RESEARCHERS BOOTCAMP

#OPENUPYOURTHINKING

READY, SET, THINK!

Education Researchers Respond to The COVID-19 Pandemic RESEARCH REPORT

Theme 7:
Putting the individual at the centre: The role of digital identity during the time of COVID-19

Project Lead: Barbara Dale-Jones

5 May 2020

JET EDUCATION SERVICES

Contents

Introduction

Background

The COVID-19 pandemic has changed the way all of us interact and operate. Social distancing and lockdown policies have led to the increased adoption of remote working and online education, with the use of digital platforms being necessary for people to stay connected and productive. In education, teachers and lecturers are increasingly using digital means to communicate, provide lessons and activities, teach remotely and give support to learners and their parents and caregivers.

While technology allows for interactions and activities to continue during lockdown, online exchanges bring with them the risk of data privacy being breached. As it is, during the time of the COVID-19 pandemic, basic freedoms have been restricted around the world as government authorities have increased their monitoring of citizens while they take up arms against the virus.

There seems to be evidence that mass contact tracing and testing is effective in managing what is a worldwide pandemic and widespread surveillance, location tracking and restrictions on movement are now commonplace. However, this approach is not without risks and ethical complexities. It is not unforeseeable that personal information of the type being collected could be used in ways other than for public health benefits and not only by governments, but also by private companies. The possible outcomes of this prospect are alarming. Formal, provable trust is required to counterbalance the move towards mass surveillance during the pandemic, and current technology makes it possible. As Bill Gates has observed, we will have “digital certificates to show who has recovered or been tested recently or when we have a vaccine who has received it” (Reuters Fact Check Team, 2020) instead of the current protocols for data collection, which seriously compromise individual privacy.

Self-sovereign identity (SSI) offers a solution. It is an alternative way of confirming who has been tested and his or her status in respect of the virus. When a vaccine arrives, SSI will allow those who are vaccinated to be verified quickly, and without compromising unnecessary personal information. This research report examines the viability of SSI.

Who should own our data?

Before turning to the body of this research report, the issue of data ownership needs to be addressed. Who owns our data is an increasingly contested question in the modern age – think of Facebook, Cambridge Analytica, Amazon and Google. In 2020, who should own our data? And, in the extraordinary and unprecedented global pandemic of COVID-19 with governments overtly controlling the rights and choices of individuals as described above, the sovereignty of our data and our rights to it are being increasingly eroded, especially as governments battle to balance individual rights to privacy and national security. Being monitored and tracked is alarming, but giving individuals ownership of and control over their data is not without complexity or risk either.

- Should individuals be given ownership of and control over their data in general?

- Should individuals be given ownership of and control over their data during a pandemic?
- What are the pros and cons of allowing individuals to own and control their data during a national or global crisis?
- Is it possible and/or advisable to have a digital ecosystem that is open and decentralised?

These are the fundamental concerns that underpin this research report.

Purpose of the study

The purpose of this project has been to identify and understand examples of the use of self-sovereign identity (SSI) in education internationally, and to identify instances in which data ownership and control have been successfully decentralised. The specific research questions were:

1. What is SSI?
2. What is the value of SSI for education?
3. Where is SSI being used in the education system, both locally and abroad?
4. How can SSI address the problems inherent in the collection of data with the mass surveillance and contact tracing measures being used during the COVID-19 pandemic?
5. What can the education system learn from the way SSI has been used during the COVID-19 pandemic?

Method

The research comprised the following steps:

1. Each member of the workstream undertook to carry out desktop research on an example of SSI that had been shared with them.
2. Each member of the workstream undertook to look for another example of SSI currently in use in education and to write it up.
3. Based on the problem statement articulated in the summary of emerging insights from the bootcamp – namely, "there is a risk that the data privacy of learners, teachers, lecturers and parents could be abused by the government in the name of managing the pandemic" – the third piece of research was to explain how SSI could be used in mitigation of this risk, what benefits SSI would bring to managing this pandemic, and what use cases we could learn from during this crisis.
4. The final piece of thinking and writing required researchers to imagine they were preparing a recommendation to the South African ministers of Basic Education and Higher Education and Training. They had to explain: (1) what SSI is, and what issues it solves; (2) what the value of SSI in

education would be, and what benefits it could bring to South African education specifically; (3) what the risks of not using SSI are; and (4) what we can learn from the way SSI has been used during the COVID-19 pandemic and what these learnings could mean for education.

Findings

Self-sovereign identity: A definition and description

Self-sovereign identity (or SSI) is a revolutionary way of thinking about personal data. It is a model of data storage and management that places security, empowerment and innovation at the heart of digital life. This technology, and way of thinking, is available now, and could improve current systems of data management significantly (Solid, Undated; Preukschat, 2018).

SSI is a concept that makes it possible for individuals to have control over their digital credentials. Examples of credentials include an individual's passport, degrees, bank cards and medical records. These are issued by a central authority such as the Department of Home Affairs or a bank, and depend on that authority's verification. SSI sees the locus of ownership and control shift away from such authorities. With SSI, an individual knows what data is collected about him or her, what it is used for and who has accessed it. SSI has gained favour as a user-centric approach for managing identity because it gives individuals the power to own, create and control their own data (Toth & Anderson-Priddy, 2019). While we usually think of our identity in terms of official attributes given to us by the government (such as our ID number, passport or driving licence numbers), social and biometric attributes are also important keys to the whole picture of our identities. Our digital identities also encompass intrinsic biometric features such as our fingerprints, how we look or our voice patterns, and also social attributes such as our family and circle of friends, hobbies and preferences (Lyons, Courcelas & Timsit, 2019).

SSI has been described as the next step in a user-centric identity approach where the onus of responsibility to administer data is on the individual (Der, Jähnichen & Sürmeli, 2017). With SSI, not only are individuals able to control their digital identities, but they also have the freedom to choose which data is associated with their identity, for example, social media accounts, verifiable credentials like an ID or phone number, or even confirmations from friends (Lyons et al., 2019).

Credentials have historically been thought of as tangible documents, such as a driver's licence, a passport or a birth certificate. In an educational setting, a credential can be something like a degree certificate or a school leaving certificate. Individuals need to prove their identity or achievements by sharing a credential. For example, they would share their ID book when they apply for a loan, or share their passport when they travel overseas.

Until recently, credentials have been paper-based, and have had features such as watermarks that help to verify them. Sometimes they have to be verified by a third-party, such as a commissioner of oaths. We all have a myriad of credentials – not only passports and an ID, but also bank cards, store cards, student cards, and so on. Many of these require a username and a password.

Easy access to the digital equivalents of physical credentials has been more elusive, even though it would be ideal to have access to these credentials digitally and carry them on a phone and access them seamlessly

online. SSI provides a digital and verifiable credentialing system that gives each credential its own digital watermark and confirms (1) who issued that data, (2) when the data was issued and (3) that the data has not been tampered with. This allows for a frictionless user experience without compromising security. It gives the user the power to create more than one digital identity, where the types of data associated with an identity can be specific to the context, for example an identity for a healthcare provider, one for professional networks and another one for social media (Lyons et al., 2019).

The question of what kind of technology we use to store our data has far-reaching implications for the questions of who owns our data and who has control over it. New models of data storage are emerging, where data is stored in decentralised systems without a central point that can control access and use. 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. In this scenario, citizens would have full ownership of their personal data through distributed and decentralised networks such as the blockchain, which offers a solution for the protection of individual privacy. As SSI is premised on a notion that the owner of the data should control his or her own data, it removes the need for a central authority and instead operates effectively through the use of decentralised technologies such as the blockchain. The blockchain provides a platform on which information can be created and shared in a community where each member has control over their own data. All entries are permanent, and each update is a new "block" added to the end of a "chain" (Grech & Camiller, 2017). When people are in control of their data, their right to privacy is not violated. They choose what happens to their data and know what their data is being used for.

The value of SSI for education

If educational data were decentralised, individuals with digital identities would be able to control their identity records, including data related to their education, training, skills, projects, job history, assessments and more, and provide this data for verification and transactions without the need to rely on institutions or a central repository of data. Individual citizens would be able to turn their skills, training and experience into genuine value in the labour market, and access better career and development opportunities.

Educational institutions are increasingly using learner data to improve outcomes and better cater to learners' needs (see for example Stahl & Karger, 2016). There is a danger that this data could be used in a way that is harmful, especially because educational institutions are often not resourced or informed on ways to protect it. SSI offers a learner-centred solution to privacy and security in educational institutions. So much personal information about people is shared and used without their knowledge. Since the education sector holds a wealth of information, protecting this information should be a priority.

The use of SSI for educational purposes is perfectly suited to securing learning achievements and educational credentials (Thomas, Koenig, Higgins & Black, 2019). The rise or need for e-learning has become evident in the time of COVID-19, but the main concern has been about the trustworthiness of the platforms that provide digital learning. Blockchain systems have been reviewed and recommended as a solution to digital learning because they store data in decentralised, secure, manipulation-proof and transparent systems (Thomas et al., 2019). Learning and education are social activities and are therefore

prone to human error. The introduction of blockchain to education will minimise human error and allow for self-sovereign control of data (Thomas et al., 2019).

Some of the specific areas where SSI brings value to educational systems are described next.

Registering learners

The SSI benefit in education or higher education occurs throughout the learner life cycle, but one of the most compelling uses is when learners are registered and authorised. Here, SSI 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 (Smith & Tobin, 2018).

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 site. 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 more safe and secure manner. Importantly, this leaves an audit trail. Students know what information has been requested and why. With no more usernames and passwords, this is a convenient approach that delivers improvements across the student life cycle and makes for a seamless and frictionless user experience.

Communicating with learners

The secure connection offered by SSI between the user and the institution creates a secure and private channel of communication. With SSI, institutions can communicate with students regarding assignments, exams, important notifications and other messaging. This can be a life-long connection, one which is not only valid during the student years of an individual, but also after qualifying. Alumni newsletters can be shared this way and, if students give permission, their data can be used to track their careers.

Enhanced securing of information

Security is enhanced through SSI by the decentralising of personal information, with the individual being given back control of his or her data. With SSI as a standard, it would no longer be necessary for data silos to house vast amounts of personal data, which are vulnerable to cyber-attack and inaccessible to the individuals to whom the data belongs. SSI provides a secure way to manage personal information, which in turn empowers individuals to have more complete control over their privacy (Lewis, 2017).

An admission office will typically keep its data on a central database. This valuable data is vulnerable to data leaks, hacks and abuse. Every time this data needs to be accessed or transactions need to be done, permission needs to be sought by the user. With SSI, users are able to access their data on their devices and only share it with third parties when they need to. This is similar to having a paper copy, only with a permanent, downloadable version that cannot get lost.

Easier credentialing and more effective access to and preparation for the world of work

SSI allows for the storage of academic records and issuing of certificates (Smith & Tobin, 2018). 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. SSI 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 higher education institutions (HEIs) and students/alumni face is that paper or physical credentials can get lost or damaged. HEIs 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 SSI 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 cost 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 control with whom they share it. In other words, through SSI, students will be able access and share genuine qualifications and credentials.

SSI 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, SSI also allows for better matching of labour demand with skills supply. As such, SSI can facilitate reciprocal relationships between education and labour that would enable the education system to provide training on appropriate workplace skills because of having a clear and current understanding of labour market needs.

Implementation and scalability

SSI entails a new way of thinking, and new paradigms can be challenging to adjust to. To introduce an entirely new paradigm of digital identity overnight could be highly disruptive. However, one of SSI's key advantages is that the technology is scalable, and can be introduced over time, gradually migrating existing systems towards decentralised data ownership and collaborative and interactive processes.

Case studies of SSI in education

The Pan-Canadian Trust framework

Established in 2012, the Digital Identity and Authentication Council of Canada (DIACC) is a neutral, non-profit, industry-led consortium of public and private sector leaders committed to developing a Canadian digital identification and authentication framework to enable Canada's full and secure participation in the

global digital economy. Canada regards collaborations between institutions and organisations as the building blocks that lead to a digital identity. The rules and tools of a digital ecosystem have been created by leading institutions and organisations in partnership with DIACC. This cooperative ecosystem allows companies to leverage the best available information to validate a customer's identity.

In this model, a secure connection is used to transmit data. A new decentralised identifier is created for each user and provider. When an interaction happens, for example in a higher education setting, the user and the university exchange identifiers via blockchain technology, creating a secure ledger where such transactions are recorded. The user now has the public key and endpoint of the university, and the university has the same for the user. This allows only the university to decrypt data sent to them by the student, and only the student to decrypt data sent from the university. The ledger is there as a store of the public keys of the credentials of issuers. The institutions issuing credentials do not need to be part of a closed consortium as this is an open ecosystem. The self-sovereign network is a permission network, meaning it needs to be given permission to run a node.

McMaster University is leading the digital revolution in higher education in Canada, being the first university in the country to move to digital degrees and diplomas in 2019. Their ethos is one of innovation, where they recognise that, just as businesses and society are innovating, so does higher education in order to keep up. The university uses a free app called Blockerts, a digital credentialing system built by the Massachusetts Institute of Technology (MIT). This is a pilot project that allows students to choose to participate or not. A student's credentials are stored on the blockchain, a secure ledger where transactions are recorded, and, once published, can be instantly verified but never changed. Students also receive an online version of their credentials, which is a digital replica of the printed version of their degree or diploma. The university believes that data should belong to the student, and thus data should be governed according to self-sovereign principles. Through this initiative, graduates are given autonomy and authority over their own credentials. It saves both the student and the institution time and money. In 2018, McMaster University reprinted 326 diplomas: the move towards digital degrees will eventually eliminate the need for this expense. Another instance where McMaster University issued digital credentials to students was when, in April 2019, students participated in a co-curricular programme. Participants received the university's first digital micro-credential for an activity outside of class.

Registree

The Registree[1] model, in use at the University of Cape Town, has three major components:

1. Storing students' data using a decentralised and distributed database;
2. Storing and identifying information in the centralised CRUD (create, read, update, and delete) databases; and
3. Linking user data and identifying information using the blockchain.

[1] https://registree.rocks/

Registree is a data services provider for universities in South Africa that can holistically track students' performance, and thus identify students needing additional academic support. Employers are also given access to this platform to search for prospective employees.

Figure 1 shows how the Registree system works. The decentralised records database stores data, and each entry in this database is linked with an SSI that is stored on the data-owner's phone. The university (custodian) holds both the decentralised records database and the identifying database, and also has the power to create data. The data-owner controls the smart contract and has the power to make the link between the data and themselves as the data-owners.

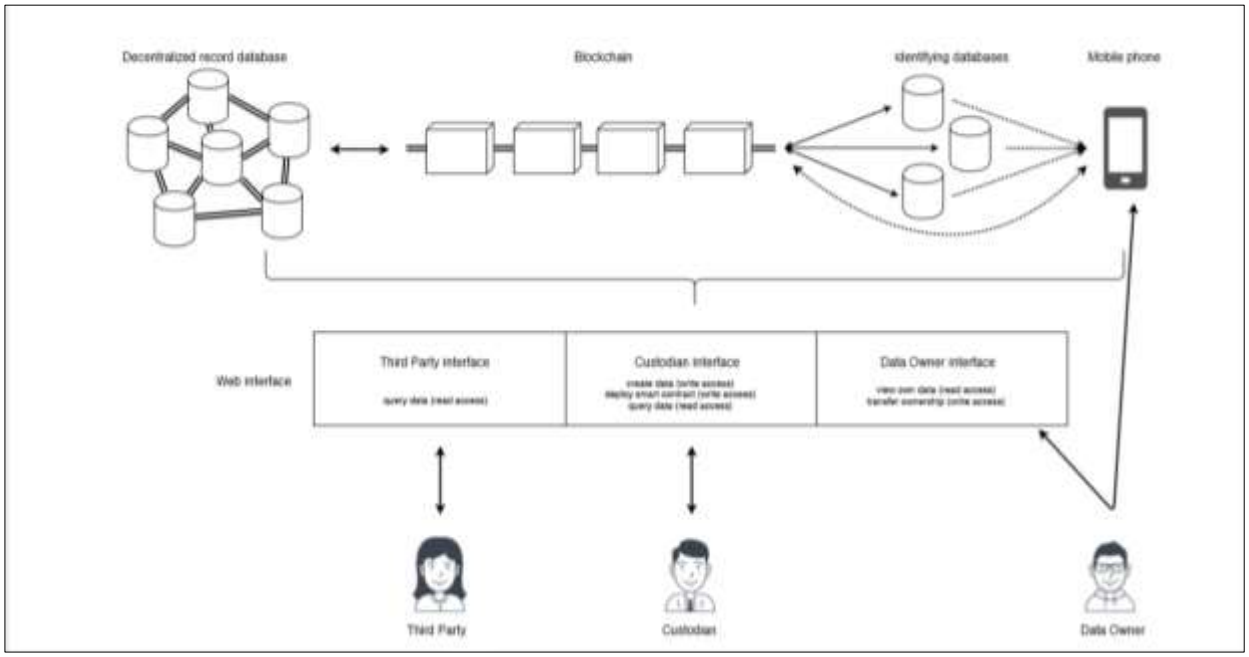

Figure 1. Registree system architecture (Source: Bertram & Georg, 2018)

The database stores all students' data except for identity information. Data is stored by the address of the matching smart contract, making it difficult to know to whom the data belongs. Only the owner of the data can identify their data since each contract contains a link to the identifying information. User data can only be created by the university, thereby ensuring the integrity of the data at all times. The data stored in the decentralised database is not encrypted and is stored in plaintext, allowing queries and searches to be carried out without revealing any user's identity.

At first, all the identifying information is stored in a centralised CRUD database held by the university. In order to enhance anonymity, additional fake data is added to the data system. This prevents the users from being mapped to their data and thus making the database more secure. The users may not create their data, but they do own it, and are able to update their identity details or move any entry to their SSI management system.

Blockchain technology is used to link user data to the students' identity and to ensure ownership and privacy. Once the smart contract is created, the students are encouraged to claim their data and update it

frequently to increase security. If the user/student denies access to their data, they can update their ID in the identifying database, but not update it in the smart contract.

The success of Registree lies in its many benefits for all parties involved, namely the data-owners (students), custodians (universities) and any third party (e.g. employers), and it comes at no financial cost. Through Registree, a student is able to store sensitive personal academic data, track their performance at university and gather credentials with which to seek employment.

The Frankfurt School of Finance and Management

The Frankfurt School of Finance and Management in Germany, in cooperation with Consensys, is one of the first universities to have issued and distributed digital credentials to students who have completed their courses. Their Blockchain for Education platform is based on the Ethereum blockchain. Ethereum is a global, open source, decentralised platform.

The Frankfurt School of Finance and Management partnered with Consensys and Ethense for this decentralised credentialing initiative, which involves the owner of a particular node deciding on a case-by-case basis which certificates he or she makes visible to other network participants. The platform gives users the capacity to create, store and control their credentials digitally in whatever form they prefer. The certificates issued are not forgeable, which protects students from identity theft. The university is also protected from any reputational damage. The data of the certifier, such as personal information, is not stored on the blockchain to protect the individual and keep their anonymity.

The Blockchain for Education platform allows certifiers to prove that they belong to a certain accredited certification authority while retaining anonymity. There is reduced manual labour involved with requests and the re-issuing of certificates. Waiting time and fees are excluded or minimised. The certificates can easily be verified even if the certification authority no longer exists. Certificates with a time-limited validity are automatically monitored and there is counterfeit protection of all certificates issued.

Evernym's Higher Education SSI Initiative

Evernym is a company seeking to help higher educational institutions realise value from existing data, while empowering students and setting them up for a digital future in which they own and control their data. It claims to provide a new way to move and prove data in a way that is secure and private and yet open to all. This is in alignment with SSI principles. One of the key issues with proving identity online is that it traditionally has required users to supply more and more information to confirm that they are who they say that they are. With SSI, credentials can be instantly and securely verified, without the need for individuals to disclose data unnecessarily. Secure connections that cut out the middleman go directly from user to service. Data watermarking is the key to verifiable data. Cryptographic tools are used to ensure this process is secure. A trusted, tamperproof Public Key directory can be used to verify the digital watermark.

Evernym outlines a number of benefits for educational institutions:

1. SSI tools are currently available and can be adopted by institutions immediately.

2. A digital "Student Wallet" can be used in multiple cases to prove credentials, such as a student ID number, email access or a student's age, for example.

3. Existing IT and infrastructure can remain in place, with no need for a “rip and replace” processes.

4. Adopting SSI practices is scalable, starting with one function (say, age verification) and then being adopted for multiple other functions, from access to email, student zones, to issuing degree certificates.

While individually these functions already exist in isolation, SSI can span multiple functions and uses, bringing them all under the same ecosystem with a single digital solution.

Identity data is often housed in separate silos, and continually trying to bring the silos together becomes complicated and unfeasible. Because of available technologies like blockchain, we are no longer limited to proprietary wallets or silos. Now open-standard, decentralised credentials are possible, and even preferable to traditional systems. When the student or citizen is placed at the centre of their digital life, many of the current problems of digital identity are solved.

SSI in the time of COVID-19

Two recent, rapid developments that use SSI in response to COVID-19 are significant: (1) the COVID-19 credentials initiative[2]; and (2) the COVI-ID app.

1. The COVID-19 credentials passport is a certificate that allows individuals to prove their COVID-19 status: that they have recovered from the coronavirus, have tested positive for antibodies or have received a vaccination (when available). A COVID-19 credentials passport is like an international certificate of vaccination, such as a yellow fever vaccination certificate, and could be required for travel during this pandemic (and possibly going forward). The use of SSI in this initiative empowers individual privacy, making the credential (the passport) accessible only by the individual and the organisation that provides it (e.g. the hospital or clinic that did the test). The individual then chooses with whom to share that credential.

   In this model, there is trust between the issuer of a credential, the holder of that credential and a verifier. The certificate is controlled by the individual and shared in a peer-to-peer manner. It consequently operates quite differently to the mass surveillance measures that have been implemented in many countries and which involve central agencies or organisations carrying out, for example, contact tracing and location tracking – an approach which can compromise and threaten data protection and an individual’s right to privacy.

   With the COVID-19 credentials passport project, the blockchain is used as the technology platform because it provides a decentralised directory of public keys. Unlike a centralised service, the decentralised blockchain technology grants control of the data to individuals.

   Sixty organisations are engaged in the development of this COVID-19 credentials passport, including DIDx[3] in South Africa.

[2] https://www.coindesk.com/covid-19-immunity-passport-unites-60-firms-on-self-sovereign-id-project

2. COVI-ID[4] has been developed as a uniquely South African response to the pandemic. This app collects an individual's location and infection status, and stores it on their phone using SSI rather than on a centralised database. This provides the individual user with full authority and control over who gets access to their health data, for what purpose and for how long, and provides a way to verifiably prove an individual's infection status in a reliable and secure way, without the loss of privacy.

   Work is ongoing to incorporate the verification of doctors into the system, as well as to find ways of making vital data accessible to the scientists who need it, while greatly improving the protection of privacy and personal data for all involved (Georg, 2020).

Conclusions: SSI and the education sector

COVI-ID and the COVID-19 credentials passport highlight not only the relevance of SSI applications, but also the realisation that it is possible (1) to gain traction and commitment quickly and effectively and (2) to mobilise resources to make SSI projects a reality and at scale. The COVID-19 credentials passport has also proved that this type of project can be achieved collaboratively on a global level, and that it is possible to create systems based on trust that are interoperable globally.

A use case for SSI in education during the COVID-19 pandemic is eminently feasible. With the pandemic entailing lockdown and physical restrictions for many, there are learners around the world who are having to study remotely and engage with schools and educational systems at a distance. SSI would provide learners with verifiable visibility and a cryptographic trail that would make managing their education much less onerous and fraught.

Furthermore, it is also easy to see how these applications could inform the adoption of SSI in educational settings beyond the pandemic.

This report has detailed five clear benefits of SSI, which in summary are as follows:

1. **SSI is an effective way of issuing and verifying digital transcripts.** SSI allows learners to be provided with digitally enabled credentials that can be utilised to apply for jobs and to be sent to prospective employers. This enables learners 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.
2. **SSI can be used in supporting and digitising the learner ecosystem.** Although digital transcripts are important, they constitute a narrow focus for SSI, which can be deployed more broadly across the entire learner life cycle and ensure the learner ecosystem is digital, frictionless and secure. Thus, for example, SSI can be used for:

[3] **https://www.didx.net/**

[4] https://coviid.me

- Onboarding of learners and verification of their identities;
- Access control (e.g. getting into classes, accessing the library, getting semester points into a digital wallet, buying books, securing accommodation, etc.); and
- Communicating securely and privately.

These uses are cryptographically provable with SSI, which would reduce friction and fraud, increase security, and remove the need for usernames and passwords as well as physical learner cards. It would also allow for greater trust between learners and their institutions.

1. **SSI can be used for matching labour demand and supply.** SSI 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, low demand, etc.
2. **SSI allows for information exchange between institutions and systems.** Data can be exchanged in real time between institutions and systems. This also allows for the linkages of networks – the South African education system is just one network of a larger meta network.
3. **SSI provides a frictionless user experience**. With SSI, phishing is a thing of the past as there are no intermediaries, every digital relationship is unique, secure and private. Exchanges of data and the verification of credentials can happen with speed and at no cost.

With the increasing need for online education, verifiable credentials would greatly benefit the fight to continue education in the face of the COVID-19 pandemic by addressing the real concerns of security and accessibility. SSI technology is scalable, interoperable and cheap, and could be applied in education in an effective and revolutionary way. COVID-19 has shown us that implementing SSI effectively and with speed is possible. It is now time for the South African education system to adopt SSI and reap its benefits. The recommended approach is to:

4. **Gradually drive the uptake of SSI in education in South Africa.** This will require stakeholder engagement and political will.
5. **Develop the necessary policy and legislation**.
6. **Utilise a user-centred approach to the adoption of SSI,** with feedback from users informing iterations through first a pilot phase and then the mainstreaming of SSI in the system.

References

Bertram S & Georg C. (2018) A privacy-preserving system for data ownership using blockchain and distributed databases. arXiv.org. Retrieved from: **https://arxiv.org/abs/1810.11655**

Der U, Jähnichen S & Sürmeli J. (2017) Self-sovereign identity – Opportunities and challenges for the digital revolution. arXiv.org. Retrieved from: **https://arxiv.org/ftp/arxiv/papers/1712/1712.01767.pdf**

Georg C. (2020, 5 April). Covi-ID: Privacy-preserving COVID-19 status verification. Medium. Retrieved from: **https://medium.com/coviid/covi-id-privacy-preserving-covid-19-status-verification-c11d59ec92f6**

Grech A. & Camilleri AF. (2017) Blockchain in education. Amorato dos Santos, A. (Ed.) JRC Scince for Policy Report Luxembourg : Publications Office of the European Union. Retrieved from: **https://www.pedocs.de/volltexte/2018/15013/pdf/Grech_Camilleri_2017_Blockchain_in_Education.pdf**

Lewis A. (2017, 17 May) A gentle introduction to self-sovereign identity. Bits on Blocks. Retrieved from: **https://bitsonblocks.net/2017/05/17/gentle-introduction-self-sovereign-identity/**

Lyons T, Courcelas, L & Timsit K. (2019) Blockchain and digital identity. EU Blockchain Observatory and Forum. Retrieved from: **https://www.eublockchainforum.eu/sites/default/files/report_identity_v0.9.4.pdf**

Preukschat A. (2018, 11 January) Self sovereign identity: A guide to privacy for your digital identity with bockchain. Medium. Retrieved from: **https://medium.com/@AlexPreukschat/self-sovereign-identity-a-guide-to-privacy-for-your-digital-identity-5b9e95677778**

Reuters Fact Check Team. (2020) False claim: Bill Gates planning to use microchip implants to fight coronavirus. Reuters, 31 March 2020. Retrieved **from https://www.reuters.com/article/uk-factcheck-coronavirus-bill-gates-micr/false-claim-bill-gates-planning-to-use-microchip-implants-to-fight-coronavirus-idUSKBN21I3EC**

Smith J & Tobin A. (2018) Self-sovereign identity for higher education [Blog post]. Evernym. Retrieved from: **https://www.evernym.com/blog/self-sovereign-identity-higher-education/**

Solid. (Undated) Frequently asked questions. Retreived from: **https://solidproject.org/faqs**

Stahl W & Karger J. (2016) Student data privacy, digital learning, and special education: Challenges at the intersection of policy and practice. Journal of Special Education Leadership 29: 79–88

Thomas A, Koenig N, Higgins, T & Black M. (2019). From learning to assessment, how to utilize blockchain technologies in gaming environments to secure learning outcomes and test results. Journal of Applied Research and Practice 3(1): 172

Toth KC & Anderson-Priddy A. (2019) Self-sovereign digital identity: A paradigm shift for identity. IEEE Security & Privacy 17(3): 17–27. doi:10.1109/msec.2018.2888782

Appendix A: Further reading

Chartrand J, Freeman S, Gallersdörfer U, Lisleve M, Mühle A & Mühle S. (2020) *Building the digital credential infrastructure for the future*. Digital Credentials Consortium White Paper. Retrieved from: **http://philippschmidt.org/articles/2020-01-White-paper-building-digital-credential-infrastructure-future.pdf**

Crocco MS, Segall A, Halvorsen A-L, Stamm A & Jacobsen R. (2020) "It's not like they're selling your data to dangerous people": Internet privacy, teens, and (non-)controversial public issues. *Journal of Social Studies Research* 44(1): 21–33

Cuda A. (2014, 1 November) Milford girl back in school after Ebola scare. *Connecticut Post*. Retrieved from: **https://www.ctpost.com/local/article/Milford-girl-back-in-school-after-Ebola-scare-5861748.php**

Doerk A. (2020) eSSIF: The European self-sovereign identity framework [Blog post]. *Medium*. Retrieved from: **https://medium.com/@SSI_Ambassador/essif-the-european-self-sovereign-identity-framework-4572f6875e12**

Federman H. (2020, 16 April) COVID-19 could have its own PATRIOT Act, but we need privacy guarantees. *TechCrunch*. Retrieved from: **https://techcrunch.com/2020/04/16/covid-19-could-have-its-own-patriot-act-but-we-need-privacy-guarantees/**

Ferdous MS, Chowdhury F & Alassafi MO. (2019) In search of self-sovereign identity leveraging blockchain technology. *IEEE Access* 7: 103059–103079. doi:10.1109/access.2019.2931173

Gräther W, Kolvenbach S, Ruland J, Schütte C, Torres C & Wendland F. (2018) Blockchain for education: Lifelong learning passport. In W Prinz & P Hoschka (Eds.), *Proceedings of the 1st ERCIM Blockchain Workshop 2018, Reports of the European Society for Socially Embedded Technologies* (ISSN 2510-2591). doi:10.18420/blockchain2018_07. Retrieved from: **https://dl.eusset.eu/bitstream/20.500.12015/3163/1/blockchain2018_07.pdf**

Irwin L. (2020, 7 April) GDPR: The implications of working from home or on the road [Blog post]. *IT Governance*. Retrieved from: **https://www.itgovernance.eu/blog/en/gdpr-the-implications-of-working-from-home-or-on-the-road**

Kharpal A. (2020, 26 March) Use of surveillance to fight coronavirus raises concerns about government power after pandemic ends. *CNBC.* Retrieved from: **https://www.cnbc.com/2020/03/27/coronavirus-surveillance-used-by-governments-to-fight-pandemic-privacy-concerns.html**

Knight W. (2020) Phones could track the spread of Covid-19. Is it a good idea? *Wired*. Retrieved from: **https://www.wired.com/story/phones-track-spread-covid19-good-idea/**

Kolvenbach S, Ruland R, Gräther W & Prinz W. (2018) Blockchain 4 education. Retrieved from: https://dl.eusset.eu/bitstream/20.500.12015/3132/1/ecscw2018_p7.pdf

Kondova G & Erbguth J. (2020) Self-sovereign identity on public blockchains and the GDPR. *SSRN*. Retrieved from: https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=3515213

Lomas N. (2020, 6 April) EU privacy experts push a decentralized approach to COVID-19 contacts tracing. *TechCrunch.* Retrieved from: https://techcrunch.com/2020/04/06/eu-privacy-experts-push-a-decentralized-approach-to-covid-19-contacts-tracing/

Lomas N. (2020, 8 April) Call for common EU approach to apps and data to fight COVID-19 and protect citizens' rights. *TechCrunch*. Retrieved from: https://techcrunch.com/2020/04/08/call-for-common-eu-approach-to-apps-and-data-to-fight-covid-19-and-protect-citizens-rights/

McDonald S. (2020, 30 March) The digital response to the outbreak of COVID-19. *Centre for International Governance Innovation*. Retrieved from: https://www.cigionline.org/articles/digital-response-outbreak-covid-19

Mühle A, Grüner A, Gayvoronskaya T & Meinel C. (2018) A survey on essential components of a self-sovereign identity. *arXiv.org*. Retrieved from: https://arxiv.org/pdf/1807.06346.pdf

Pfeiffer A. (2020, 19 April) What role can blockchain technologies play during the Covid-19 crisis (and beyond)? *Comparative Media Studies | Writing*. Retrieved from: https://cmsw.mit.edu/blockchain-covid-19-crisis/

Santani S. (2019, April 26) The government vs citizens: The fight for personal data [blog post]. *Information Space*. Syracuse University iSchool. Retrieved from: https://ischool.syr.edu/infospace/2019/04/26/the-government-vs-citizens-the-fight-for-personal-data/

Sheng J & Xu C. (2020) Collection and use of personal information during the COVID-19 Pandemic: Q&A from a Chinese Law perspective. *Pillsbury Law*. Retrieved from: https://www.pillsburylaw.com/en/news-and-insights/collection-and-use-of-personal-information-during-covid-19-pandemic.html

So W. (2020) South Korea: COVID-19 daily new cases. *Statista*. Retrieved from: https://www.statista.com/statistics/1102777/south-korea-covid-19-daily-new-cases/

St. Clair J, Ingraham A, King D, Marchant MB, Cotesworth McCraw F, Metcalf D & Squeo J. (2019) Blockchain, interoperability and self-sovereign identity: Trust me, it's my data. *Blockchain in Healthcare Today* 3. doi:10.30953/bhty.v3.122. Retrieved from: https://blockchainhealthcaretoday.com/index.php/journal/article/view/122/144

Van Bokkem D, Hageman R, Koning G, Nguyen TL & Zarin N. (2019) Self-sovereign identity solutions: The necessity of blockchain technology. Delft University of Technology. Retrieved from: https://www.researchgate.net/publication/332750774_Self-Sovereign_Identity_Solutions_The_Necessity_of_Blockchain_Technology

Wang F & De Filippi P. (2020) Self-sovereign identity in a globalized world: Credentials-based identity systems as a driver for economic inclusion. *Frontiers in Blockchain* 2. doi:10.3389/fbloc.2019.00028

Appendix B: The research team

Barbara Dale-Jones	The Field Institute	Team Lead
More Manda	MerSETA	Quality Assurance
Eduarda Castel-Branco	European Training Foundation	Quality Assurance
Anam Magudu	Academic Medic Tutor	Researcher
Ashley Tshabalala	Rev.com	Researcher
Buhleng Masake	'Girls in Tech' programme at IBM	Researcher
Gomolemo Fritz	Effective Engineering and Artisan Centre	Researcher
Michael Raven	Barnyard Theatre Company	Researcher
Zani de Wit	UCT Lung Institute	Researcher
Maureen Mosselson	Jet Education Services	Editor