THE GDN NETWORK

DEVELOPING A GLOBAL GOVERNANCE

Framework for Credentialing Platforms for Work and Learning

Authors: Dr. Rooksana Rajab, Koichi Nakasaki

ACKNOWLEDGEMENTS

Gratitude is extended to the authors for their research and to all those who contributed to the development and enrichment of this paper including the staff and board members of the Groningen Declaration Network (GDN Network). The authors are particularly grateful to one of the primary reviewers, Mr. Rick Torres (former President and CEO of the National Student Clearinghouse and Chair for the GDN Strategic Advisory Council) for his insightful feedback and constructive suggestions. His critical engagement helped to refine the report and clarify key points, ensuring a more comprehensive and coherent outcome.

The authors also wish to acknowledge the valuable input from other colleagues and peers consulted during the creation of this report whose perspectives and expertise were instrumental in shaping the final version of this paper. Their encouragement and thoughtful contributions added depth to the analysis and broadened the understanding of the complexities surrounding global migration, digital credentialing platforms, and ethical governance.

Finally, the authors express their appreciation to the broader academic and professional communities for their ongoing discourse on these important topics within and beyond the GDN community, which inspired and informed the research. The GDN anticipates this paper will contribute meaningfully to the continued exploration and development of global governance framework to help guide the creation and sustainment of credentialing platforms and networks.

ABOUT THE GDN

The GDN Network is an international, non-profit federated trust located in the Netherlands. It represents a voluntary network of like-minded organizations and individuals that seek to make digital student data portability happen. This governance paper contributes to the overarching goals of the GDN to catalyse a Network of Networks convening of supports, pilots and frameworks to ensure scalable, interoperable national digital networks for credential exchange that are built on open standards and principles.

Disclaimer: This paper contains the opinions and research of the authors and does not necessarily reflect those of the Groningen Declaration Network (GDN Network). The GDN Network assumes responsibility for the accuracy of information in this report nor for the currency of information. Mention of products, vendors, services, and announcements in this report does not constitute GDN Network endorsement, actual or implied. The GDN Network retains exclusive copyright on all works that it publishes.

CONTENTS

ABSTRACT

The phenomenon of individuals migrating across borders in pursuit of economic opportunities and educational advancement represents a significant trend that warrants careful consideration when creating digital credential ecosystems to support learner mobility. In 2020, around 281 million people were international migrants, comprising 3.6% of the global population (International Migration Report, 2022). While international students pursue opportunities for higher education abroad for diverse purposes, such as acquiring international experience, enhancing readiness for the job market, and experiencing alternative styles of study and learning (Tucker, 2020), around 110 million people were forcefully displaced worldwide by the middle of 2023 (UNHCR, 2024) escalating the number of people crossing borders.

Advancements in technology have notably monitored this migration by simplifying and enabling the tracking of such movements. Digital platforms play a pivotal role in the process of effectively capturing comprehensive data and credentials acquired during educational pursuits of many of these individuals. These digital platforms can additionally facilitate the seamless sharing, presenting and access-to pertinent information in a permission based context dependent upon the authenticity of the data and the trustworthiness of the collaborating partners involved. Since 2012, the Groningen Declaration Network (GDN Network) operates on the premise that citizens worldwide should be able to consult and share their authentic educational data with whomever they want, whenever they want, wherever they are. To achieve the objective, Signatories of the GDN Network sign a Declaration which aims to establish a global alignment and interoperability of digital student data depositories and networks, while respecting their autonomy and diversity (GDN, 2012).

For such global initiatives, improving the capabilities of technical platforms and creating policies and standards on how data exchange, presentation, and access-permissioning as a support to citizen and learner mobility can be improved, becomes compelling. Widespread collaboration is necessary to ensure compatibility and comparability of data. However, initiatives such as these underscore numerous challenges related to data privacy, control, decision-making, ownership, monopolies, and overall governance, prompting questions about what measures are being taken to safeguard ethical considerations. By presenting and deepening the understanding of governance principles of humanities and global fairness, transparency and trust for autonomous collaborations, and openness for dynamic value creation, this report intends to provide a foundation to facilitate the GDN Network developing a global governance framework for creating and sustaining digital credentialling platforms and networks. A well-considered governance framework is proposed to be created through GDN engagement and consultation that embeds citizen agency.

1. INTRODUCTION

The phenomenon of individuals migrating across borders in pursuit of economic opportunities and educational advancement represents a significant trend that warrants careful consideration. In 2020, around 281 million people were international migrants, comprising 3.6% of the global population (International Migration Report, 2022). While international students pursue opportunities for higher education abroad for diverse purposes, such as acquiring international experience, enhancing readiness for the job market, and experiencing alternative styles of study and learning (Tucker, 2020), around 110 million people were forcefully displaced worldwide by the middle of 2023 (UNHCR, 2024) escalating the number of people crossing borders.

Advancements in technology have notably facilitated this migration by simplifying and enabling the tracking of such movements. Of importance, is that digital platforms play a pivotal role in the process of effectively capturing comprehensive data and credentials acquired during educational pursuits of many of these individuals. These digital platforms can additionally facilitate the seamless sharing of pertinent information, dependent upon the authenticity of the data and the trustworthiness of the collaborating partners involved. Since 2012, the Groningen Declaration Network (GDN Network) operates on the premise that citizens worldwide should be able to consult and share their authentic educational data with whomever they want, whenever they want, wherever they are. To achieve the objective, the declaration aims to establish a global area of convergence on digital student data platforms and networks, while respecting local autonomy and diversity (GDN, 2012).

For such global initiatives, the development of capabilities of technical platforms and the need for policies on how data exchange as a support to citizen and learner mobility can be improved, becomes compelling. Widespread collaboration is necessary to ensure compatibility and comparability of data. However, initiatives such as these underscore numerous challenges related to data privacy, control, decision-making, ownership, monopolies, and overall governance, prompting questions about what measures are being taken to safeguard ethical considerations. By presenting and deepening the understanding of governance principles of fairness, transparency and trust for autonomous collaborations, and openness for dynamic value creation, this paper serves as a foundation to support development of a global GDN governance framework for credentialling platforms and networks. In terms of inclusivity, a well-considered strategy for citizen agency as a new horizon for governance is proposed and can to be taken forward to ensure widespread community engagement and inclusivity.

Evidence suggests a significant gap exists that must still be addressed, and the authors propose that the GDN Network with its mandate to support learners is one place to address the situation by providing guidance to its community with a governance framework. Developing this for credentialling platforms provides a structured approach to managing risks, ensuring compliance, enhancing efficiency, building trust, and driving continuous improvement within organizations or systems, ultimately contributing to their long-term success and sustainability.

2. BACKGROUND

The education system worldwide is currently undergoing structural change and a variety of digital transformation processes, driven by the need to adapt to evolving technological advancements, shifting societal demands, and the growing emphasis on personalized learning experiences. The inception of standardized data collection in the industry was pioneered more than thirty years ago by organizations such as UCAS in the UK, the Ontario Universities' Application Centre in Canada, and later by organizations like the National Clearing House. The latter organization as with these and other early examples, played a crucial role in laying the groundwork for modern data practices in the US (National Student Clearing House, 2015). However, the evolution of data management has since expanded beyond its early foundations. Today, institutions and companies are grappling with the complexities of data acquisition, storage, usage, obtaining proper consent or ensuring transparency to individuals. This journey using the National Clearing House's initial efforts to the current US based landscape as one example, underscores the ongoing challenges and the need for ethical and responsible data practices.

Several platforms in the past two decades have been launched for the purposes of issuing credentials. Examples include Credential Engine which was launched in 2017 in the US with the aim of mapping the credential landscape with consistent information with an focus on ancillary non-personal data to enable and empower credential exchange solutions and other capacities as a support to individuals to help them find the best pathways for learning and work (GDN Network Webinar Series, Jan-March 2025). Other examples include the European Blockchain Services Infrastructure (EBSI) which was established in 2018, MyCreds which was launched as a national credential exchange network in 2020 to support official verification, curation and sharing of documents issued by Canada's colleges, universities, secondary schools and governments. This network delivers digitised and portable transcripts and credentials – including badges and microcredentials – to post-secondary learners and to verifiers around the world online anytime, anywhere. My eQuals in Australia and New Zealand launched prior to MyCreds and is part of its international network. These two taken together are supporting the circulation of over 10 million officially verified digital document transactions through and beyond the network itself which is reliant on various data standards and is readily interoperable with other systems. YoMobi is another South African platform that was launched in June 2022.

As technology advances and more credentialling platforms and networks emerge, there is a concomitant increase in the number of challenges that have arisen. Smolenski (2016) in her quest to highlight what capability means and what credentials do, raised the issue

of professionals being unable to practice their trades internationally due to differences in credential evaluation. While this issue predates technology matters, it remains a challenge in the present day. She proposed standardized global data definitions to empower professionals to work worldwide, enhancing productivity and international cooperation. Concurrently, credentialing platforms and networks, which are used to verify and manage individuals' qualifications, certifications, licenses, or other credentials, foreground the need for robust governance mechanisms to ensure the integrity, security, and interoperability of the credentials they handle. Generally, the governance and management of interoperable platforms are typically guided by a combination of industry standards, regulatory frameworks, consortiums, and individual company, institutional and provincial, state or national policies. However, there is no consistency in the approach to governance as evidenced in the study conducted on several international interoperable platforms for work and learning (Rajab et al, 2023).

As AI systems become increasingly common throughout the education system, they give rise to a variety of issues and pose significant challenges for the protection of data and impact the rights of citizens on data privacy and misinformation due to lack of appropriate understanding of the underlying foundational data. Blockchain technology in education, defined as a distributed database or ledger that is shared among the nodes of a computer network (The Economic Times, 2023; Rajab et al, 2023), is relatively new in education and the ethos behind it is similar to Bitcoin, that is, to empower a decentralized community of learners with full control over their trusted credentials and transcripts. A human rights-based approach is crucial for addressing issues in AI deployment, particularly in safeguarding vulnerable populations like migrants and refugees. Implementing human rights impact assessments before deploying AI systems can enhance fairness, accountability, and prevent harm. Upholding the "do no harm" principle during the entire AI lifecycle can mitigate risks associated with these technologies in migration processes (McAuliffe et al, 2021).

Several interoperable platforms and networks continue to be developed and managed by consortia or collaborative initiatives involving multiple stakeholders from industry, academia, government, and non-profit organizations. These entities work together to establish common protocols, specifications, and best practices for interoperability. Individual companies, governments, and organizations that develop interoperable platforms and networks often have their own governance structures and policies in place to manage their development, operation, and evolution. This may include internal committees, processes for handling feedback and feature requests, and mechanisms for ensuring backward compatibility and version control. This paper considers and explores whether additional measures are needed to serve as a framework for national and international interoperability.

It further argues that gaps remain that must still be addressed and that the GDN Network with its mandate is best placed to do this to support the education digital credentialing efforts. As a starting point, for a governance framework to be established, ethical principles for digital platforms for work and learning, need to be agreed on.

3. GOVERNANCE PRINCIPLES OF DIGITAL PLATFORMS

In establishing governance principles for digital platforms, it is essential to consider their fundamental characteristics within the broader economic and technological contexts. By doing so, it becomes possible to identify ethical principles that serve as a common foundation for the responsible development and management of these platforms.

3.1 PRINCIPLE 1 – HUMANITIES AND GLOBAL FAIRNESS

Users On Global Cyber Space

As of the time when the research for this paper occurred in 2023/24, 5.3 billion people worldwide reportedly used the Internet an average of seven hours a day, with 4.95 billion of them engaging with social networking media. The Internet functions as a single global network, enabling unprecedented levels of interaction. For the first time in human history, the majority of world citizens are conducting daily economic and social activities in a single conceptual space - cyberspace.

Within this cyberspace, the behavioral history data generated by the 10 different sensors in the smartphones of 4.7 billion users is being collected and accumulated by IT giant digital platforms as Big Data. Big Data is processed by artificial intelligence to more effectively attract users to the cyberspace. This data is processed by artificial intelligence to more effectively engage users in cyberspace, creating a feedback loop that further attracts social and economic behaviors into this space.

Consequently, information exchange and economic transactions are increasingly migrating from the physical space to cyberspace. As of 2022, 23% of global consumer market transactions occurred online (Insider Intelligence, 2022). This shift has facilitated

the globalization of markets, rendering physical boundaries less relevant. The speed at which cyberspace operates has become a critical factor in economic competition.

In response to the global economic competition, companies are distributing research, development, engineering, and design globally, rather than the traditional structure of knowledge-intensive work at headquarters and labour-intensive work in developing countries (Levinson, 2022). Demand for human resources to support the global organization of companies is increasing, and supply is not keeping up. A Deloitte survey of 175 executives from leading companies in the Asia-Pacific region found that 71% of companies believe the lack of global talent is their biggest external challenge (2022).

Furthermore, the authors believe that some of the 5.3 billion people who continue to migrate information exchange and economic transactions into the global cyberspace are not simply migrating but are forced to rely entirely on the cyberspace due to their vulnerable position in the physical space.

As of the end of 2022, 110 million people worldwide were forcibly displaced because of persecution, conflict, violence, human rights violations, and events that seriously disrupt security (UNHCR, 2024). At least 69% of them have been unable to obtain proof of academic credentials, resulting in the loss of their academic credentials and other possessions (CGD et al 2023). The lack of history and documentation regarding proof of study are barriers to further work and learning in the revalidation process of foreign study credentials in subsequent host countries, resulting in denial of access to higher education institutions and opportunities to exercise income-generating skills. Vulnerable populations, by thei4 nature, transcend borders and cultures, making inclusivity and protection only possible within the global cyberspace.

Furthermore, the authors argue that some of the 5.3 billion users of digital platforms are increasingly shifting and relying on the global cyberspace to transcend borders and cultures for their socioeconomic behavior and corporate activities. Digital platforms of work and learning could potentially function more effectively if they are part of a harmonious part of a cyberspace that transcends borders and cultures. Therefore, ethical principles that provide a common foundation for digital platforms require the consideration and adoption of universal values that are acceptable to people across borders and cultures in the cyberspace. UNESCO's work with the Global Convention on Higher Education provides a foundational example and instrument to help support development of a governance framework (UNESCO, n.d.).

Implications from Broader Ecosystems

What kind of values can be acceptable for people across the borders and cultures that help to support creation and sustainment of digital platforms and networks?

Looking at the wider ecosystem of digital credentials, there are international organizations such as UNESCO and the European Commission as conveners similar to the GDN Network, and national qualification authorities and quality assurance agencies that play an important part in the ecosystem as key players. The ethical principles of digital platforms and networks for work and learning will need to function harmoniously with them in their local contexts.

The first and most fundamental step in this consideration must be human rights, specifically the international declarations of human rights. This begins with the Universal Declaration of Human Rights (UDHR) (1948) and is followed by other United Nations human rights covenants and International Labour Organization (ILO) conventions. Key documents include the International Covenant on Economic, Social, and Cultural Rights, adopted by the United Nations General Assembly in 1966, with an optional protocol added in 2008, which provides an exhaustive list of rights within the labor context. Additionally, the UN Global Compact, with its ten ethical principles for business, further reinforces these human rights standards (Melé et al, 2013).

The human rights have been incorporated into conceptual ethical principles in the form of four ethical principles established by the United Nations Evaluation Group (UNEG, 2020).

The four ethical principles are:

- Integrity - which means the active adherence to moral values and professional standards such as honesty, independence, and impartiality.
- Accountability - which is the obligation to be answerable for all decisions made and actions taken such as transparency, responsiveness.
- Respect - which involves engaging with all stakeholders in a way that honours their dignity, well-being and personal agency
- Beneficence - which means striving to do good for people and planet while minimizing harms.

These concepts present a valid reference model as ethical principles upon which digital platforms and networks would rely. These ethical principles are being translated into more concrete goals through the UN Global Compact, in which 24,625 companies and others from around the world participate.

Of the 17 United Nations Sustainable Development Goals, the Goal 4, related to work and learning, is “Ensure inclusive and equitable quality education and promote lifelong learning opportunities for all”. In addition, UNESCO has identified human rights, transparency, and accountability as ethical principles that digital platforms should follow in the guidelines for their governance (2023a). Those ethical principles and the common goals on which they are based provide the common goals and ethical principles that digital platforms and networks are advised to share.

Implications from Academic Research

Another approach to identifying values that are universally acceptable across borders and cultures is to consider humans as a biological species through disciplines such as neuroscience and cultural anthropology. Within this framework, the concept of fairness emerges as a fundamental ethical awareness inherent in the human species.
From a sociological perspective, humans are intrinsically motivated to seek and appreciate fairness, which is indispensable to human well-being (Scarpa et al, 2021). Research indicates that higher social justice index scores, with fairness being a pivotal component, correlate with higher national levels of life satisfaction (Di Martino et al, 2020).

Cultural anthropological research by Oliver Scott Curry and his team, which examined the ethics of 60 societies worldwide, identified seven forms of cooperative behavior—helping kin, helping one's group, reciprocating, being brave, deferring to superiors, dividing disputed resources, and respecting prior possession—as universally recognized as morally good. Among these, the division of disputed resources, which is identified as fairness, stands out as a key universal value across cultures (Curry et al., 2019).

Behavioral and neuroscientific evidence also suggests that fairness is an instinct for humans. Fairness behaviors, such as making sacrifices for fairness in situations where (1) they have less than others, (2) others have been unfair, and (3) they have more than others, can be observed in childhood (McAuliffe, 2017). This indicates that a sense of fairness, although implicit and expressed differently across cultures, is instinctive for humans.

Cognitive neuroscience research suggests that fairness is not emotionally driven but cognitively driven. Functional magnetic resonance imaging (fMRI) studies reveal that participants' brain activity, particularly in the anterior insula, increases in response to unfair situations, indicating its role in monitoring fairness (Yoder et al., 2014; Li and Tracer, 2017). Fairness has been described as “the most essential rule in social engagement” (Sun, 2013; Avelino-Silva et al, 2023). Additionally, neural activity in the ventromedial prefrontal cortex and ventral striatum increases when participants donate money to their preferred charity, further emphasizing the cognitive basis of fairness (Avelino-Silva et al., 2023).

From an evolutionary perspective, fairness is suggested to be hardwired into the brain, as failure to distribute rewards fairly can lead to aggressive behavior and exclusion from the group (Brosnan et al, 2014).

In conclusion, by examining ethical principles from both the perspective of the global ecosystem and the scientific study of humans as a biological species, it becomes evident that fairness is the foremost ethical principle for digital platforms and networks. This principle is essential for ensuring that these platforms function harmoniously within a society increasingly dependent on global cyberspace.

3.2 PRINCIPLE 2 – TRANSPARENCY AND TRUST FOR AUTONOMOUS COLLABORATIONS

This principle emphasizes the importance of transparency and trust as foundational elements for successful autonomous collaborations. While these values are essential for fostering cooperative relationships, it is recognized that there may be cases where collaboration is not desired or viable. In such instances, transparency remains crucial for clear communication and understanding, ensuring that all parties are aware of the boundaries and reasons for opting out of collaboration. Trust is maintained by respecting these decisions and ensuring that non-collaboration does not result in negative consequences. This approach allows for autonomy while still upholding the integrity of all involved parties.

The cyberspace inhabited by 5.3 billion people across borders and cultures which digital platforms and networks rely on, operates without a centralized management

organization as the architecture of the Internet. The authors argue that the absence of centralized management significantly influences the behavior of the ecosystem and stakeholders involved in digital platforms and networks, creating a fundamentally different environment compared to the traditional pre-Internet era.

Due to the absence of a centralized management organization in the global cyberspace, relationships at each network access point whether between individuals, between individuals and organizations, or between organizations themselves are inherently equal and horizontal. Consequently, the behavioural principles of human work and learning are fundamentally autonomous for each individual.

An example where this architectural relationship is evident as well as one of the apparent challenges is “standardization” of technical standards, particularly interoperability. In the past, standardization was successful through an industry group of a small number of top industry players, in such way as organizations, typically at the top of the supply chain in their respective industry, would come together to agree on a standard. However, unlike such industrial standards, where is a one-way and one-to-many relationship from supplier to users, digital platforms are peer-to-peer and many-to-many between users and between users and suppliers in the cyberspace through SNS and other platforms. (Hindman, 2022).

In digital platforms in the cyberspace, individual users can choose the various web-based services they use every minute and every second, and this creates a feedback loop which attracts more users to the services that are used by more users. This is because the more users a service has, the more interoperable it is for users, the larger the population with whom information can be exchanged, and the more opportunities are available. This effect, known as the network effect, means in terms of “standardisation” that more people will use technical standards that are currently used by more people. In this way, the ‘standardisation’ of technical standards for digital platforms is not fully controllable by industry groups but more effectively driven by the autonomous behaviour of individual users.

The challenge here is to converge autonomously acting individuals and organizations into globally interoperable digital platform(s) or networks. This requires not power, but the ability to motivate world citizens to collaborate voluntarily and autonomously. To achieve this, a user, or learner-centred mindset, is needed to build trust from learners, through transparency and ethical practices in digital platforms.

The Japan International Cooperation Agency concluded, after case studies of several rural official development assistance projects, that “Effective means of mitigating a sense of unfairness among farmers include the establishment of clear and transparent criteria for the provision of assistance. Transparency and fairness is [sic] important in providing relatedness support” (JICA, 2016).

Other empirical studies also suggest that transparent communication has a concurrent effect on employee engagement (physical engagement, emotional engagement, and cognitive engagement) with empirical evidence in a sample of 210 employees of medium and large IT enterprises in Bosnia and Herzegovina, Croatia, and Serbia (Hadziahmetovic et al, 2022), and that disclosure of good and bad information improves performance (Brandes et al, 2017).

Furthermore, AI, which has rapidly and disruptively transformed the way people work and learn in recent years, simultaneously presents ethical issues. As a result, legal systems have been enacted, or guidelines have been provided that require transparency and accountability of AI processing logic. In this aspect too, transparency is an important ethical principle for digital platforms for work and learning as specified for example by UNESCO guidelines for governance of digital platforms (2023a).

3.3 PRINCIPLE 3 – OPENNESS FOR DYNAMIC VALUE-CREATIONS

Another fundamental characteristic of digital platforms and networks in the broader economic and technological context is that the reproduction of digital technology - in other words, the “copying of software” – is, in principle, capital-free. This capital free reproduction of digital technology brings significant changes to the post-R&D production process, making it almost instantaneous, in contrast with industrial products where post-R&D reproduction processes involve a long-term process from capital procurement, factory construction, through channel set-up.

This characteristic of digital technology has given rise to a dynamic development methodology known as "Agile", which incorporates feedback from users into the development process. Agile development emphasizes iterative progress, flexibility, and responsiveness to user needs, allowing for continuous improvement and rapid adaptation in the creation of digital products and services

In addition, as reproduction became capital free, the costs of distribution, trading, selling, and marketing became dramatically lower or free. Thus, individual users of digital platforms can now function not only as consumers but also as producers and sellers: on social network services used by 4.7 billion people, most content is produced and distributed by individuals. On trading platforms such as Amazon, individuals function not only as buyers but also as sellers. Access to computer resources and software services also have become inexpensive. This allows individual users to instantly access knowledge and information for free that was once available only to corporations in the 20th century. The rise of open-source software has played a crucial role in this shift, providing users with powerful tools and platforms at no cost. This, in turn, empowers them to use software services, develop and sell apps on their own, and engage in innovative projects without the need for substantial financial resources. Open source has levelled the playing field, fostering creativity and entrepreneurship on a global scale.

All these changes on digital platforms make users constitute parts of the producers, playing a role in production and providing value. The feedback from these users is what makes development and production process of digital platforms dynamic by allowing them to more easily adapt to an evolving user value chain. Alex Mozad and Nicholas L. Johnson, researchers and entrepreneurs in the platform business, describe this dynamic interaction of production and consumption as follows.

> A linear business focuses on creating value internally and moving that value to its customers. Value flows in one direction, from left to right, from producer to consumer. However, the exchange of value in a network has a variety of directions, from left to right and right to left. As a result, the structure of a platform business is very different from that of a company operating within a traditional supply chain. (Mozad et al. 2018)

In this dynamic development and production process, "platforms create value by coordinating a large external network of consumers and producers, rather than investing in internal resources such as employees, factories, and warehouses" (Moazed et al, 2018). In other words, in digital platforms, value for users is created by capturing value through openness to external networks and by sharing it within the ecosystem. Therefore, openness is the key to value creation in digital platforms.

Another aspect of the in-principle, capital-free nature of digital technology reproduction is that it has increased the rate of technological progress geometrically. Perhaps one of the most obvious ways this has affected our work and learning is through artificial intelligence. AI is rapidly shifting the frontier between humans and machines. As companies adopt the latest digital technologies such as artificial intelligence, tasks such as office work and accounting, services, manufacturing, and even design and marketing are being automated. Required skills and work styles are changing dramatically (WEF, 2023).

For example, the World Economic Forum estimates that between 2023 and 2027, the labour market will be fundamentally and significantly reorganized with the disruptive impact of expanding or shrinking occupations representing 23% of the current working population globally.

This disruptive reconfiguration of occupations and skill sets has increased the need for new skill sets in a wide range of occupations, partly because of the shortage of skilled workers in certain fields around the world in the first place. As a result, demand for ongoing training and skills development has increased. As people's active involvement in the labour market continues to increase over the coming decades in the context of demographic change, reskilling and skills development are becoming an integral part of professional life (UNESCO, 2023b).

In this way, dynamically evolving and geometrically advancing digital technologies have disruptively reorganized skill sets, which has dramatically increased the need for lifelong learning. Lifelong learning has thus become one of the critical missions of our digital platforms for work and learning.

The dynamic evolution of digital technology involving individual users through the global cyberspace has also spread the idea that innovation is created through collaboration and competition among diverse human resources in businesses and government agencies around the world. As a result, the number of international students worldwide increased from approximately 2.1 million worldwide in 2000 (of which 1.2 million were in higher education) to 6.3 million in 2021 (of which 5.6 million were in higher education), an increase of approximately three times (4.6 times for higher education) in 20 years even after the Corona disaster (IIE 2020).

A digital platform shaped by dynamic interactions with highly mobile, lifelong learners from around the world, and supported by the stakeholders of the Groningen Declaration Network and other partners, will generate significant learner-centric value. This value is achieved by embracing openness to a diverse range of external networks, which are deployed autonomously and in a decentralized manner. Openness, as an ethical cornerstone, will be a key guiding principle for our digital platform.

4. BEST PRACTICES

4.1 ORGANIZATIONAL MODELS

Nationwide digital *credentialing* was started as early as the 1990's in the United States, Scandinavia, the Netherlands and other European nations.[1] In the 2000s, more organizations followed suite in regions such as China, South Korea and other nations, followed by the Australia, New Zealand, India, Singapore, Canada, and other nations in the 2010s.

Organizations who are managing those nationwide initiatives in each country can be categorized in terms of body's natures and roles as shown in the diagram below.[2] Note that the countries/regions picked up here are some of those in which digital credentials have been implemented in all or most universities/higher education institutions with interoperability in the country/region.

The operating organizations are classified by the following four categories (Table 1):

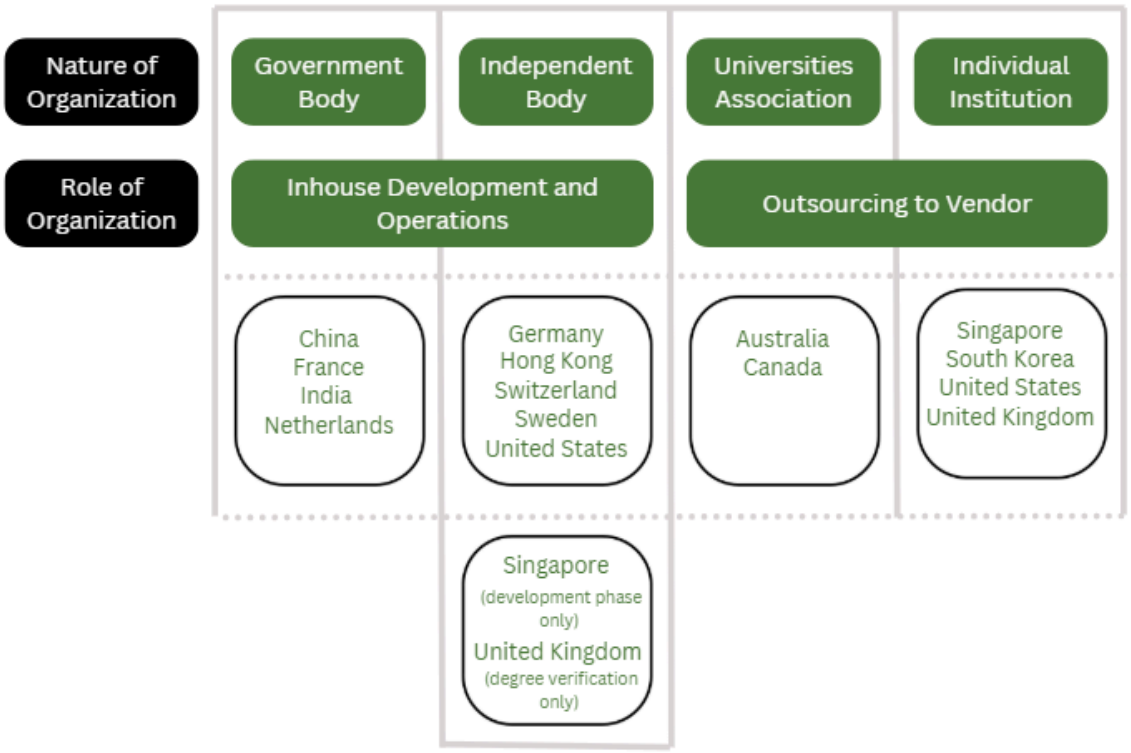
- Countries where existing or newly established *government* bodies take the national initiatives and centrally govern the digital credential platforms for higher education institutions across the country (such as China, France, the Nederland, and others)
- Countries where existing or newly established *independent* bodies take the national initiatives and centrally govern the digital credential platforms for higher education institutions across the country (such as Germany, Hong Kong, Switzerland, Sweden, and others for the entire digital credentials services, as well as only the verification service part of the UK and the US)
- Countries where the existing *college and/or university associations* take the national initiatives (such as Australia, Canada and others)
- Countries where each *individual educational institution* acts as the operating organization (such as Singapore, South Korea, the UK, the US and others)

[1] Note that digital exchange of learner data to support nation wide and province/statewide exchange began in the 70s with UCAS (UK) and OUAC (Canada).
[2] Information is this section (including the conclusions) is based on research conducted by K. Nakasaki in 2023/24.

There are two main role categories evident in Table 1. These include the following:

- countries in which the operating organization develops and operates the digital credential platforms in-house, and
- countries in which the operating organization selects a vendor and outsources the platform development and operations to the selected vendor.

Table 1 Organizational Landscape



Government Body

Below outlines the nature of each organization in countries where a government body is governing the national digital credential service (Nakasaki, 2023).

China: The Chinese digital credential platform, the Higher Education Qualification Database (service brand CHESI), is governed solely by CSSD (Center for Student Services and Development, Ministry of Education, P. R. China). The former name of this organization was CHESICC; it was originally established in 1991 under the Ministry of Education and was appointed as the operating organization of the Higher Education Qualification Database in 2001, followed by its launch in 2003. All universities (specifically, certified institutions) have student data stored at the CSSD, and all digital credentials are issued and verified through the CSSD's platform. CSSD is also developing and operating other services such as higher education entrance examinations, storage and management of student data, and employment support for graduates of higher education institutions.

France: The French digital credential platform (the service is branded Diplome.govu.fr) is developed and operated by the Ministry of National Education and Youth of the French government (Ministère de l'Éducation nationale et de la Jeunesse). Learning records of all higher education institutions in France are stored within the central depository of the ministry managed platform, and digital credentials are issued and verified through this same environment. In addition, some universities, such as the University of Lille, have independently implemented other digital credential services.

India: India's digital credential platform, National Academic Depository (NAD), was originally developed by University Grants Commission (UGC) which was designated as an authorized implementing body by the Ministry of Education (MoE) in 2016. The development was conducted with a tripartite agreement of UGC with NSDL Database Management Limited (NDML) and CDSL ventures Limited (CVL) for a period of three years to operationalize the NAD. NAD was launched in 2018 and afterward became DigiLocker, which was considered a flagship initiative of the Ministry of Electronics & IT (MeitY) under Digital India programme. It took over the role of implementation body in 2019. Most of universities in India store learning records on the NAD and digital credentials are issued and verified through the NAD.

Nederland: The Dutch digital credential platform, Diplomaregister, is developed and operated by DUO (Dienst Uitvoering Onderwijs), an education services agency commissioned by the Ministry of Education through its long history since its launch in 1996. All higher education institutions learning records are stored within the platform and digital credentials are issued and verified through this environment. DUO is also responsible for managing educational history data including scholarships and secondary education.

Independent Body

Below outlines the nature of each organization in countries where an independent body is governing the national digital credentialing service (Nakasaki, 2023).

Germany: 98% of universities and 95% of higher education institutions issue transcripts in PDF form, which is managed by each individual education institution in Germany. In addition, the Platform for International Mobility (PIM), a digital academic credentials platform, is developed and operated by the German Academic Exchange Service (Deutscher Akademischer Austauschdienst (DAAD)). As of the date of this research, DAAD was in the process of rolling the platform out to all German universities, a plan that started in 2021. As of January 2024, approximately 20% of German higher education institutions had implemented PIM.

Hong Kong: Hong Kong's digital credential platform, Academic Certificate Verification Platform (ACVP), is developed and operated by JUCC (Joint Universities Computer Centre), an organization voluntarily established by eight universities in Hong Kong for common IT resources and systems. ACVP was launched in 2022 and was in the process of being rolled out to all members of JUCC as of January 2024.

Singapore: OpenCerts, a development consortium consisting of the Government Technology Agency, the Ministry of Education, Ngee Ang Polytechnic, and SkillsFuture Singapore (SSG), has developed a digital credential software service with Blockchain architecture, which it launched in 2019. After the start of commercial operation, the

development and operation of the service has been moved out of this consortium and taken over by Singapore's higher education institutions' digital credential services which are commercially provided by Accredify, a private company.

Sweden: The Swedish digital credential platform was developed and is operated by the Ladok Consortium, an organization that develops and operates a joint student information system. The stakeholders of the Ladok consortium are 37 Swedish universities and one government agency. The Ladok consortium covers 99.5% of student data in Sweden.

Switzerland: Switzerland's digital credential platform, edu-ID, was developed and is operated by Switch, a foundation established by Switzerland's eight autonomous university cantons for the purpose of developing and operating an education and research network with the UNESCO SDGs as its guiding philosophy. Approximately 70% of Swiss universities have implemented edu-ID. Some universities have also implemented their own digital proof of study software services.

United Kingdom: In the UK, 98% of the UK universities' degree data are accumulated by an organization called Jisc which is now providing verification services through the Higher Education Degree Datacheck (HEDD), to employers and other verifiers. Jisc is a non-profit corporation with membership including from higher education and research institutions in the UK and is focused on developing and operating the genome database and other commonly used information systems. It has been funded by the Office for Students (OfS) for development of HEDD for the first two years in 2011 and shifted to self-funding after the launch of HEDD in 2013. While the degree verification service is centrally managed by Jisc, issuing digital credentials are managed by each individual education institution.

United States of America: In the US, 97% of higher education institutions store degree data at a warehouse of the National Student Clearinghouse (NSC); it provides verification service to employers, government, and other verifiers for degrees on a free of charge basis since 1999. NSC is a non-profit organization voluntarily established in 1993 by several higher education institutions. While the verification service is mostly centrally managed by the NSC on non-profit basis, issuing digital credentials is managed by each individual education institution with NSC's sharing and interoperability alleviating work burdens for these same organizations.

University/College Associations

The nature of each organization in countries where a university/college association is governing the digital credential are described below.

Australia: Australia's digital credentials platform, My eQuals, is managed by HES (Higher Education Services PTY), a consulting subsidiary of the Federation of Australian Universities. HES was appointed as the management organization for digital credentials in 2016. In 2016, HES conducted an international bidding process to select a vendor to which operational outsourcing could be established for the digital credential service. It launched My eQuals in 2017 and in 2018 the roll-out of all universities in Australia and New Zealand was completed.

Canada: Today, Canada's digital credentials platform, MyCreds | MesCertif, is managed by ARUCC (Association of Registrars of the Universities and Colleges of Canada), a not-for-profit organization comprised of registrars of universities and colleges of all provinces and territories in Canada. ARUCC responded to a consortium call and research to establish a national credential exchange network that was originally led by expert volunteers,[3] and, over time, drew in the support, contributions, and efforts of the Canadian Postsecondary Electronic Standards Council (CanPESC), the Council of University Chief Information Officers (CUCCIO), the Pan-Canadian Consortium on Admissions and Transfer (PCCAT), and government funding agencies from across Canada that supported the research and evolution (Duklas, 2023, 2024). The research and consultation for this initiative began in 2014 and was directly inspired by the GDN Network. In December 2019 and with the support of this consortium, ARUCC conducted an international bidding process to select a vendor for outsourcing the national digital credential platform operation. In June 2020, Digitary, which subsequently was purchased by Parchment and then Instructure, was the winning firm with Duklas Cornerstone Consulting Inc. tasked with leading the creation and set up of the network for ARUCC. In November 2020, MyCreds | MesCertif launched with its first institution, the University of Lethbridge, supported in advance by the early pilots which included the Toronto Metropolitan University (formerly Ryerson University) and Seneca College. This network is now serving close to two million learners, has been rolled out to support Canadian government issuers and close to 200 colleges, universities, and Indigenous Institutes, and is part of the My eQuals international network supporting approximately 10 million transactions every year.

Individual Education Institution

In this model and as mentioned above in the other examples, the issuing of digital credentials is managed by each individual education institution, while credential verification services are mostly centrally managed by Jisc and NSC respectively in the US and UK examples.

In Singapore, as mentioned above, the post-development digital credential platform is managed by each individual education institution while the development phase of OpenCerts was conducted by the consortium.

In South Korea, both issuing and verification services are managed by each individual education institution, and almost all higher education institutions deployed the software services of either of I&Tech or DigitalZone. Both these vendors interface the digital credential software services with the government's digital administration service called "Government 24".

[3] This early work beginning in 2014 was led by Kathleen Massey (former GDN board president), with support from Charmaine Hack (current GDN Board vice president), and Joanne Duklas (current executive director of the GDN; former executive lead of MyCreds) as volunteers from Canada. Several other volunteer experts in Canadian higher education from ARUCC, CanPESC, CUCCIO, and PCCAT supported the early research and work that led to the creation of what eventually became known as the ARUCC MyCreds | MesCertif National Network (Duklas, 2023, 2024).

4.2 PRIVACY GOVERNANCE MODELS

As mentioned in the previous section, 5.3 billion people and businesses that continue to move their information exchange and economic transactions into global cyberspace are also the end users on the receiving end of academic credentials.[4]

Credentials, which can only fulfil their role when they are trusted by end-users, can effectively function in line with the mechanisms of trust widely used in the economic society. The mechanisms of "trust" in the cyberspace have already been legislated internationally through the European eIDAS (Electronic Identification, Authentication and Trust Services) and its equivalent legal systems in many counties. The mechanism of privacy has been legislated through mutual recognition and international cooperation between Europe's General Data Protection Regulation (GDPR,2018) and many countries. In the Asia-Pacific Economic Cooperation Organization, the APEC Cross-border Privacy Rule (CBPR) has been adopted as the framework of the Data Free Flow with Trust (DFFT) in the Asia-Pacific Economic Cooperation. In an economic society where global information exchange and economic transactions transcending physical space in cyberspace have become the speed of people and businesses, academic credentials can also be effectively made to work only using trust mechanisms in those adopted systems and frameworks in the cyberspace.

Although international collaboration is underway, currently, there are different legal systems in different countries, which the users of digital platforms access from all over the planet. This creates some tension regarding which country/region's laws and privacy regulations (for example) should govern these networks.

As a practical resolution for it, many organizations have adopted the idea of complying with the European GDPR, which has a broader concept of privacy and a large learner population across multiple jurisdictional areas. This approach appears to work effectively for credential digital platforms.

Taking GDPR compliance one step further into the legal system, a significant concern arises regarding who will be designated as the Controller, as defined by the GDPR. The GDPR defines the Controller, along with its counterpart, the Processor (2018).

- Controller: A natural person, legal entity, public authority, administrative agency or other body that, alone or jointly with others, determines the purposes and means of processing personal data (Article 4, item 7).
- Processor: A natural person, legal entity, public institution, administrative agency, or other entity that handles personal data on behalf of the controller (Article 4, Item 8).

Determining which entity is the Controller can lead to substantial cost management challenges, particularly when dealing with data sharing among different entities.

An overview of the forms of privacy governance of digital platforms in terms of which entity takes on the Controller role can be typified as follows (Nakasaki, 2023):

- Central Repository

[4] The research in this section is provided by K. Nakasaki (2023/24).

- Switching Network
- Hub and Spoke

Central Repository

The central repository is a privacy governance form in which student records from universities across the country are accumulated in a data warehouse run by an operating organization, and the operating organization of this central data warehouse is the Controller. A benefit of this form is realized by concentrating the system on one management organization, which results in cost and operational burdens on each issuing organization being potentially lower than other forms. Among the countries/regional examples mentioned earlier, the verification services operating in the United States and the United Kingdom, and the national digital credential platforms of China, Germany, France, Switzerland, the Netherlands, and Sweden have adopted this form of privacy governance.

Exchange Network

The exchange network is a privacy governance form in which many operating institutions and individual universities are connected as access points to exchange data. Each access point will jointly govern privacy i.e. to be the Controllers. This form is used to connect institutions that operate in a centralized manner, such as the Netherlands and Sweden.

Hub and Spoke

Hub and Spoke is a privacy governance form in which each educational institution takes the privacy responsibility i.e. to be the Controller. Compared to other forms, the benefit of this form is reliability and efficiency because failure points such as personal information leakage are dispersed. Australia and Canada appear to have adopted this form of privacy governance for the respective national platforms. Most of the institutions in the UK and US appear to have adopted this form for issuing credentials by using commercial vendors selected by each institution.

4.3 INTEROPERABILITY

Interoperability is defined as "exchangeability between a range of products, or similar products from several different providers, or even between past and future revisions of the same product" (Chakroun et al, 2018). Interoperability schemes that are currently in widespread use worldwide that could be considered best practice in digital credentialing are as follows:[5]

- PDF Digital Signature
- XML Data Scheme
- OpenBadge 3.0
- Verifiable Credentials

Of these, PDF digital signatures are the most commonly adopted scheme for degree-related credentials (macro-credentials), followed by XML data format; both

[5] The research in this section has been provided by K. Nakasaki (2023/24).

methods are currently used to support international interoperability. For micro-credentials, OpenBadge 3.0 appears to be the most used. The Verifiable Credentials Data Model (VC) has gained momentum in the last few years, especially in Europe, where major projects have been launched, but operational use is limited as of May 2024.

PDF Digital Signature

PDF Digital Signature is a mechanism for digitally signing PDFs. PDF is used by everyone in the world, and enables extensive interoperability between different hardware, operating systems, and applications. PDF Digital Signatures have been legislated in many countries (e.g. eIDAS in Europe, e-sign laws in the US) and adopted in many fields such as software distribution, financial transactions, and contracts.

It is also the most widely used interoperability scheme in the digital credential field. Of the 14 countries/regions covered in the previous chapter, the following countries' national digital credential platforms have adopted PDF digital signatures as an interoperability scheme for degrees, grades, proof of enrollment, etc. (macro-credentials):

- Australia
- Canada
- China (mainland)
- France
- The Netherlands
- Sweden

In the following countries, where vendor selection is conducted by individual education institutions, PDF Digital Signatures have been most adopted as an interoperability scheme for degrees, transcript, proof of enrolment, etc. (macro credentials):

- Germany
- United Kingdom
- United States

XML Data Scheme

Although PDF Digital Signatures have become widely used around the world, PDF Digital Signatures by themselves only provide interoperability in the sense that they can be viewed and verified by humans. To achieve interoperability between systems, XML or JSON format data can be embedded in PDF, or XML data alone can constitute a digital credential. In such cases, interoperability requires data standards in order for the data format to be matched between the sending and receiving systems.

Efforts to standardize the data format have been made throughout the history of digital credentials. In the United States, the PESC (Post-secondary Electronic Standards Council), a voluntary organization, was established in 1997 to lead the standardization effort.

Toward the end of the 1990s, there was a growing momentum in Europe to ensure international interoperability. The European Emrex was the first to achieve such interoperability. Six European countries came together to define ELMO (European

Learner Mobility (ELM) + Metadata for Learner Opportunities (MLO)), an XML international interoperability scheme with interoperability for digital academic credentials between European countries. It was implemented in the Emrex network which went live in 2018. However, even within Europe, standardization of the XML format has not been achieved to date. For example, the UK government specified a national XML specification separately from ELMO in 2011.

In Europe, there has been little adoption of PESC XML standards, the most popular format in the United States and Canada. In the United States, there are currently six different XML digital academic transcript data formats in the country found by the researcher for this project. Overall, despite nearly 25 years of efforts to standardize XML data formats since the establishment of PESC, to date, no XML data format has been adopted as a global standard.

Among the countries/regions discussed in the previous chapter, the XML Data Scheme is adopted in the following countries:

- Australia: According to a very rough estimate, approximately half of the universities have adopted XML Data Scheme by attaching data to PDF Digital Signatures. Multiple data formats such as PESC are supported.
- Canada: The method of attaching XML data to a PDF Digital Signature is adopted by approximately half of the universities that have implemented digital credentials according to Nakasaki (2023/2024).
- China (mainland): The method of attaching XML data to PDF Digital Signatures is adopted by all universities. The data format is standardized to PESC.
- Germany: 98% of universities use PDF Digital Signature for transcripts. XML data format is rarely attached to them. On the other hand, the national digital credential platform of PIM adopts XML data and ELMO is used as the data format.
- France: It is externally assumed that the method of attaching data to PDF digital signatures is adopted, but the French government which operates the national digital credential platform appears to have not publicly disclosed the specifications. It is assumed that all universities use the same domestic proprietary system.
- The Netherlands: Both the method of attaching data to PDF Digital Signature and the method of XML data functioning standalone are adopted by all higher education institutions. The XML data format is standardized to ELMO.
- Sweden: All universities have adopted both method of attaching data to PDF Digital Signature and the method of XML data functioning standalone. The data format is standardized to ELMO.

XML Data Scheme is also adopted in the following countries where each individual education institution manages issuing services of digital credential platforms:

- UK: Higher education institutions that select vendors that use XML Data Scheme may use the XML Data Scheme as a result. The data format is not standardized, with national specifications set by the UK Department of Education and OpenBadge being used.

- USA: Higher education institutions that select vendors that use XML Data Scheme may use XML Data Scheme as a result. Data formats are fragmented, with six data formats, although PESC is the most widely adopted.

OpenBadge

Nakasaki (2023/24) proposes that the Open Badge standard offers a solution. Instead of seeking standardization through organizational explicit agreements, Open Badge has taken a strategy of directly driving individual learners' behaviors at the psychological level.

Open Badge is an interoperability scheme which 1EdTech (formerly IMS Global Consortium) takes stewardship for and is characterized by "visual digital tokens of achievement, affiliation, authorization or some other trust relationship sharable across the web" (Chakroun et al, 2018). It is conceived as an infrastructure that allows users to recognize acquired skills and accomplishments anytime, anywhere.

Above all, the specification of embedding the learning record in a PNG image matches the modern lifestyle that is motivated by social connections through SNS. When learners complete a course or obtain a certification, they can share their sense of accomplishment with society via Twitter and Facebook with the visual impact of an image (symbolizing the course). This has led to an explosion of OpenBadge technical specifications around the world. In this sense, it has arguably disrupted the "standardization" paradigm of XML data formats.

Since the launch of OpenBadge 1.0 in 2013, it has begun to be widely used by companies and educational institutions, MOOCs (Massive Open Online Courses), and others. Since OpenBadge 2.0 was finalized in 2018, the number of issued badges has increased from 24.1 million in 2018, to 43.4 million in 2020, and 74.7 million in 2022 (1EdTech 2022).

The OpenBadge community has also been participating in the Verifiable Credential Data Model (VC) use case described below since 2018 to improve the privacy and security features of the OpenBadge standard. In 2021 the IMS Global Consortium (now 1 EdTech) announced that the next version of OpenBadge (3.0) will be compliant with the Verifiable Credential Data Model (VC) and was released in 2024.

Blockchain Credentials

Blockcerts, first implemented at MIT in 2017, uses Bitcoin and open badges to issue degree credentials, allowing graduates to hold their own graduation credentials without relying on a hosting vendor and on a public ledger of blockchain credentials. The system is considered tamper-proof and immutable.

At the time of the launch of Blockcerts, an MIT official said that "all kinds of disasters can happen," and that linking academic credentials to the blockchain "allows people to actually own their identity documents without a single point of failure and without continuous dependence on the issuer or a specific vendor without a single point of failure and without ongoing dependence on an issuer or specific vendor," highlighting the benefits of Blockcerts (Schembri, 2018).

Today, this idea is also supported and promoted in terms of human rights issues such as the protection of the educational entitlements of refugees in the context of the UNESCO

Sustainable Development Goals (SDGs). In this sense, Blockchain is an interoperability scheme that is particularly conducive to lifelong and inclusive education.

Among the countries/regions mentioned in the previous section, the Hong Kong's digital credential platform ACVP has adopted the interoperability scheme of Blockchain credentials, and in Korea, where each educational institution serves as an operating agency, almost all higher education institutions have adopted blockchain credentials. In the United States, blockchain utilization has raised some questions around whether it can be used for education records due to a regulation known as FERPA, which requires further study (Family Education Rights Privacy Act).

Verifiable Credentials Data Model (VC)

The Verifiable Credentials Data Model is a technical specification for digital credentials defined and endorsed by the World Wide Web Consortium (W3C), a standards organization for Web technologies. Using this technical representation for credentials allows presentation and sharing of all of the same information that is typically found in passports, driver's licenses, and health insurance cards used in the physical space (photo, name, identification number, issuing authority, attribute information such as nationality and license type claimed by the issuer regarding the subject of the credential, validity period and conditions of use, etc.). It is a technical specification for digital credentials that suggested as delivering more reliable and tamper-proof support than physical credential documents and cards.

Verifiable Credentials function in a three-party distribution model consisting of an issuer (issuer), a holder (holder), and a verifier (verifier). Each of the three parties has verifiable attributes, such as a specific identifier, that are stored in a verifiable data registry for credentials, such as a database, distributed database, government identity database, or distributed ledger.

The holder makes a request to the issuer to issue credentials, holds the credentials issued by the issuer, generates a credential (presentation), and presents it to the verifier (present). The issuer stores the credentials claimed for the subject (holder) in the verifiable data registry and issues the credentials to the holder after confirming that the holder is a qualified person in response to the request from the holder. The verifier receives the credentials presented by the holder, verifies the authenticity of the credentials stored in the verifiable data registry using the identifiers of the issuer and the holder, etc., contained in the credentials, and processes the credentials into data.

The movement to adopt Verifiable Credentials (VC) for digital academic credentials is gaining momentum, especially in Europe and elsewhere in 2023. The European Commission (EC) has established a framework, eIDAS (Electronic Identification, Authentication and Trust Services Regulation), which specifies the legal and technical requirements and third-party assessments for "trust services" that guarantee the identity and authenticity of people and objects and that the data and content they handle have not been tampered with. Version eIDAS 2.0 has been adopted as a technical requirement (EC 2023). As part of this effort, the European Union Digital Identity Wallet (EUDI Wallet), which will be Europe's next-generation data infrastructure and available to all European citizens, is being built with a budget of about 90 million Euros (Norder, 2023; EC, 2023).

With regard to academic credentials, the Digital Credentials for Europe (DC4EU) was launched as one component of the EUDI Wallet project, with a grant budget of approximately 19.21 million Euros over two years. One of the grantees, Emrex, has already validated digital credentials platforms in 10 European countries (Croatia, Denmark, Finland, Germany, Greece, Italy, the Netherlands, Norway, Poland, and Sweden) that are currently connected to the network. The development of connecting digital academic transcript platforms in 10 European countries (Croatia, Denmark, Finland, Germany, Greece, Italy, Netherlands, Poland, and Sweden) to the Verifiable Credentials (VC) system is underway, with practical operation scheduled to begin in 2024 (Norder, 2023).

In Singapore, Accredify mentioned previously was working as of the date of this research to update its service to be compliant with the Verifiable Credentials Data Model (VC). In Australia and Canada, the digital academic credentials network described earlier has already implemented the ability to issue micro-credentials with VC if the end user (Holders/learner) chooses to do so which results from work funded by the Ontario government in Canada and the efforts of the Duklas Cornerstone, Instructure, and MATTR teams responsible for creating this expansion to the MyCreds network (Hack et al, 2023, Duklas, 2024).

5. TECHNOLOGICAL UNDERSTANDING IN CIVIL SOCIETY

The rapid advancement and integration of technology in data collection and analytics, particularly within educational and employment contexts, have outpaced the general public's understanding of these systems. Civil society often lacks comprehensive knowledge about the mechanisms of data collection, the intricacies of data analytics, and the broader implications of these technologies on privacy and personal data security. This knowledge gap poses significant challenges in fostering informed consent and meaningful engagement with data privacy practices (Smith, 2020).

Research demonstrates that while there is an increasing awareness about data privacy issues, the depth of understanding regarding the technologies that drive data collection and analysis remains limited among the general populace (Jones et al, 2019). Consequently, individuals may not fully comprehend the extent to which their data is being utilized, potentially leading to uninformed decisions about data sharing and consent (Brown et al, 2021). This gap underscores the necessity for targeted educational initiatives and transparent communication from institutions that collect and use data, to bridge the understanding between technological practices and their societal implications (EDUCAUSE Review, 2021).

Moreover, the complexity of data privacy frameworks and the fast-evolving nature of digital technologies necessitate a concerted effort to enhance public literacy in data ethics and privacy as mentioned in the case of the United States with the Family Education Rights Privacy Act (FERPA). By empowering communities with knowledge and tools to navigate the digital landscape, we can promote a more informed and engaged civil society capable of advocating for their data privacy rights (Hoel et al, 2017).

has been convening collaboration globally in the last few years and is therefore an ideal place to continue playing a co-ordinating role of engagement, inclusion of communities, and empowering citizens regarding their rights to the protection of their data on interoperable digital platforms for work and learning.

Central to the notion of individual agency in data privacy is the principle of informed consent, where individuals should have the autonomy to make informed decisions about the collection, storage, and utilization of their personal data. However, there are exceptions, such as in cases involving federal supports, fraud prevention, or the prevention of misrepresentation, where certain data may need to be managed with less direct consent to ensure broader public safety and integrity. While several digital platforms have been transparent regarding the purposes for which data is collected, as well as the ability for individuals to opt-in or opt-out of data processing activities, a governance framework to support digital platforms for work and learning is well positioned to highlight the importance of these matters related to privacy.

Robust legal and regulatory frameworks have been essential for upholding individuals' rights to data privacy and fostering a culture of accountability among data controllers. Legislation such as the General Data Protection Regulation (GDPR) in the European Union, the California Consumer Privacy Act (CCPA) in the United States, and the Protection of Privacy of Information Act (POPIA) in South Africa are examples that

establish clear rights and obligations concerning data protection, empowering individuals to assert their privacy rights and seek recourse in the event of data breaches or privacy violations. Jurisdictions that have a plethora of privacy regulations tend to lead to a patchwork of regional laws, which creates significant obstacles for data portability, making it challenging for individuals and businesses to navigate and comply with varying standards across the country.

Beyond legal compliance, ethical considerations should underpin efforts to develop individual agency in data privacy. Organizations and policymakers through governance frameworks are encouraged to prioritize ethical data practices, respecting individuals' autonomy, and ensuring that data collection and processing activities align with principles of fairness, transparency, and accountability. While individual agency is critical, collective action and advocacy are also essential for driving systemic change in the realm of data privacy. Individuals, civil society organizations, and advocacy groups can mobilize to advocate for stronger privacy protections, hold policymakers and corporations accountable, and shape the trajectory of data governance to prioritize individual rights and freedoms and the GDN remains a central stakeholder to initiate such an advocacy strategy through its governance framework efforts for credential exchange to address the need for widespread knowledge sharing in this regard.

5.2 A RECOMMENDED STRATEGY FOR CITIZEN AGENCY

By addressing these key points in a future governance framework suggested for creating and sustaining digital credential ecosystems, the GDN can articulate a compelling argument for the importance of developing agency of individuals regarding their rights for data privacy, laying the groundwork for further exploration and action in this critical area. To build agency among communities regarding the privacy of their data, a multifaceted strategy should be considered when creating a governance framework for credential exchange network use. Additionally, network leaders considering creating or leading credential exchange environments will want to build into their governance frameworks initiatives to build knowledge amongst their communities which might include raising awareness about data privacy issues and rights. Workshops, seminars, and online courses can be developed to inform community members about the types of data being collected, the purposes for which it is used, and the potential risks associated with data breaches and misuse. By empowering individuals with knowledge, communities can better understand the implications of data sharing and develop informed opinions on privacy matters.

The second component of the strategy involves the implementation of robust data protection policies and practices within educational institutions and workplaces. These entities must adopt transparent data collection and usage policies, ensuring that learners are fully informed about how their data will be used and for what purposes. Additionally, institutions should provide opt-in and opt-out options, allowing learners to exercise greater control over their personal information. Regular audits and assessments of data management practices should be conducted to identify and mitigate potential vulnerabilities. By establishing clear and stringent data protection protocols, institutions

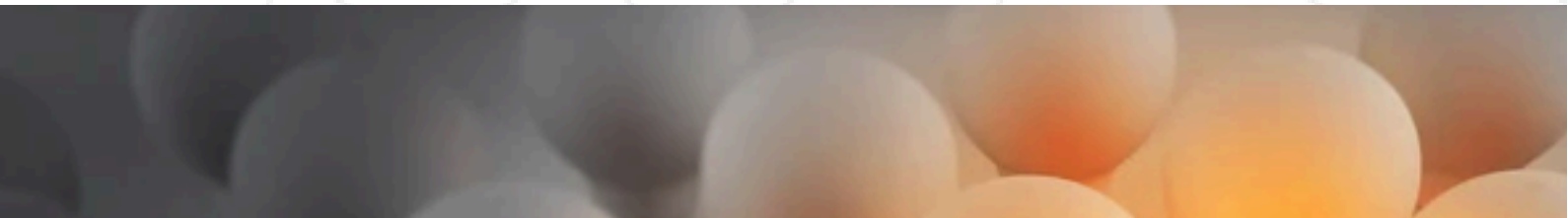
can foster a culture of trust and accountability, thereby enhancing community agency over data privacy.

Finally, fostering community agency requires active participation and collaboration between all stakeholders, including learners, educators, employers, and policymakers. Establishing forums and platforms for dialogue can facilitate the exchange of ideas and concerns related to data privacy. Community advisory boards comprising representatives from various stakeholder groups can be formed to oversee data privacy initiatives and advocate for the rights of learners. Additionally, policymakers must be engaged to develop and enforce regulations that protect learner data and promote ethical data usage. Through collective action and sustained advocacy, communities can ensure that their data privacy concerns are addressed, leading to more equitable and responsible handling of learner data by employers and higher education institutions.

6. CONCLUSION

In conclusion, the intersection of global migration, technological advancements, and the rise of digital credentialing platforms presents both opportunities and challenges when considering a governance framework for creating and sustaining digital credential ecosystems. This research confirms that the ability of digital platforms to facilitate the seamless sharing and verification of educational credentials across borders underscores the need for robust policies and standards that ensure ethical data governance. The paper highlights the challenges and ethical considerations, such as data privacy, ownership, and governance, that need to be addressed for successful implementation. As migration trends continue to rise, particularly in the context of forced displacement, it is crucial to address these challenges.

Moving forward, the development of a global governance framework that prioritizes transparency, fairness, and inclusivity is imperative. By fostering widespread collaboration and community engagement, we can ensure that these platforms not only support mobility but also uphold the principles of ethical governance, creating a more equitable and interconnected global society in shaping the future of credentialing platforms.



REFERENCES

Avelino-Silva et al, 2023: Avelino-Silva, T.J., Trujillo, N., and Chinedu Udeh-Momoh, C. Fairness: from the guts to the brain – a critical examination by Atlantic fellows of the Global Brain Health Institute. Frontiers in Psychology 19 October 2023 Volume 14 - 2023.

Brandes et al, 2017: Brandes, L and Darai, D. The value and motivating mechanism of transparency in organizations. European Economic Review Volume 98, 2017, Pages 189-198.

Brosnan et al, 2014: Brosnan, S. F., and de Waal, F. B. (2014). Evolution of responses to (un)fairness. Science 346:1251776. doi: 10.1126/science.1251776

Brown et al, 2021: Brown, A., & Adams, P. (2021). Understanding Data Privacy: Challenges and Opportunities. Journal of Technology and Society, 15(2), 134-150.

Chakroun et al, 2018: Chakroun, B. & Keevy, J. Digital Credentialing Implications for the recognition of learning across borders. UNESCO. 2018.

Yoder et al, 2014: Yoder, K.J. & Jean Decety, J. The Good, the Bad, and the Just: Justice Sensitivity Predicts Neural Response during Moral Evaluation of Actions Performed by Others. Journal of Neuroscience 19 March 2014, 34 (12) 4161-4166.

Deloitte, 2022: Deloitte. Accessing Global Talent – Embracing The New Era. 2022. https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/tax/deloitte-uk-accessing-global-talent-v08.pdf

Di Martino et al, 2020: Di Martino, S., & Prilleltensky, I. (2020). Happiness as fairness: The relationship between national life satisfaction and social justice in EU countries. J. Community Psychol. 48, 1997–2012. doi: 10.1002/jcop.22398

diplome.gouv.fr 2024: https://diplome.gouv.fr/sanddiplome/perimeter

Duklas, 2023: Recognition and technology: Considering a trust framework for learner mobility. In S. Eaton & J. Carmichael (Eds.). Fake Degrees and Fraudulent Credentials in Higher Education. Springer.

Duklas, 2024: Considering the Dimensions of Trust, Privacy, and Technology Innovations to Enable Quality-Assured Credential Assessment Practice. In: Eaton, S.E. (eds) Second Handbook of Academic Integrity. Springer International Handbooks of Education. Springer, Cham. https://doi.org/10.1007/978-3-031-54144-5_149

EC, 2023: European Commission. The European Digital Identity Wallet Architecture and Reference Framework. Published 10 February 2023. https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-wallet-architecture-and-reference-framework （2023/12 access）

EDUCAUSE Review, 2021: Data Privacy in Higher Education: Yes, Students Care. Retrieved from EDUCAUSE

GDPR, 2018: Retrieved from General Data Protection Regulations: https://gdpr.eu/

Hack et al, 2023: Claire Barber, Charmaine Hack, Nader Helmy. Designing for Trust. Groningen Declaration Network 2023 Annual Meeting in Amman. October 2023. https://groningendeclaration.org/video-library/ （2023/10 access）

Hadziahmetovic et al, 2022: Hadziahmetovic, N., & Salihovic, N. (2022). The Role of Transparent Communication and Leadership in Employee Engagement. International Journal of Academic Research in Economics and Management and Sciences. 11(2), 558 - 571.

Hindman, 2022: Matthew Hindman. The Internet Trap: How the Digital Economy Builds Monopolies and Undermines Democracy (Japanese version). Diamond Publishing. 2022.

Hoel, T. et al, 2017: Privacy and data protection in learning analytics. Research and Practice in Technology Enhanced Learning. Retrieved from Springer Open.

Insider Intelligence, 2022: Ethan Cramer-Flood. Global Ecommerce Forecast & Growth Projections: As 2-Year Boom Subsides, Plenty of Bright Spots Remain. Insider Intelligence. Feb 2, 2022.
https://www.insiderintelligence.com/content/global-ecommerce-forecast-2022

JICA, 2016: Japan International Cooperation Agency. Introduction to the Psychology of International Cooperation. August 2016.
https://www.jica.go.jp/Resource/english/our_work/thematic_issues/agricultural/shep/c8h0vm0000bm5ayp-att/introduction_en.pdf

Jones, M. et al. 2019: Public Understanding of Data Privacy Technologies. Data and Society Journal, 8(3), 201-219.

Levinson 2022: Levinson, M. Outside the Box: How Globalization Changed from Moving Stuff to Spreading Ideas (Japanese Edition). Diamond Publisher. 2022.

McAuliffe et al, 2017: McAuliffe, K., Blake PR., Steinbeis N., & Warneken F. The developmental foundations of human fairness. Nat Hum Behav. 2017;1:0042.

McAuliffe et al, 2021: McAuliffe, K. & Triandafyllidou, A. (eds.) (2021). World Migration Report 2022. International Organization for Migration (IOM), Geneva

Melé et al, 2013: Melé, D., & Sánchez-Runde, C. Cultural Diversity and Universal Ethics in a Global World. J Bus Ethics 116, 681–687 (2013).
https://doi.org/10.1007/s10551-013-1814-z

Moazed et al, 2016: Moazed, A. & Johnson, N.L., Modern Monopolies: What It Takes to Dominate the 21st-Century Economy (Japanese Version). Eiji Publishing. 2018.

Norder, 2023: Norder, J.J. EMREX in your wallet. Groningen Declaration Network 2023 Annual Meeting in Amman. October 2023.
https://groningendeclaration.org/video-library/（2023/10 access）

Rajab et al, 2023: Rajab, R. & Ntuli, S. (2023). A deep dive into governance mechanisms for interoperable digital platforms for work and learning. Johannesburg: JET Education Services.

Scarpa et al, 2021: Scarpa, M. P., Di Martino, S., & Prilleltensky, I. (2021). Mattering mediates between fairness and well-being. Front. Psychol. 12:744201. doi: 10.3389/fpsyg.2021.744201

Schembri 2018: Schembri, F. Digital diplomas: Blockchain technology gives grads control over their academic credentials. MIT Technology Review. April 25, 2018. https://www.technologyreview.com/2018/04/25/143311/digital-diplomas/（2023/12 access）

Smith, 2020: Smith, J. (2020). Technological Literacy and Data Privacy in the Digital Age. International Journal of Digital Ethics, 12(1), 45-62.

Smolenski, 2016: Smolenski, N. (2016). Why the Blockchain will Revolutionize Academic Credentialing. Educause, October 22, 2016, Anaheim, CA

Sun, 2013: Sun, L. (2013). The Fairness Instinct: The Robin Hood Mentality and our Biological Nature. (New York, United States: Prometheus Books).

Tucker, 2020: Tucker, P.L. (2020). 25 Reasons to Study Abroad. TOP UNIVERSITIES. Retrieved from https://www.topuniversities.com/blog/25-reasons-study-abroad

UNEG, 2020: United Nations Evaluation Group. Ethical Principles for Guidelines for Evaluation. United Nations Evaluation Group. 2020. https://www.unevaluation.org/document/detail/2866

UNESCO, 2023a: UNESCO. Guidelines for the governance of digital platforms: safeguarding freedom of expression and access to information through a multi-stakeholder approach. 2023. https://unesdoc.unesco.org/ark:/48223/pf0000387339

UNESCO 2023b: UNESCO. International trends of lifelong learning in higher education: research report. June 2023. https://epale.ec.europa.eu/en/resource-centre/content/international-trends-lifelong-learning-higher-education-research-report-1 （2023/12 access）

UNESCO, n.d.: UNESCO (n.d.). https://www.unesco.org/en/higher-education/global-convention

UNHCR, 2024: Refugee Data Finder. UNHCR. unhcr.org/refugee-statistics/ (Accessed 24 March 2024)

WEF, 2023: World Economic Forum. Future of Jobs Report 2023 Insight Report. May 2023. https://www.weforum.org/publications/the-future-of-jobs-report-2023/（2023/12 access)