Chapter 9

Digital credentials: Discussions on fluency, data privacy and the recognition of learning in higher education beyond COVID-19[9]

Barbara Dale-Jones[a,b]
[a]The Field Institute, Cape Town, South Africa
[b]PASCAL International Observatory (Africa)/
Centre for Local Economic Development (CENLED),
School of Economics, College of Business and Economics,
University of Johannesburg,
Johannesburg, South Africa

[9] The authors of this chapter were invited to participate as 'guest authors' with PASCAL/ CENLED, for the project on 'Learning for a better future: Perspectives on higher education, cities, business & civil society'.

How to cite: Dale-Jones, B. & Keevy, J., 2021, 'Digital credentials: Discussions on fluency, data privacy and the recognition of learning in higher education beyond COVID-19', in M. Venter & S. Hattingh (eds.), *Learning for a Better Future: Perspectives on Higher Education, Cities, Business & Civil Society* (Centre for Local Economic Development: Topics in Local Development Volume 1), pp. 193–209, AOSIS, Cape Town. https://doi.org/10.4102/aosis.2021.BK214.09

James Keevy[a,b]
[a]JET Education Services,
Johannesburg, South Africa
[b]PASCAL International Observatory (Africa)/
Centre for Local Economic Development (CENLED),
School of Economics, College of Business and Economics,
University of Johannesburg,
Johannesburg, South Africa

Abstract

Credentials have historically been thought of as tangible documents such as a driver's licence, a passport or a birth certificate. In the educational sector, a credential can be something like a degree certificate or a school leaving certificate. It is customary in contemporary society that an individual proves his/her identity or achievements by sharing a credential in one way or another. The advent of COVID-19, and in fact even many new developments during the months preceding the pandemic, has starkly illustrated that digital credentials are not only useful but also necessary for global citizenship and mobility (Dale-Jones et al. 2020). Together with this accelerated trend towards digitalisation, there is an increased risk of the potential abuse of data and information under the guise of the pandemic and more broadly, for non-altruistic purposes (Motsepe et al. 2020). This chapter draws on research into these areas, completed in May 2020, as well as research that has been underway in South Africa since 2018 to develop a national digital ecosystem for the post-schooling sector (Rajab et al. 2020; Shiohira & Dale-Jones 2019) in order to build a case for the responsible use of digital credentials for the recognition of learning beyond the COVID-19 pandemic. The chapter specifically positions the concept of self-sovereign identity as a key consideration for the education sector in the new digital age.

Introduction

The chapter explores the benefits of replacing the current higher education credentialing system in which external entities issue credentials to individuals to confirm identity, status and achievements through documents with digital credentials. In the educational setting, credentials are generally in the form of a degree certificate or a school leaving certificate. This chapter illustrates the benefits of the utilisation of self-sovereign identity in the recognition of learning in broader education and training contexts throughout the student life cycle, and specifically in higher education, for a seamless and frictionless user experience. Educational credentialing can change the nature of the relationship between individuals and their educational data. The decentralisation of educational data through digital identities will enable students and others to control their identity records and data related to their education, training, assessments and skills, and provide this data for verification and transactions without the need to rely on institutions or a central repository of data.

The advent of COVID-19 together with many other new developments during the months preceding the pandemic have starkly illustrated the fact that digital credentials are not only useful but also necessary for global citizenship and mobility (Dale-Jones et al. 2020). Concomitant with this accelerated trend towards digitalisation, there is an increased risk of the potential abuse of data and information under the guise of the pandemic and more broadly, for non-altruistic purposes (Motsepe et al. 2020).

This chapter draws on research into these areas, completed in May 2020, as well as research that has been underway in South Africa since 2018 to develop a national digital ecosystem for the post-schooling sector (Rajab et al. 2020; Shiohira & Dale-Jones 2019) in order to build a case for the responsible use of digital credentials for the recognition of learning beyond the COVID-19 pandemic. The chapter specifically positions the concept of self-sovereign identity as a key consideration for the higher education sector in the new digital age.

The emergence of digital credentials

The body of work on digital credentials has been expanding at a pace over the last few years (Commonwealth of Learning [COL]

2019; Keevy & Chakroun 2018; Oliver 2019). The landscape is very dynamic, even described as a ‘wild west’ (Jirgensons & Kapenieks 2018), as the lack of clarity over standards, governance and administration processes (COL 2019) has created a vacuum wherein outlier organisations such as Mozilla and others are playing an important role. There is also an increased trend in South Africa where both public and private education institutions are starting to explore this new modality. PrivySeal, a local technology company working with both the South African Qualifications Authority (SAQA) and the South African Council for Educators, is a good example. Although many of these institutions have been involved with the massive open online courses and the open learning movement over the last two or more decades, the emergence of more dynamic and agile digital credentialing schema is still foreign to most. Quality assurance bodies are also grappling with validating what seems to be a moving target.

The intrinsic digital nature of this new form of credentialing is both a strength and weakness and, like the COVID-19 pandemic, also presents both a threat and an opportunity to South Africa and the wider global community. The new digital credentials are designed to be associated with extensive sets of metadata, making it possible to utilise big data techniques in new and incredibly sophisticated ways (Gloss et al. 2014). This presents a chance to link work opportunities with appropriately-skilled individuals, and many such examples are already being piloted internationally (Rampelt, Orr & Knoth 2019). One would imagine that with increasing unemployment because of the debilitating impact of COVID-19, such a ‘line of sight’ from job vacancies to available skills would be in even higher demand than before. The commensurate threat of this new form of credentialing also lies in its digital nature. The ability to regulate, quality assure or even just map a wave of smaller just-in-time pockets of learning that lie outside the traditional structures is simply not possible with the current credentialing system and thus opens the door for the exploitation of the public and, as is often the case, the more vulnerable sectors of society. The inevitable limited impact of traditional quality assurance regimes to new ‘qualifications’ with an inherent digital nature, can lead to inferior and low-quality courses being offered with very few key signals available to the unassuming learner. Certainly not the signals they are used to, such as government endorsement or quality assurer’s registration number. More progressive authorities across the globe, such as in New Zealand, Malta and the United States, have started to deal systematically with these risks, but there is still much to do, with the majority of countries at an early stage of managing the process.

In order to make some sense of this new constellation of credentials and the opportunities and threats it introduces, as noted above, it is useful to turn to a few contemporary ways in which the broader credentialing ecosystem in training is in some way, trying to self-correct. This rebalancing of the fluency equation between vacant jobs and available skills is inevitable and can be done in an organised and governed manner or be left to simply happen in an organic way. Taking a leaf from the last few decades of development in digital platforms such as Pymetrics, Skills Lab (managed by the European Training Foundation), Credential Engine, Mozilla and many others, a more organic model, even machine learning-based, would be better suited to the digital context, while a more structured, non-digital approach may be preferred by the humans involved. In this increasingly complex and data rich ecosystem, it is inevitable that the former will outlast the latter. Two examples are provided further to illustrate this. The first is rooted in an emerging digital architecture, while the second is a more human response to try and develop common metrics for learning, in this case, on a global scale.

The first example is the notion of interoperability. Two main types of interoperability are found in the literature: (1) syntactic interoperability, which is ‘the ability of multiple systems to communicate and exchange data, regardless of whether or not they have shared programming languages or use interfaces’; and (2) semantic interoperability, which is (Shiohira & Dale-Jones 2019):

> [*T*]he ability of discrete systems to understand and make meaningful use of shared resources by using common interpretations of data and services and common identifiers for individuals as well as for institutions. (p. 23)

In order to make sense of interoperability, a range of frameworks are being developed such as the data commons framework and the statistical information system collaboration community. Examples include the World Wide Web Consortium and the well-known International Organization for Standardization, as well as open standards, such as the Open Geospatial Consortium, Statistical Data and Metadata eXchange and .Stat. Shiohira and Dale-Jones (2019) provide a useful overview of these various elements of interoperability, including the potential benefits to the mobility and portability of student data. An important related concept is data ownership and the differences between centralised and decentralised ecosystems. This will be discussed later in the chapter.

The second example is an international response to try and evolve more traditional normative instruments, such as the various regional UNESCO conventions, into a global convention on the recognition of qualifications concerning higher education (UNESCO 2019). The new global convention finds its alliances in the development of national and regional qualifications frameworks, most recently the move towards an African Continental Qualifications Framework (African Union Commission 2019). This example represents the intent to establish more independent global metrics within which learning can be recognised and made more transparent and portable across countries, regions and even continents. Encouragingly, there are signs of a new fourth generation of qualifications frameworks emerging. The beta version of the American Credential Framework (Keevy et al. 2019) is a key example that warrants greater exposure and review.

So where is this leading us? On the one hand, the emergence of interoperable systems and platforms is evident and, on the other, there is new thinking related to global metrics to recognise learning.

Common to these juxtaposed examples lies the notion of the locus of control of data. New thinking, such as the emergence of interoperable systems and platforms, suggests that the individual is at the centre of data ownership; new forms of legislation and increased data privacy measures across the world bear testimony to this. Historically, data belong to the education and training provider, the quality assurance body or even the relevant government department. Traditional systems such as qualifications frameworks and even conventions are more akin to older forms of data control, while interoperable systems lean towards decentralised forms of control and individual data ownership, as mentioned earlier.

In this time of COVID-19, the acceleration of technological solutions (Foster et al. 2020) is evident. This chapter argues that digital credentials present a real opportunity to rethink the recognition of learning beyond the COVID-19 pandemic. While the new approaches exemplified in digital interoperable systems and the growing response represented in recast normative instruments are not mutually exclusive, neither engages sufficiently with the foundational principle of data privacy. The next section introduces the concept of self-sovereign identity as a key consideration for the education sector for the digital age that lies ahead.

■ Self-sovereign identity

Currently, it is generally the case that third-party records over which we have no control prove who we are and what we own. This is a centralised identity model where a single authority has control over our data and where credentials like ID numbers or an Instagram login are issued to users by a third party. The model can be infuriating for the user, who has to remember all the username and password details for a wide range of different credentials, and where password reuse is consequently widespread. A report by Amber Gott (2017) claims that, on average, business employees make use of 191 passwords. This also undermines the security of credentials and makes them more vulnerable to phishing and other fraudulent activities. Similarly, as with third-party records, data tend not to be portable but rather part of a larger dataset which is centrally owned (and sometimes abused or breached) by large corporations, such as the notorious recent case of Facebook and Cambridge Analytica.

The principle of self-sovereign identity is that control over identity data shifts away from central authorities to the individual in a move to a peer-to-peer data exchange where no one party controls the relationship with the other (Preukschat & Reed 2019). Self-sovereign identity is, in other words, a form of decentralised identity management (Allen 2016):

> Self-sovereign identity is the next step beyond user-centric identity and that means it begins at the same place: the user must be central to the administration of identity. That requires not just the interoperability of a user's identity across multiple locations, with the user's consent, but also true user control of that digital identity, creating user autonomy. (n.p.)

The principles of self-sovereign identity are that users must be able to not only access their identity data but also have agency with respect to their identities, which must be interoperable, widely available and global. Users' rights must be protected, and users must permit the use of their identity data. Another important principle is that systems and algorithms that host these data must be transparent and allow an identity to persist over time, whatever happens to the entity that first issued it (Allen 2016).

The question of what kind of technology is used to store data has had a significant and far-reaching influence on the development of such a decentralised model of data ownership (Dale-Jones et al. 2020). New models of data storage have developed in recent years and continue to emerge, whereby data are stored in decentralised systems without a central point that can control access and use. The blockchain specifically provides the technology platform needed to allow for a new model that has no need for a central authority. Blockchain technology and other decentralised network technologies provide a strong solution for exchanging public keys directly. These form secure, private connections between any two peers and also store public keys on public blockchains in order to verify the signatures on digital identity credentials (also known as verifiable credentials) that peers can exchange to provide proof of their real-world identity (Preukschat & Reed 2019).

Self-sovereign identity is therefore made possible by technologies like cryptography, distributed ledgers and the decentralised blockchain, and thus the principles and the technologies of self-sovereign identity are closely interlinked and mirror each other. The verification of data occurs cryptographically, typically through the use of distributed ledgers. Because of this and because credentials can be verified and accessed whether or not the issuing organisation is operating at the time that verification occurs, self-sovereign identity gives individuals access to their own data at any time and the capacity to control who can access their record(s) and when (US Chamber of Commerce Foundation & T3 Innovation Network 2020).

How does self-sovereign identity work? The chapter does not cover the technical details of how self-sovereign identity operates, but explores the philosophy, approach and benefits of self-sovereign identity. Credentials, like an individual's passport, bank cards or medical records, are typically paper or plastic documents that are issued by a central authority such as the Department of Home Affairs, a bank or a doctor's rooms respectively. While the veracity of these credentials depends on that authority's verification of those credentials, what self-sovereign identity offers is the opportunity for individuals to have digital equivalents of these credentials that are private, secure and verifiable and over which the individual has control and agency. Each digital credential has a data or digital watermark that enables the trust between the parties in the data exchange. The watermark is enabled by cryptography and allows for the successful issuing, holding and verifying of the credential in a way that is significantly more secure than traditional physical credential issuing. The digital watermark confirms firstly, who issued that data, secondly, when the data were issued and thirdly, that the data have not been tampered with.

Self-sovereign identity will not replace the Department of Home Affairs, for example, nor will it even replace the passport itself. Instead, self-sovereign identity provides a digital version of a credential, similar to a passport, which improves the user experience, increases privacy and security and reduces the burden of administration as well as the risk of phishing or fraud. Self-sovereign identity is, in other words, an improved digital version of a physical credential. It proves who (or what) issued the credential; to whom (or what) it was issued; whether it has been altered since it was issued; and whether it has been revoked by the issuer. Self-sovereign identity also sees the locus of ownership and control shift away from the central authority (the Department of Home Affairs, for example) to the individual user. With self-sovereign identity, no one person or thing is able to withhold an individual's access to his or her own data and the individual is able to choose what he or she shares with others.

Self-sovereign identity may seem radical but given the value of data and the dangers of allowing centralised organisations and systems to control and monetise data, it may ultimately be desirable to allow citizens not only to have agency in respect of their own data but also to control every aspect of their data. The situation in the COVID-19 pandemic is instructive in this regard. Extensive contact tracing to establish where points of contact have occurred between people is now being carried out by governments. While this is evidently appropriate for the gathering of public health data during a pandemic, the real risk exists that this data will be misused. Allowing citizens to have full ownership of their personal data through distributed and decentralised networks offers a solution for the protection of individual privacy. Consequently, there are self-sovereign identity initiatives emerging which aim to gather data safely during the pandemic. An example of this is the COVID-19 credentials initiative, which at the time of writing is a global community of over 300 individuals from more than 100 organisations. These individuals and organisations are undertaking verifiable credential projects to help contain the spread of COVID-19 (see Linux Foundation Public Health [LFPH] 2020). The projects aim to ensure that data privacy is ensured.

Recognising learning beyond COVID-19

There is a strong case to be made for the utilisation of self-sovereign identity in the recognition of learning in broader education and training contexts. At one level, institutions of learning and workplaces issue student identity cards, course results, transcripts and qualifications, to name a few. This can be an expensive and administratively burdensome exercise for institutions, more so when work-integrated learning merges with more formal training programmes and is offered in more agile and accessible packages. For students, gaining access to educational credentials can be time-consuming and expensive. The processes students need to follow are mostly highly administrative on a local level and increasingly obtuse when attempting to secure formal comparability across countries and regions. The work of the National Academic Recognition Information Centres[10] network has been helpful in opening some of these debates, as has the Groningen Declaration Network,[11] but there is still a long way to go, and technology is advancing at a pace that the system cannot manage. COVID-19 has shown us that this pace of development will most likely accelerate even more in the coming months and years.

This chapter argues that self-sovereign identity provides an alternative. It offers flexibility to education institutions by providing them with the ability to issue students with digital credentials that

[10] See https://www.enic-naric.net.

[11] See https://www.groningendeclaration.org/.

allow the end user, the student, to prove their educational achievements anywhere, to anyone, at any time. These credentials can help students to gain access to other institutions of learning, to demonstrate their qualifications and experience and, ultimately, to secure a job. Self-sovereign identity gives students direct access to and agency regarding the management of these credentials while ensuring that data are not only verifiable, but also private. Self-sovereign identity also allows students to prove who they are, to interact securely and to share their educational credentials with anyone or any institution at any time, thus enabling not only the mobility and portability of learning but also lifelong learning.

Self-sovereign identity represents a paradigm shift in how digital identity is handled and its benefits apply equally to individuals, HEIs, companies and communities, but its uptake and success will only be realised when key stakeholders like governments and businesses start to accept each other's credentials (Preukschat & Reed 2019). It is understandable that there will be opposition to self-sovereign identity. Shifting the power balance to the student will be a complex and multi-faceted process and, in all likelihood, will only really happen organically. The vested interests of the broader education architecture, including providers, national authorities and even international agencies, are considerable, and there is much to lose by surrendering the power of the control over vast data lakes. The authors argue that, once the power issue is at least taken account of, self-sovereign identity can be used to support and digitise the whole educational ecosystem, including the work of educational institutions in areas of registration and authentication, the issuing of results transcripts and qualifications and, critically, linking the student to the world of work. Some examples relating to both students and institutions are described further.

■ Linking students to the world of work

Self-sovereign identity is ideal for a frictionless post-qualification experience – allowing students to move seamlessly into the job market with the necessary proof of their achievements. Significantly, self-sovereign identity also allows for better matching of labour demand with skills supply. As such, self-sovereign identity can facilitate reciprocal relationships between education and labour. This may enable the education system to provide training on appropriate workplace-relevant skills based on a clear and current understanding of labour market needs. Self-sovereign identity provides students with digitally-enabled credentials that can be utilised to apply for jobs and be sent to prospective employers. This enables students to take control over their transcripts (which would reduce the paperwork as well as the administration burden on institutions) and to have them as verifiable evidence of their achievements.

Self-sovereign identity can enable matching between two ecosystems, with education on the supply side and labour on the demand side. Labour can publicise its requirements for certain types of skills, and education can respond in an immediate way. This would ensure that the education system is preparing appropriate skills for the workplace and would also allow for a clear and current view of oversupply or a low demand. These benefits would enable educational institutions and systems to reduce costs while increasing efficiency and security. For students, greater privacy and security is a key benefit, along with a preferable user experience. However, this presupposes an educational ecosystem that is sufficiently agile and non-bureaucratic, so as to be responsive to changing and newly emerging skills needs.

Registration and authentication

Self-sovereign identity for student registration

The self-sovereign identity benefit in education spans the student life cycle, but one of the most compelling uses is when students are registered and authorised. Here, self-sovereign identity allows for greater efficiency and reliability, and for the cost of identity verification in the process to be reduced for both the user and institution. Universities and other institutions of learning require students to prove who they are before they can enrol and register for an academic year. This requires students to have physical proof of their identities and either use a university system to register or physically go to the campus. This process costs money and time for both the student and the institution. Digital identities allow students to be verified and enrolled or registered from a distance, using the credentials of their personal digital identity document. It also allows them to seamlessly log into university systems and access other campus services in a safer and more secure manner. Importantly, this leaves an audit trail. Students know what information has been requested and why. The eradication of usernames and passwords will provide improvements across the student life cycle and make for a seamless and frictionless user experience.

Self-sovereign identity for issuing of results transcripts and qualifications

Self-sovereign identity allows for the storage of academic records and issuing of certificates. Through innovations in blockchain technology, many kinds of digital verification and credentialing can be streamlined, removing the need for complicated and expensive processes. There are also growing solutions available to those students without access to smart phones or devices. Self-sovereign identity allows educational institutions to secure, share and verify their learning achievements. The blockchain can provide a certification database which keeps a list of issuers and receivers of each certificate, accessible anywhere, on any computer. Importantly, the certificate cannot be forged.

Besides the problem of fraud, another problem HEIs and students/alumni face is that paper or physical credentials can get lost or damaged. Higher education institutions have to reprint degrees and diplomas every year, which is costly for students as well as institutions. Issuing a digital version of a degree or diploma will empower students, providing them with control and autonomy over their own credentials. Furthermore, micro-credentials can be issued for access to extracurricular activities, the completion of assignments or to prove class attendance.

Academic credential fraud is currently a thriving business. As mentioned earlier, the use of self-sovereign identity and digital identities can drastically reduce fraud. This will help potential employers to be confident in their decision to appoint a new staff member. Students can instantly apply for jobs and save time and money, while employers can save costs and time with the recruitment and human resource processes. Companies will be able to request information from applicants, and applicants will be able to download the necessary data and determine with whom it is shared. In other words, through self-sovereign identity, students will be able access and share genuine qualifications and credentials.

The challenges of self-sovereign identity

There are inevitably not insignificant challenges to self-sovereign identity, such as the time and cost of the personal responsibility for data security, as well as the complexity of individuals deciding who and what should have access to their data. However, these issues can be minimised and addressed by identity solutions. In addition, uneven access to the internet and appropriate computer technology, especially in rural communities and HEIs outside the major cities, will be an obstacle to the widespread use of self-sovereign identity. However, as these obstacles are addressed and mitigated, all students and HEIs will gain the benefits from migrating from the current system to self-sovereign identity.

Conclusion and recommendations

The interest in and relevance of portable, verifiable and interoperable credentials has increased as a result of COVID-19.

Linked to this, the emergence of immunity credentials along with processes like contact tracing has meant that the issue of data rights and privacy is of increasing importance. If the issue of data privacy is not addressed urgently, the control over who owns and uses a person's data could be entirely eroded. The opportunity exists for educational credentialing to change the nature of the relationship between individuals and their educational data. If educational data are decentralised, individuals with digital identities will be able to control their identity records, including data related to their education, training, skills, projects, job history, assessments and more. They will also be able to provide this data for verification and transactions without the need to rely on institutions or a central repository of data. Individual citizens will be able to turn their skills, training and experience into genuine value in the labour market and access better career and development opportunities.

Self-sovereign identity allows students to prove who they are, to interact securely and to share their educational credentials with anyone or any institution at any time, thus enabling the mobility and portability of learning. For the first time, since the concept of lifelong learning was first mooted in a UNESCO report (Faure et al. 1972), the technology is now available to realise this vision of a seamless learning environment, wherein all learning matters, albeit formal, informal or non-formal.

The notion of self-sovereign identity and the shift in the locus of control to the individual is not a straightforward matter and will not be uncontested. For it to be successfully deployed in the education system, it requires HEIs, quality assurance bodies, governments and businesses alike to recognise and accept each other's credentials. Its success will also require political will. Many local and international researchers and policymakers are exploring issues covered in this chapter. COVID-19 has been a wakeup call in many ways to a global community that was starting to explore these new ideas, which for many were simply futuristic and unlikely to materialise. The landscape has shifted in a short space of time and it is foreseen that digital credentials will become more mainstream in the coming months and years. With this shift, the responsible use of these new ways for the recognition of learning both in higher education and across the education landscape needs to be carefully considered. Credential fluency and data privacy are explicit components of this process. Self-sovereign identity is the implicit side of the same (bit)coin.