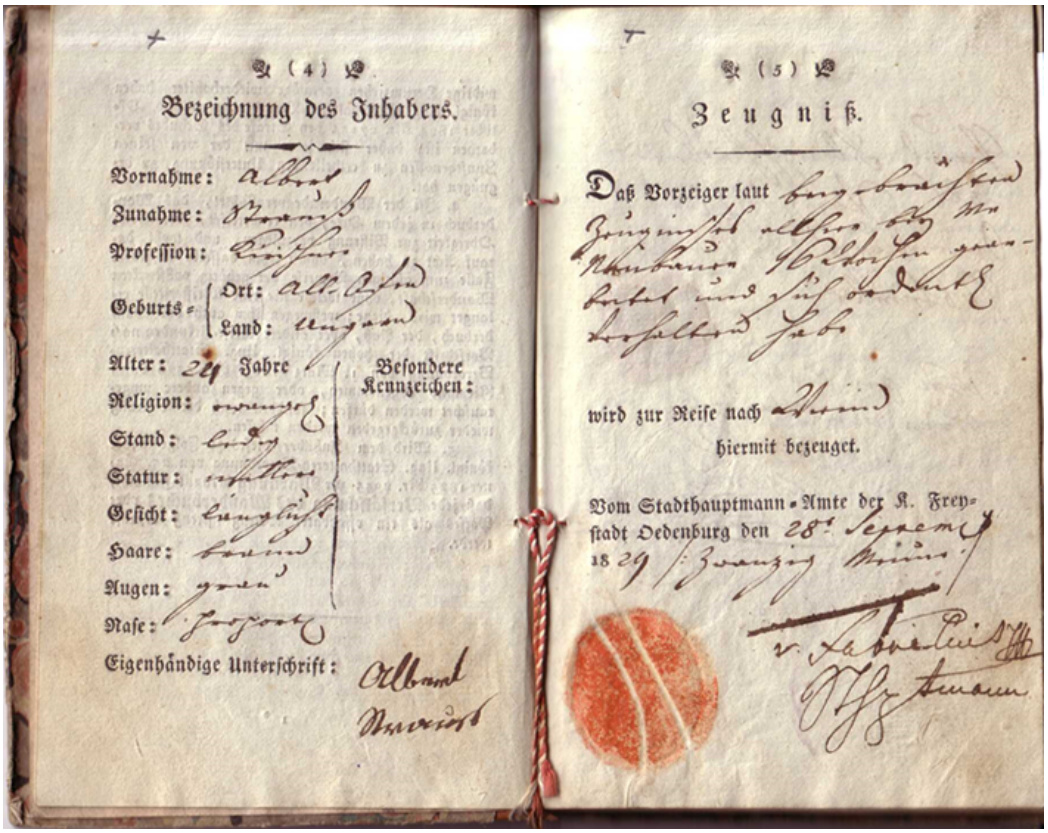
Credentials not only determine who can pass on knowledge, but they also help us identify members of a community who have certain skills. When we lived in small, tight-knit communities, people knew to whom they could turn when they needed an expert (and whom to avoid). However, as we started moving around and our lives and networks grew, we needed to come up with portable ways to signal our expertise to new acquaintances. Some of these original systems are still used today. For example, in some European countries carpenters can still do an apprenticeship tour that lasts no less than three years

and one day. They carry a small book, called a *Wanderbuch* (literally a "book of wandering"), in which they collect stamps and references from the master carpenters with whom they work along the way. The carpenter's traditional (and now hipster) outfit, the book of stamps they carry, and — if all goes well — the certificate of acceptance into the carpenters' guild are proof that here is a man or woman you can trust to build your house. See figure 3, **via Wikipedia Commons**.



Sigismund von Dobschütz, October 16, 2011; CC BY-SA 3.0
Figure 3. "Wandergeselle 02" by Sigismund von Dobschütz

The journeymen have a clearly defined process of learning and knowledge acquisition. They also have quality standards for their work. Both of these concepts are expressed through the credentials in the book they carry. When arriving in the next town, the Wanderbuch and what it says about its bearer is crucial for finding work. Credentials, in this example, act as a license to acquire and apply knowledge — to engage in an activity based on the learning already done and to engage in tasks that are appropriate given the book owner's existing experience. See figure 4, **via Wikimedia Commons**, which shows the traveling book of German-Hungarian furrier Albert Strauss, July 1816, pages 4 and 5.

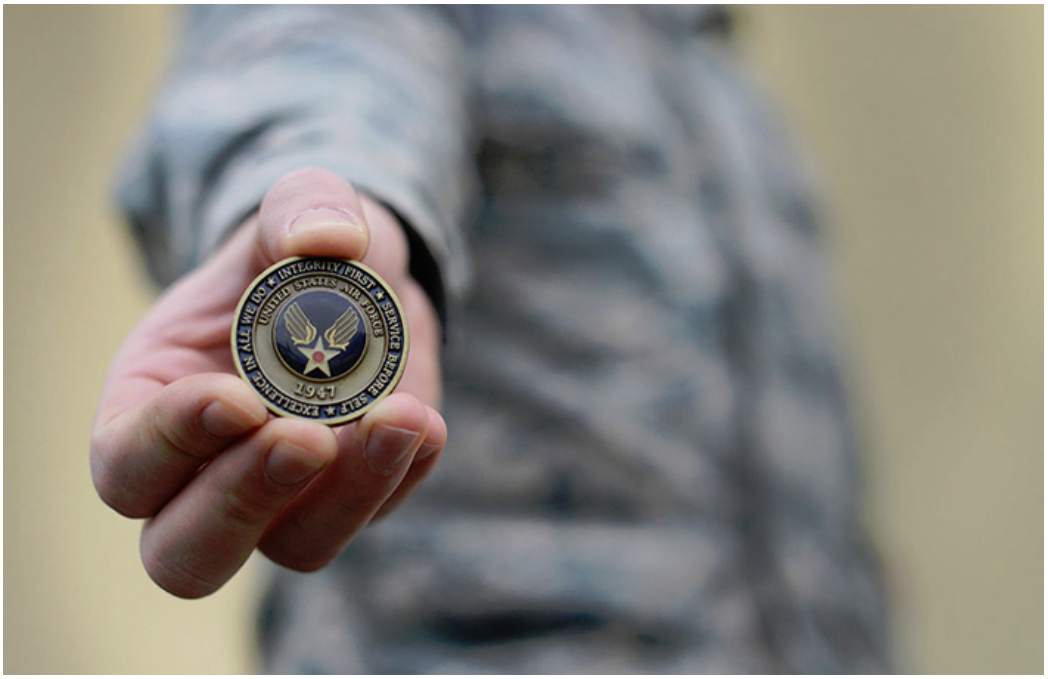


Freystadt Oedenburg im Königreiche Ungarn; public domain
Figure 4. "Wanderbuch" by Magistrate der Königl

Challenge Coins

Finally, while not technically the same type of credentials, challenge coins fascinate me, and I believe we can learn much from them for the design of modern systems of credentials. Originally created within the military, these coins had a number of different purposes, including as a form of authentication or a way to boost morale. By some accounts, coins were also used to delegate authority, allowing the holder of a coin to perform some action on behalf of the issuer of the coin.

Figure 5 shows an airman's coin as of March 25, 2015. The coin signifies the beginning of an enlisted USAF member's career when graduating basic training.



U.S. Air Force photo by Airman 1st Class Deana Heitzman; public domain
Figure 5. Airman's coin, 2015

Whatever their origins, challenge coins have been used in a number of interesting ways over time. They have served as tokens of gratitude that can be shared by soldiers across hierarchies but also with outsiders. While some challenge coins are issued by high-ranking officers and tightly controlled (the president of the United States has a challenge coin that is frequently handed out to family members of soldiers who died in the line of duty), most challenge coins are created through more of a grassroots initiative. A group of soldiers will get together and issue their own challenge coin, which they pay for and may even design themselves.

Challenge coins can also be used to confirm membership in a group. The name comes from the act of "challenging" someone to demonstrate that they are members of a certain group by producing the necessary coin. These challenges often involve drinking games, where soldiers who failed to carry their coin have to pay for a round of drinks.

Learning from the Past

Many of the lessons from these historical examples remain relevant, offering useful pointers for the design of new systems of credentials. For example, there are advantages for recipients in having more control over the certificates they earn, in the way the carpenters in Austria and Germany do. Their system allows them to carry their book of credentials with them, providing a verifiable history of their apprenticeship.

Giving recipients more control doesn't mean creating more opportunities for fraud. In the carpenter's book of references, for example, it is not possible to rip out a few pages without

anyone noticing. Being in control means having a way to store credentials, to carry them around, and to share them with an employer without having to pay or ask for the issuer's permission or cooperation. Individual control also enables a higher level of mobility, allowing credentials to travel with the individual.

Different credential systems deal with trust and verification in different ways. The early systems had limited ways to identify forged credentials. Elaborate designs of the ijâzah made forgery hard, but not impossible. The same is true for the stamps in journeymen books. By and large, credentials are just pieces of paper that carry value beyond the materials themselves (importantly, the same is true of paper money). While they may contain some intricate designs that make duplication hard, what makes them truly meaningful is the social construct of trust that we place in them.

Most traditional credentialing systems, such as university diplomas, offer some ways for verification by contacting the original issuer or third-party services, but (as anyone who has ever called a registrar's office to request a transcript knows) they are often cumbersome and not immune to fraud. Job seekers have to request official transcripts from their alma maters (and typically pay a small fee), while employers still need to call the university if they want to be sure that a transcript wasn't forged — and there is no way to know for sure.

An aspect of these historical credentials that I find particularly engrossing is the notion of delegating authority or giving agency to an individual to act on behalf of a community. In the same way as the ijâzah and the licentia docendi indicate who can pass on certain knowledge, I would like to see digital credential systems enabling new types of agency, where individuals or groups of individuals together can act on behalf of communities. I see this as part of a structured process to bring more people into a community.

Digital Systems

In two areas in particular digital systems surpass the practices evolved in non-digital systems and open up exciting new possibilities: (1) trust and verification and (2) data and insight.

New verification systems can be built on strong cryptography that makes it easy to detect if the content of a credential has been tampered with. Public/private key systems can be used to authenticate both the issuer and the student, and could make fraud virtually impossible. While this has some obvious advantages, it also comes with new risks. Do we really want an uneditable history of all of our achievements, or is there value in being able to curate and shape one's own trajectory?

Digital systems also allow us to store and analyze much more data about the use and value of credentials. We are starting to see the power of such data in projects like LinkedIn's university ranking, which took into account which degrees would lead to the most desirable jobs (all based on data from within LinkedIn).[3] The experiment produced some surprising results, but it was also short-lived, and LinkedIn has since removed it from its site — one of the hazards of privately owned data. The public has no way of demanding access, even though it contributed all of the individual data points used in the analysis.

An Open System for Digital Credentials

The key design questions when it comes to digital credential systems are centralization vs. decentralization, and open vs. closed. Centralized systems are often easier to architect and manage, but they also tend to create winner-takes-all scenarios, can stifle innovation (once a market has been captured), and limit diversity. Take the World Wide Web, for example. In the late 1980s and early '90s there was fierce competition among private companies vying to establish proprietary centralized standards for hyperlinked media content. But ultimately HTTP, the hypertext transfer protocol developed by Tim Berners-Lee at CERN, won out. The fact that the HTTP standard was open, and anyone could build applications on top of it without central control, has led to an incredible amount of creativity and innovation, enabling projects like Wikipedia, YouTube, Khan Academy, and Kickstarter.

A similar scenario is easy to imagine for credentials. In some ways, social networks such as LinkedIn or Facebook already control much of the data that make up our professional experiences and networks. I worry about storing our professional histories in closed corporate systems, which effectively end up "owning" the data, given that we may not be able to easily export the data and that network effects make it hard for new entrants to compete. Ultimately, storing our data in closed, centralized systems may limit the value we can derive from it, at the individual level, and the public benefit it could produce when analyzed in the aggregate.

I hope that we can establish a robust open standard for a decentralized system of digital credentials so that we will see a similar level of innovation and experimentation in the space of academic credentials as we have seen on the web. Furthermore, only an open standard allows individuals to remain fully in control of their own academic history. That is important because academic certificates are markers of our past lives and tickets to our future ones.

Blockchain-Based Decentralized Trust

Using the blockchain and strong cryptography, it is now possible to create a certification infrastructure that puts us in control of the full record of our achievements and accomplishments. It allows us to share a digital degree with an employer while giving the employer complete trust that the degree was in fact issued to the person presenting it.

This is exciting because it is not only a better way to deal with the way certificates work today, but it is also an opportunity to revisit some of our ideas about more inclusive and diverse credential systems from the open badges white paper. What was missing at the time was the technical infrastructure that would let us reliably store and manage these certificates. Enter the blockchain.

Blockchain technology is best known for its connection to the cryptocurrency Bitcoin. But a simple way to understand it is as a public ledger that allows anyone to record transactions. What makes it special is that it is durable, time-stamped, transparent, and decentralized. Those characteristics are equally useful for managing financial transactions as for a system

of reputation. In fact, you can think of reputation as a type of currency for social capital rather than financial capital.

The Basic Design: How It Works

A basic digital credentialing system should make it possible to verify who a certificate was issued to and by whom, and validate the content of the certificate. We developed a fairly simple implementation that uses the Bitcoin blockchain as a public notary, where we store a few pieces of information in an open (but secure) place so that anyone can verify the authenticity and integrity of the credentials this information refers to. The process follows:

- The basic information such as the name of the recipient, the name of the issuer, an issue date, and a few other fields is stored in a digital file, the credential, which is structured according to the IMS **open badges** standard. The file is cryptographically "signed" with a private key to which only the issuer has access, and the signature is appended to the credential itself.
- The cryptographic hash of the credential file, which is essentially a long string of letters and numbers that can be used to verify that nobody has tampered with the contents of the certificate is created and stored on the Bitcoin blockchain. There is exactly one possible combination of letters and numbers that corresponds to a digital file, and any change to the file would result in a different hash.
- The digital credentials themselves can be stored on a hard drive or in a mobile wallet, from where they can easily be shared with others, or even printed out on paper. The data needed to verify their integrity and authenticity is stored on the blockchain.
- In order to verify a credential, an employer (or a company offering verification services) will essentially follow the same process backwards to ensure that the hash corresponds to the original file and that the keys used by the issuer point back to the right institution.

Over the past few years Juliana Nazaré, a graduate student at the MIT Media Lab, and I have developed a number of prototypes of such a system, experimenting with credentials for the Media Lab Director's Fellows and for attendees at our 30th anniversary. Out of these early prototypes grew *blockcerts,* a set of open-source software tools and documentation that enables anyone to start issuing, sharing, and verifying digital credentials. In addition to the open-source tools, the first commercial implementations of the blockcerts standard have appeared, and universities like MIT will start experimenting with digital diplomas for some of their students later this year. Much of the **development of blockcerts** going forward is being driven by Learning Machine, an education technology company based in Cambridge, Massachusetts.

Future Directions

The first sets of blockchain-based credential systems, such as blockcerts, represent an important step toward an open digital credentialing ecosystem. They give us a foundation

and new tools to experiment with. We can now start building out larger implementations, and experimenting with blockchain-based credentials in different settings, and learn more about the best ways to manage and govern the evolution of open standards for digital credentials.

During the coming years, we will see additional features and capabilities added to these digital credential systems. In particular, I expect the development of better ways to store and protect personal data, allowing individuals to securely record the use of their credentials and more selectively share parts of their education history with others. And I believe we need to find a way to make verification of institutions easier, ensuring that a particular key actually refers to the institution it says it does. Such systems are ideally also built in open and decentralized ways (e.g. using a web-of-trust approach) in which verifiers share data with each other, and the system as a whole gets smarter and more reliable over time.

I also expect future systems to take advantage of some of the more powerful features that blockchain systems offer, namely the ability to construct the exchange of information as a series of verifiable transactions. In such scenarios, credentials are not fixed documents, but can act as smart contracts between issuers, learners, and employers. In the same way that we say a degree may "unlock" new opportunities, these digital credentials could actually unlock some new digital capabilities for the recipient.

In terms of the benefit to public education, I see two areas where digital credential systems could help drive positive change. One is the emergence of a much more diverse set of credentials that hold real value to the learners. I am hopeful that in the next few years, we will see new types of learning pathways that can be a viable alternative or strong complement to more traditional degrees, at lower cost. Two, I am excited about finding ways to aggregate data on the use of credentials while respecting the individual student's privacy. Such data will allow us to make better recommendations to students and employers, reducing the potential for dubious for-profit colleges to charge students money for degrees that won't help them find jobs.

As the first generation of decentralized digital credential systems starts to mature, much interesting work lies ahead. Seemingly minor technical design decision taken today can have far-reaching implications in the future. This is particularly true for standards, which are hard to change once they have been adopted by a number of partners and which always face the danger of noncompliant implementation, especially by organizations that have significant market power. Back in the 1990s, for example, Microsoft came late to the Internet and tried to wrest control over the emerging HTML standard by implementing additional optional features that were only available to users of its Internet Explorer software. A similar scenario is easy to imagine in education because the potential profit of controlling the standards is so great.

The most important work that lies ahead is not technical. Much has to do with institutions and governance. It will require a concerted effort to ensure that the standards for digital credentialing systems are open and that they take into account the needs of all involved — learners, educational institutions, employers, and governments — and don't prioritize the

interests of some organizations over others. This is the time to experiment, to collaborate, and to share experiences to realize the full potential of building a new ecosystem of digital credentials. For those interested in learning more, and potentially getting involved, good starting points are MIT's **Digital Currency Initiative**, the **blockcerts project community**, and the **W3C Verifiable Claims** task force.

Acknowledgments

A shorter version of this article was originally posted on the MIT Media Lab **blog**. I would like to thank Juliana Nazaré and Herman de Leeuw for their feedback and input to this article. They deserve credit for their thoughtful comments, while I retain responsibility for any errors or omissions.

Notes

1. William A. Graham, "**Traditionalism in Islam: An Essay in Interpretation**," *Journal of Interdisciplinary History*, Vol. 23, No. 3 (Winter 1993): 495–522.
2. Ibid.
3. Navneet Kupar, "**Ranking Universities Based on Career Outcomes**," LinkedIn Official Blog, October 1, 2014.

Philipp Schmidt (**ps1@media.mit.edu**) is director of Learning Innovation at the **MIT Media Lab**.

Badges and Credentialing, **Badges and Credentialing**