Digital Transformation of Education Credential Processes and Life Cycles — A Framework of Research Questions Based on the Main Challenges

Ingo R. Keck
Scientific Data Management
TIB Leibniz Information Centre
for Science and Technology
Hannover, Germany
Email: Ingo.Keck@tib.eu

Maria-Esther Vidal
Scientific Data Management
TIB Leibniz Information Centre
for Science and Technology
Hannover, Germany
Email: Maria.Vidal@tib.eu

Lambert Heller
Open Science Lab
TIB Leibniz Information Centre
for Science and Technology
Hannover, Germany
Email: Lambert.Heller@tib.eu

***Abstract*—This article describes the challenges that arise in the using and managing education credentials, and from the switch from analogue paper-based education credentials to digital education credentials. We analyse the available literature and notice that this transformation—from paper to digital for education credentials—has not been the focus of research so far. Using an approach based on the use cases and identified challenges, we propose a general methodology to capture qualitative descriptions and measurable quantitative results that estimate the effectiveness of a digital credential management system in solving these challenges. This methodology is applied to the European Union Horizon 2020 project QualiChain use case, where five pilots have been selected to study a broad field of digital credential workflows and credential management. It can form the basis of a future framework that will capture the whole life cycle of educational credentials, from creation, storage, management, access control, till it expires or is retracted.**

Keywords–Credentials; Education credentials; Digitisation; Challenges in digitisation; Digital Badges.

I. INTRODUCTION

Education and academic credentials are an essential part of our modern life. Pupils finalise schools with a set of marks certified on their final school report. Then, based on these results, they can apply for acceptance at higher education institutes or apprenticeship. Students and employees continue to collect credentials at university, at work, or via other education ways. Even today, when digitisation has entered into almost every part of our lives, education credentials are still often printed and written on paper. A transformation to digital workflows seems desirable to take advantage of the additional possibilities of digital certificates. However, such a transition is not without challenges. In [1], we first looked at these challenges and presented a proposal for a framework to evaluate credential management systems that support digital credentials transformation. This article now builds on and extends [1] by adding to the initial reasoning and providing an overview of related works.

Paper-based credentials show several problems in practice. For example, when applying for a job position, the handling of paper based credentials is tiresome for the applicant and even more so for the company that offers the position. Indeed, most companies nowadays require scans of the paper credentials, and will only check the validity of the originals once the candidate for the position has been selected, to avoid the manual labour involved. Additionally, surveys show that lying about education and employment credentials is a common problem. According to a survey by CareerBuilder [2], 58% of employers have caught a lie on a resume. Similar findings arise from another recent survey by StatisticBrain [3], which reports that over half of resumes and job applications (53%) contain falsifications and over three quarters (78%) are misleading. Digitisation of education credentials has the potential to make credential handling both easier and more secure. Nevertheless, it is important to ask the correct questions to be able to investigate how well a solution performs in the implementation and management of digital education credentials.

Everhart et al. define in [4] important key terms and concepts regarding digital badges, that we believe can be extended to credentials in general:

- *Authentication*: Certifies that a credential is authentic, i.e., has been awarded according to the standards referred to by the credential.
- *Authorisation*: The issuer of a credential has the power to issue the credential. This power can be certified by a trusted third party, usually the government where the issuer is based, or a well trusted public organisation.
- *Endorsement*: Other parties can endorse a credential, i.e., signing the credential, confirming its validity and thus adding trust to the content of the credential.
- *Validation*: Validation refers to the value a credential holds in the education ecosystem, i.e., how do the consumers of the credential interpret its value?
- *Verification*: Verification tests if the credential is genuine and has not been falsified.

As Room notes in [5], setting the standards in education, and thus, defining each credential's value, is a social policy issue and decided on a political level. Technology cannot be used solely to solve this problem. However, the combination of easily accessible background information as open data about the educational standards references in a credential, together with semantic information in digital credentials that make the access to this information accessible and immediate, can significantly increase the transparency in this field. This also has the potential to facilitate the labour intense practice of cross-country credential equivalence estimations, up to the point where this could be done automatically, once the background information supplies enough detail.

Looking at frameworks to measure digitisation in the economy, it appears that credentials have not been in focus so far. In [6], Kotarba gives an overview of standard digital economy metrics like the Digital Density Index (DDI) by Oxford Economics and Accenture, the Digital Economy and Society Index (DESI) by the EU commission, and Digital Society Metrics as part of OECD's digital economy measurement system. None of them refer to credential management as far as we can see.

The main contribution in this article is to present the main challenges encountered in education credential management and usage, and the changes from analogue to digital credential workflows. We propose specific questions that will allow a qualitative and quantitative assessment of the performance of a credential management system and infrastructure regarding these challenges (given in Table I). Finally, we introduce the use case of the EU Horizon 2020 project QualiChain [7], where these research questions will be evaluated with the help of the participants in the project's pilots.

The article is organised as follows: Section II presents different challenges encountered while analysing the reports and questionnaires provided by the QualiChain pilots. In Section III, we propose a set of questions for every challenge presented in the previous section. In Section IV, we offer the use case of QualiChain. In Section V, we give an overview of relevant related work. The article closes with Section VI, where our conclusions and future work are outlined.

II. Challenges in Education Credential Management

How can a solution offering the issuing, management, and verification of digital education credentials be evaluated? Two ways appear natural to approach this question: One can either start looking at it from the user perspective—where the users are the issuers, the holders, and the consumers of the credentials—or follow the switch from the well-established handling of paper-based credentials to digital credential management and look at all the challenges that appear. Both ways are of equal validity and should arrive at the same results. Based on the results acquired in [8], we noted that the overlap in requirements between credential issuers, credential holders, and credential consumers is substantial and that it seems more adequate for the investigation of the digital transformation of the education credential process and life cycles to follow the process of changing from an analogue to a digital setting. We, therefore, propose to segment the questions of interest into three subtopics:

- Challenges of paper-based credentials;
- Challenges of transition to digital credentials; and
- Challenges of digital credentials.

In the following sections, we deduce and present these difficulties and propose ways how to measure the performance of a presented solution for the implementation and management of digital education credentials. Figure 1 gives an overview of the complex of challenges.

A. Challenges of Paper-Based Credentials

Paper-based credentials are the state of the art and have a history dating back to medieval times. Their use over centuries makes it evident that, before digitisation, they were widely seen as the best solution. However, the developments in the last decades and the move to digital workflows increased the pressure on analogue, paper-based credentials and led to growing problems, especially in fraud prevention.

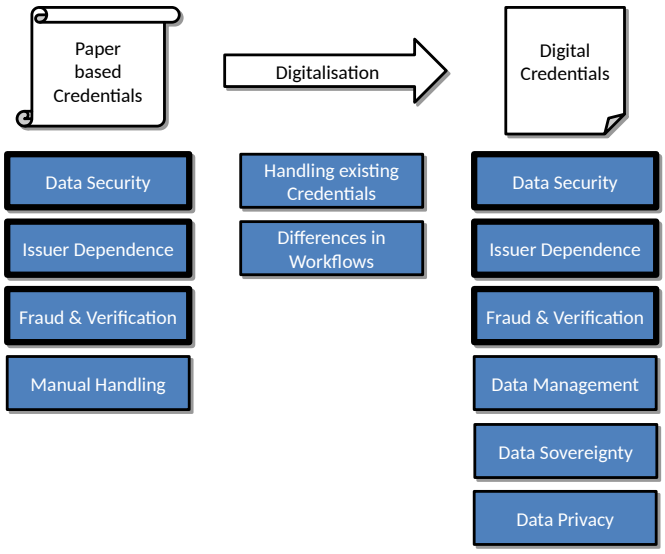

Figure 1. Challenges in the digital transformation of education credential processes and life cycles. Paper based credentials, the digitisation process itself, and digital credentials each are sources of specific areas of problems that are presented as darkly coloured boxes. It can be seen that both digital and paper based forms share a set of common challenges (thick outline).

1) Fraud and Verification: Advances in digital printing make it continuously more difficult to protect paper-based credentials against fraud. As already mentioned, a survey by CareerBuilder [2] reports that 58% of employers have caught a lie on a resume and 33% of them have seen an increase in resume embellishments and fabrications like embellished skill sets (57%), heightened responsibilities (55%), dates of employment (42%), job titles (34%), academic degrees (33%), companies worked for (26%) and awards (18%). A different survey [3] states that over half of resumes and job applications (53%) contain falsifications, and over three quarters (78%) are misleading. Most issuers do not have the capabilities to use advanced falsification protection in their paper credentials, compared to what is done, for example, for paper-based money. Without a general standard, it would also be impossible for a non-expert to decide if the credential in front of him/her has the correct characteristics. There are over 3,000 higher education establishments in the European Union alone [9]. Instead, institutions and states commonly register necessary credentials and allow interested individuals to inquire about a presented credential's validity. The UK, for example, offers the Higher Education Datacheck service [10]. The use of this service is chargeable, and the process can take up to seven days [11]. The process is also highly manual and time-consuming.

2) Dependence on Issuer: The problems with fraud make it challenging to issue education credentials for anyone else other than official education establishments. This leads to the issue that learners will be unable to furnish sufficient and incontestable proof over several types of qualifications gained outside this established system. In the job market, written recommendation statements (also easily to falsifiable)

or contact persons of reference are used to compensate for this. These methods are also manual and time costs for the people involved. The challenge to correctly identify the issuer of such statements is related to this problem. Additionally, this can be why direct access to contacts for reference is often preferred. In this case, the authenticity of the reference can be checked by other means, like contact over official phone numbers, personal knowledge, or email addresses.

3) Handling: Paper-based credentials are easy to handle and store for the bearer. Still, in situations where many credentials have to be collected, screened, and analysed, the high manual handling costs make their use expensive. This leads to a time consuming and costly labour intense recruitment process. For staffing private and most public sector organisations, it can be challenging to efficiently handle competency management in large organisational structures. This observation is supported by the outcomes of our questionnaire collection at the QualiChain pilots.

4) Data Security: Paper-based documents have successfully been archived over many decades using high-quality, acid-free paper, storage in low humidity and room temperature in pest-free environments. Additionally, data protection can be enforced by physical access restrictions that are commonly available and do not require specialised information technology (IT) skills. However, most users of paper-based credentials outside of official archives and libraries lack the means of long-term storage, which makes paper-based credentials vulnerable to loss and damage. This is made more severe by the impossibility to create identical copies of paper-based credentials. In this context, it is interesting to note that digitisation in libraries often captures more than just the works' content. Further, digitisation is not seen as a substitute for archiving the works, but as an additional effort to make them readily available and keep at least part of the contained information safe from physical decay [12].

B. Challenges of Transition to Digital Credentials

Any solution that asks users to move from a well-established analogue paper-based workflow to a digital workflow will face challenges in this transition. Furthermore, how well the solution solves these issues will determine how well the users will receive it. In the following points, we present the problems we encountered mentioned in our data collection.

1) Digitisation of Existing Credentials: Analogue credentials are put into existence using written text, images, drawings, and security characteristics in various forms. To retain all this information in digital form is difficult. To efficiently work with the content of the credential, it is necessary to convert the unstructured text, e.g., gained by a scan of the document, into structured data that has been semantically enriched.

2) Interaction Between Analogue and Digital Workflows: While workflows for both digital and analogue paper-based credentials exist, it is desirable to cater to both types. The users' transition is seamless and can import paper-based credentials to take advantage of the added possibilities of digital workflows. These transitions will often mean making manual adjustments possible in a digital workflow or temporarily creating digital twins of paper-based credentials to incorporate them into pure digital workflows. This can also mean that digital credentials are printed out, to be included in paper-based credential workflows.

C. Challenges of Digital Credentials

Digital representations of credentials have their own challenges, that may be quite different from the paper-based ones.

1) Private Data Protection: Digital data can easily be copied, and creating identical copies of digital data is part of IT workflow. For example, if a digital credential is sent from the issuer over a secure channel to the credential holder, its actual data is copied multiple times in the process. First, the credential is copied from the data storage at the issuer to the network stack of the issuers system. Then, it duplicated into a transport format, over various relays in the communication system, and into the network stack of the receiver, unpacked. Finally, the receiving application's memory stores the last copy. This characteristic of digital data makes it also easy to leak private data in the process. In paper-based credentials, simple physical access control is often enough. Contrary, access control has to be secured digitally for digital credentials.

2) Data Security: Digital data ultimately is stored in physical form, and this storage will degenerate over time. It is, therefore, important to be able to copy the digital credential to new physical storage, and to continuously monitor the quality of the storage before the degradation leads to damaged data. In libraries, the "lots of copies keep stuff safe" (LOCKS) model has been successfully implemented for electronic publications, based on the idea that independent copies of the same data in physical and geographical independent data stores, ensure high data security and availability [13].

3) Data Management: Differently to paper-based credentials, a digital credential can only be perceived by a user if content or metadata is rendered in a perceivable form (usually visual). Management systems need to ensure that users know what is stored and what is transmitted if requested. This requirement is also demanded in the EU General Data Protection Regulation (see Section II-C4 for more details.) Digital credentials also have the unique possibility to easily collect and visualise each credential's context and relations to other skills and achievements. Beattie [14] argues that by making these connections and context apparent to the user, learning can shift from collecting credentials and thus increasing the "height" of the credential collection towards increased understanding and amplification if the "depth" of knowledge. Beattie [14] also sees it as an essential means of the learners' motivation, based on experience in role-playing games design. Elkordy also reports increasing motivation in [15]. Buchem in [16] gives an example where the depth of a credential is codified by three levels: *basic*, meaning "what everyone needs to know", *expertise*, meaning "what you not only know but also can do" and *master*, meaning "what only a few people know and can do."

4) Data Sovereignty: The ease of copying of digital data allows for the storage of digital credentials physically far from the users, e.g., in the cloud. However, this also means that the actual data then is outside the physical oversight of the user. The term "data sovereignty" [17] has been coined in recent years to describe "the idea that users, being citizens or companies, have control over their data" [18]. Improved data sovereignty for the user is also at the base of recent legislative developments like the General Data Protection Regulation (GDPR) of the European Union [19]. According GDPR, data subjects have the rights:

TABLE I. PROPOSED RESEARCH QUESTIONS TO EVALUATE THE PERFORMANCE OF A DIGITAL EDUCATION CREDENTIAL MANAGEMENT SYSTEM IN SOLVING THE CHALLENGES EXPERIENCED BY THE USER.

Challenge	Question	Units
Fraud protection and verification	How is the system protected against fraud?	qualitative
	What are the costs of a successful attack against the fraud protection?	time, money
Issuer dependence	What are the requirements for an issuer of digital credentials?	qualitative
	How much does issuing a credential cost?	time, money
Handling	Describe the workflow of a credential in the system.	qualitative
	How much does handling of a credential in the workflow cost?	time, money
Data security	How is the credential stored in the system?	qualitative
	Is the credential data format public and open?	yes/no
	How many independent copies of the credential are stored in the system at any time?	number
	How is the credential secured against accidental loss or data change?	qualitative
	How is the credential secured against unauthorised, but intentional, loss or change of data?	qualitative
Digitisation of existing credentials	How can existing analogue credentials be included into the digital workflow?	qualitative
	Is the content of the analogue credential converted to structured data to the same level of detail as digital credentials?	yes/no
Interaction between analogue and digital workflows	How can the system interact at the same time with digital and analogue credentials	qualitative
	How much increases the effort in the workflow, if digital and analogue credentials are mixed?	time, money
Private data protection	How is the private data stored in the system protected against unauthorised access?	qualitative
	What are the costs of a successful attack against the private data protection?	time, money
Data management	How is the data managed from the user perspective?	qualitative
	Can the user tell at any time of the workflow, what data exactly he/she is working with?	yes/no
	Can the user tell at any time of the workflow, who is able to access the data in question?	yes/no
Data sovereignty	How is data sovereignty enforced in the system?	qualitative
	Can the holder of the credential decide at any time of the workflow, who is able to access the data in question?	yes/no
	How much does it cost the user to store the data under his/her exclusive physical access?	time, money
	What are the costs of a successful attack against the access protection (access, denial of service, data change)?	time, money
	If there are other possibilities of storage, how convenient are they to the user?	time money
	What are the costs of a successful attack against these other storage possibilities (access, denial of service, data change)?	time, money

1) Obtain information about the processing of personal data;
2) Access to their personal data;
3) Potentially collect incorrect and incomplete personal data;
4) Request that personal data be erased when it is no longer needed or if processing it is unlawful;
5) Receive personal data in a machine-readable format and send it to another controller ("data portability"); and
6) Request that decisions based on automated processing are made by natural persons, not only by computers.

Education credentials certainly are personal data in the sense of GDPR. To provide the previously mentioned rights 1–4 to the holder of the credential, a management system must be able to provide access to the credential on request, and to remove or replace credentials if required. Credentials need to be available in portable formats (right 5), and the processes where the credentials are used to make decisions must be transparent (right 6).

III. PROPOSED RESEARCH QUESTIONS

In this section, we collect the questions whose answers will be utilised to validate the effectiveness of a system devised to achieve the challenges presented in the previous Section II. Each given topic translates into a set of questions. We start each topic with a question asking for a qualitative description of how the proposed solution approaches a relevant challenge. Then, we go into detail by adding quantitative questions that will enable us to measure the effect that the proposed solution has on each challenge in a given use case. Lastly, a digital credential solution is compared to the status quo of non-digital workflows using this mixed qualitative and quantitative approach. Table I presents our research questions; they are grouped according to the challenges presented in Section II. The challenge *data security* affects both digital and paper-based credentials in very similar ways, so we were able to combine all relevant questions into one field.

IV. USE CASE

The EU Horizon 2020 research and innovation action QualiChain "targets the creation, piloting and evaluation of a decentralised platform for storing, sharing and verifying education and employment qualifications and focuses on the assessment of the potential of blockchain technology, algorithmic techniques and computational intelligence for disrupting the domain of public education, as well as its interfaces with private education, the labour market, public sector administrative procedures and the wider socio-economic developments."[20] The fundamental idea of the project is to build an open source based distributed platform, supporting the storage, sharing and verification of education credentials. This platform will allow for the implementation of additional services, which will fulfil the needs of the participating actors, such as data analytics and decision support systems. QualiChain hosts five pilot projects distributed over Europe (for details please see [21]), where the system is tested in four real-world scenarios:

- Lifelong learning;
- Smart curriculum design;
- Staffing the public sector; and
- Providing HR consultancy and competency management services.

We provided online questionnaires to support the participants in the pilots in the definition of the use cases, challenges and possible research questions, as well as to define key performance indicators. These questionnaires were filled in and discussed with the people involved in the pilots in early 2019. The process is discussed in detail in [8] and not repeated here for the sake of brevity.

V. Related Work

In this section, we present relevant related work, segregated into literature that looks at the impact of digital education credentials, open badges infrastructure, and examples of transformation from analogue to digital credentials.

A. Impact of Digital Education Credentials

The articles in the collection edited by Ifenthaler et al. [22] offer a deep introduction into the topic of digital badges and micro-credentials. Digital badges are a special form of education credentials, usually following the open badges standard [23], that are often meant to be displayed prominently by their owner. Ellis et al. [24] write "Traditional badges are often graphic representations of what it is that the badge represents. For example, a scout merit badge has a symbolic graphic of what the topic of the badge is." Digital badges follow this tradition by incorporating images that represent the achievements certified by the badge. Micro-credentials are credentials that certify only a small and easy to define achievement of the learner—thus the name micro.

In [25], Willis et al. remark that open digital badges can bring transparency into awarding of credentials in education and raise question about the roles of instructors, badge providers and learning management systems. They note that digital credentials empower individual learners to "to take control of determining how their learning experiences can be validated and shared." They assume easy scaling for digital credentials, but also warn of issues of trust, confidence, excessive data collection, data protection and ethics. In [24], Ellis et al. also press the point that digital badges will face the risk of loosing their value in the education system if no commonly accepted way can be found to audit and evaluate them. Coleman et al. describe in [26] design principles for digital badges. They argue that creativity please an important role in learning and can be supported in badge design and badge management. They propose to use the principles of *transmedia story telling* [27], a "Curated Learning Journey", to create an experience for the learner that allows the learner to "participate in the learning process in an organic way."

Lockley et al.[28] note that "badges can be agnostic as to the education provider. They enable digital credentials to be issued outside higher education providers"; thus, removing the dependence on the traditional issuers of education credentials. They also note that micro-credentials allow learners more flexibility in their education process. More flexible and shorter education pathways empower education processes and provide a unique opportunity not supported in traditional certification methods. Lockley et al. [28] devise credential badges as "*lingua franca* for learners, educators and employers"; Willis et al. [25] refer to badges as "a currency to demonstrate marketable skills and abilities, at least in theory." Grant in [29] shares the point of view of badges being a currency in credential markets and the reputation economy.

Gander in [30] is proposing to evaluate the implicit and explicit promises and expectations of digital credentials, concentrating on micro-credentials. He notes that explicit promises are rarely expressed, while the implicit promises are that micro-credentials will meet the following properties:

- Follow established standards of evidence for skills and knowledge achievements;
- Are related to other digital micro-credentials;
- Offer authentication of experience;
- Promise individualisation highlighting each individual's developmental history, special interests, and talents;
- Enable longevity of the digital information; and
- Facilitate use and continued availability.

Gander further suggests to capture as much data as possible about these implicit expectations in the application of micro-credentials. As a result, the analysis of their impact is conducted by comparing the evaluation in regular intervals over time. The article also presents a case study of an institute situated in the US, which created a series of 17 micro-credentials and reports the start of the data collection. Aberdour in [31] argues that a transformation of workplace learning is necessary for organisations to stay agile, resilient, and effective. A digital badge program is shown as a way to establish a learning culture in a work place.

The main point of focus in the literature cited so far, is on the social impact of digital credentials and their effect on the transformation of the education system in itself. Though, we think that this is an important field of research, in our work, we decided to not go down this route. Instead, we look at the management of education credentials, ignoring the changes it may have on the education system itself. We note, however, that there is an overlap because of fundamental properties of digital badges, that drive these reported changes in education. This is especially true for the possibility to issue digital (micro-) credentials without being an official recognised learning institute, i.e., what we describe as the issuer dependence of credentials.

B. Open Badges Infrastructure

Dimitrijević et al. [32] present a framework of scenarios to define requirements for Open Badges platforms. The scenarios with the extracted requirements are:

- *Offering badges*: Education provider must be able to issue digital badges, i.e., creation of badges and badges templates, use of badge metadata, documentation, alignment to existing learning standards and publication of badges.
- *Badge discovery*: Learners must be able to search and find chances for badges, i.e., search for badge opportunities, review and comparison, selection of a badge opportunity.
- *Applying for badges*: Learners must be able to request badges, i.e., registration for badge chances, application for badges.
- *Awarding badges*: The process of awarding badges contains multiple requirements. They include the support

for **i)** automated assessment of an achievement and self-assessment; **ii)** multiple assessors and peer assessors; **iii)** evidence of achievements; **iv)** automated and manual badge awarding; and **v)** digital signing of badges, information of badge applicant of decision, and issuing of badges.
- *Management of and reflection over collected badges*: Learners must be able to collect and manage their badges, i.e., collection of badges, import of badges, organisation of badges, overview dashboards, and visualisation of badges and data.
- *Displaying and sharing badges*: display tailoring, tailoring of social media posts and display, support for personal badge stores, support for web display, and permissions management.
- (*Re)viewing a badge earner's achievements*: Other people than the learner must also be able to consume and review badges, e.g., a recruiter. Functional requirements are: User-based search, badge-based search, (re)view of the overall badge earner's experience, (re)view of individual badges, and evidence validation.

Based on these use cases and requirements, Dimitrijević et al. [32] then evaluate selected badging platforms, namely *BadgeList*, *BadgeOS*, *Credly*, *ForAllRubrics*, *Open Badge Factory + Open Badge*, *Passport* and *Peer 2 Peer University (P2PU)*. They report in their article that all inspected platforms cover the most basic functional requirements. The requirements of the detailed scenarios however are much less likely to be fulfilled. Few platforms fulfil all requirements of the "Offering badges" scenario. Half of the platforms support searching for opportunities from the "Badge discovery" scenario, but none of them allow comparisons of the opportunities. Regarding "Applying for badges", all platforms allow learners to support evidence by various means for the application. Also, the basic functional requirements of the "Awarding badges" scenario are in general well supported, but requirements related to assessment are rarely fulfilled. The authors also report that they were not able to verify the claim that is was possible to digitally sign badges on the platforms. All platforms, however, allowed the users to manage their badges gained at the same platforms, while few allowed to import badges from other places. The "Displaying and sharing" scenario in general was found to be well supported, while the "Reviewing achievements" scenario presented a mixed picture: all platforms were found to provide an overview of the achievements of the learner, but very few also allowed user-based or badge-based searches. For our investigation we followed the same basic approach as presented by Dimitrijević et al. [32], i.e., to define the relevant scenarios and then derive the functional requirements for it. This method is a very natural way to approach an evaluation. It also allows for including users in the field in the analysis, as the given scenarios translate directly into their use cases, requirements and experiences.

On a side note, in [16], Buchem presents design patterns that can be useful in the design a digital credential management solution. In the "Digital badges as parts of a digital portfolio" pattern, he describes the use of a grid system that describes the necessary skill sets for certain topics, activities and levels, resembling an easy to understand board game.

C. Examples of Transformation From Analogue to Digital Education Credentials

In [33], Glover describes the case of the Sheffield Business School at Sheffield Hallam University. They switched from paper based education credentials to digital Open Badges in 2014 for a selected program for students wishing to represent their peers in discussions with teaching staff and university management. An anonymous survey was then executed to capture the participating students' impressions of the badges in comparison to the previous paper certificates. Glover selected the following hypotheses:

- *H1*: Students see badges as a way to differentiate themselves from peers.
- *H2*: Badges motivate some students to complete existing or undertake additional work.
- *H3*: Students want badges that represent all aspects of their studies, including both formal and semi-formal learning.

Out of 89 students participating in the programme, 46 responded in the survey. The results confirmed H1 and H3, but not H2. It is interesting to note for the transformation to digital credentials, that participants reported overall positive or neutral reactions by their peers when sharing the digital badge and all sharing students stated that they might or would share the digital badges again. Glover also writes that "Several respondents explicitly contrasted the digital badges with an equivalent paper certificate, asserting that, as the certificate is a tangible artefact and is a widely recognised method of representing experience and learning, it would carry much more credibility than a digital badge. However, despite their scepticism around the value of digital badges, most of the respondents qualified these remarks with statements such as '... unless they are recognised by employers ...', suggesting that the utility of digital badges is directly linked to their wider acceptance." Glover, therefore, recommends that the concept of badges and their purpose is to be clearly explained, in order to maximise the perceived value of badges. He also remarks that the open nature of digital badges means that they can be created and issued by anyone, and for any purpose. He assumes that this creates a credibility problem for digital badges and recommends that organisations should implement quality control over the creation and issuing of badges to ensure that badges represent standardised levels of achievement, similar to processes already in place for academic programmes at education providers such as universities.

VI. Conclusion and Future Work

In this article, we discussed the main challenges in education credential management. We showed that the transformation from analogue to digital in education credentials had not received intense attention from the scientific community. Based on the available literature and information collected from participants in the EU QualiChain project pilots, we developed a methodology to qualitatively and quantitatively measure a system's effectiveness in addressing education credential management's challenges and the transformation from paper-based credentials to digital credentials. We will apply this methodology to the use cases of the Horizon 2020 EU Project QualiChain, which covers a wide area of applications of education credentials. Applying this methodology will allow us an in-depth evaluation of the project's performance.

Based on the experience gathered in this process, we plan to extend this work in the future to a full framework for the evaluation of the performance of education credential management solutions. This framework should capture the whole life cycle of education credentials from creation and issue over storage, management, and access control, towards credential expiring or retraction. We expect that this novel framework will provide transparency in the way how education credentials are managed, as well as the possibility to tracking down all the decisions done during the whole life cycle.

ACKNOWLEDGEMENT

This work has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 822404 (QualiChain). The authors would like to express their thanks for proof reading of this article to Simon Worthington and Salua Nassabay.

REFERENCES

[1] I. R. Keck, M.-E. Vidal and L. Heller, 'Digital transformation of education credential processes and life cycles – a structured overview on main challenges and research questions', in *Proceedings of the Twelfth International Conference on Mobile, Hybrid, and On-line Learning eLmL 2020, July 12–14, 2013, Valencia, Spain*, Mikroyannidis, A., Chang, M. and White, S., Ed., ISBN: 978-1-61208-764-1, ISSN: 2308-4367, Think Mind, 2020, pp. 53–56. [Online]. Available: https://www.thinkmind.org/index.php?view=article&articleid=elml_2020_1_60_58006 (visited on 2020-12-01).

[2] CareerBuilder, *Fifty-eight percent of employers have caught a lie on a resume, according to a new careerbuilder survey*. [Online]. Available: http://press.careerbuilder.com/2014-08-07-Fifty-eight-Percent-of-Employers-Have-Caught-a-Lie-on-a-Resume-According-to-a-New-CareerBuilder-Survey (visited on 2020-12-03).

[3] S. Brain, *Statisticbrain - resume falsification statistics*, 2017. [Online]. Available: https://web.archive.org/web/20170907150814/http://www.statisticbrain.com/resume-falsification-statistics (visited on 2020-12-03).

[4] D. Everhart, A. Derryberry, E. Knight and S. Lee, 'The role of endorsement in open badges ecosystems', in *Foundation of digital badges and micro-credentials*, Springer, 2016, pp. 221–235.

[5] G. Room, 'Globalisation, social policy and international standard-setting: The case of higher education credentials', *International Journal of Social Welfare*, vol. 9, no. 2, pp. 103–119, 2000.

[6] M. Kotarba, 'Measuring digitalization–key metrics', *Foundations of Management*, vol. 9, no. 1, pp. 123–138, 2017.

[7] *QualiChain – decentralised qualifications' verification and management for learner empowerment, education reengineering and public sector transformation*. [Online]. Available: https://qualichain-project.eu (visited on 2020-12-04).

[8] I. Keck, M. E. Vidal, A. Mikroyannidis, C. Kontzinos, S. Skalidakis *et al.*, 'D7.1 – qualichain pilots preparation handbook', Tech. Rep., 2019. [Online]. Available: https://alfresco.epu.ntua.gr/share/s/AQjQwquNRwOl-CtaHFDBLQ (visited on 2020-12-03).

[9] European Commission, *The role of universities in the europe of knowledge*, 2003. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:c11067 (visited on 2020-12-04).

[10] HECSU, *Prospects hedd verification + authentication*. [Online]. Available: https://hedd.ac.uk/ (visited on 2020-12-04).

[11] D. Matthews, 'What blockchain technology could mean for universities', *Times Higher Education*, Aug. 2017. [Online]. Available: https://www.timeshighereducation.com/news/what-blockchain-technology-could-mean-for-universities (visited on 2020-12-04).

[12] B. A. Fabunmi, M. Paris and M. Fabunmi, 'Digitization of library resources: Challenges and implications for policy and planning', *International Journal of African & African-American Studies*, vol. 5, no. 2, 2009.

[13] V. A. Reich, 'Lots of copies keep stuff safe as a cooperative archiving solution for e-journals', *Issues in Science and Technology Librarianship*, 2002. [Online]. Available: http://doi.org/10.5062/F47P8WCW (visited on 2020-12-04).

[14] S. Beattie, 'Height vs. depth in badging framework design', in *Foundation of Digital Badges and Micro-Credentials*, Springer, 2016, pp. 307–324.

[15] A. Elkordy, 'Development and implementation of digital badges for learning science, technologly, engineering and math (stem) practices in secondary contexts: A pedagogical approach with empirical evidence', in *Foundation of Digital Badges and Micro-Credentials*, Springer, 2016, pp. 483–508.

[16] I. Buchem, 'Digital badges as (parts of) digital portfolios: Design patterns for educational and personal learning practice', in *Foundation of digital badges and micro-credentials*, Springer, 2016, pp. 343–367.

[17] R. Posch, 'Digital sovereignty and it-security for a prosperous society', in *Informatics in the Future*, H. Werthner and F. van Harmelen, Eds., Cham: Springer International Publishing, 2017, pp. 77–86, ISBN: 978-3-319-55735-9.

[18] S. Amaro, *Europe's dream to claim its 'digital sovereignty' could be the next big challenge for us tech giants*, Nov. 2019. [Online]. Available: https://www.cnbc.com/2019/11/20/us-tech-could-face-new-hurdles-as-europe-considers-digital-sovereignty.html (visited on 2020-12-04).

[19] General Data Protection Regulation, 'Regulation (eu) 2016/679 of the european parliament and of the council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46', *Official Journal of the European Union (OJ)*, vol. 59, no. 1-88, p. 294, 2016. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32016R0679 (visited on 2020-12-04).

[20] *QualiChain – decentralised qualifications' verification and management for learner empowerment, education reengineering and public sector transformation*, Nov. 2018. [Online]. Available: https://cordis.europa.eu/project/rcn/218758_en.html (visited on 2020-12-04).

[21] C. Agostinho, R. Melo, I. Keck, C. Kontzinos, V. Karakolis *et al.*, 'D2.2 – qualichain stakeholders' requirements and use cases', Tech. Rep., 2019. [Online]. Available: https://alfresco.epu.ntua.gr/share/s/EflUU9mbTESnrZo74WAZHg (visited on 2020-12-03).

[22] D. Ifenthaler, N. Bellin-Mularski and D.-K. Mah, Eds., *Foundation of Digital Badges and Micro-Credentials*. Springer International Publishing, 2016. DOI: 10.1007/978-3-319-15425-1. [Online]. Available: https://doi.org/10.1007/978-3-319-15425-1 (visited on 2020-12-04).

[23] J. Bohrer, T. F. Cook, M. Esquela, S. Gance, J. Goodell *et al.* (Apr. 2018). Open Badges v2.0: IMS Final Release. Open Badges specification, [Online]. Available: https://openbadgespec.org/ (visited on 2020-12-04).

[24] L. E. Ellis, S. G. Nunn and J. T. Avella, 'Digital badges and micro-credentials: Historical overview, motivational aspects, issues, and challenges', in *Foundation of Digital Badges and Micro-Credentials*, Springer, 2016, pp. 3–21.

[25] J. E. Willis, K. Flintoff and B. McGraw, 'A philosophy of open digital badges', in *Foundation of Digital Badges and Micro-Credentials*, Springer, 2016, pp. 23–40.

[26] K. S. Coleman and K. V. Johnson, 'Badge claims: Creativity, evidence and the curated learning journey', in *Foundation of digital badges and micro-credentials*, Springer, 2016, pp. 369–387.

[27] R. Pratten, *Getting started with transmedia storytelling*. CreateSpace, 2011, ISBN: 978-1456564681.

[28] A. Lockley, A. Derryberry and D. West, 'Drivers, affordances and challenges of digital badges', in *Foundation of digital badges and micro-credentials*, Springer, 2016, pp. 55–70.

[29] S. Grant, 'Building collective belief in badges: Designing trust networks', in *Foundation of Digital Badges and Micro-Credentials*, Springer, 2016, pp. 97–114.

[30] S. L. Gander, 'Evaluating the public promise', in *Foundation of Digital Badges and Micro-Credentials*, Springer, 2016, pp. 71–95.

[31] M. Aberdour, 'Transforming workplace learning culture with digital badges', in *Foundation of Digital Badges and Micro-Credentials*, Springer, 2016, pp. 203–220.

[32] S. Dimitrijević, V. Devedzić, J. Jovanović and N. Milikić, 'Badging platforms: A scenario-based comparison of features and uses', in *Foundation of Digital Badges and Micro-Credentials*, Springer, 2016, pp. 141–161.

[33] I. Glover, 'Student perceptions of digital badges as recognition of achievement and engagement in co-curricular activities', in *Foundation of digital badges and micro-credentials*, Springer, 2016, pp. 443–455.