CONCEPT NOTE

Education credentials on a distributed ledger

Introduction

The value of education is just as intangible as the concept of education itself. It is a "tool" to eliminate prejudice, unemployment and hunger. It is also regarded as a decisive factor when it comes to facing the challenges of the future. The value of education is correspondingly high. Verified qualifications and transferable credentials are needed to prove an educational path and history. However, it is precisely when such certificates are issued, need to be accessed or validated that numerous difficulties arise.

Problem description

Across the globe, the future of work shifts the focus from manual labour to knowledge work. Knowledge economies thrive on the paradigm of life-long learning. Individuals are tasked to acquire new skills and update their qualifications on an ongoing basis. To do so, they increasingly engage in new ways of learning that tend to be digital and globally interwoven, involving ‘micro degrees’ from a variety of institutions. Universities and other education providers have started to offer their courses on online platforms so that learners can take classes part-time, from anywhere and at the time of their choosing. As new actors in the educational ecosystem, the operators of such platforms use innovative analytics to understand educational demands and match them with new course offers flexibly. – A future seems to be at our fingertips in which anybody will at any stage of their career be able to acquire just the right skills at just the right time.

Meanwhile, the turn towards an unbundling of educational programmes continues. Degrees are split into independently verifiable learning modules. Learners benefit from this restructuring in several ways: They can bank credits; this allows them to increasingly progress on their educational path at their own pace. They get the means to showcase even partial fulfilments to third parties, avoiding the disadvantages of being enrolled in programmes that only certify one final degree after year-long studies. Finally, modular crediting schemes improve portability and inter-institutional acknowledgement of achievements. The unbundling of education also shifts the role of universities and other educational authorities: Were they previously the sole providers of all courses and bookkeepers of a learner’s progress, we can re-imagine them as curators of degrees that represent collections of independently verifiable and also external learning modules. Learners accumulate such certificates – similar to a credit bank model – so to earn a degree or certificate of competence.

Changes on the provisioning side of education prompt expectations towards the receiving ends. This is where individuals and institutions such as employers and governmental authorities interact with the educational records that have been issued. On the job market, individuals are expected to readily produce authorised versions of their educational records – not only at a few predefined moments in their lifes (such as when entering from higher education into university), but flexibly and at any stage of their career. Employers, other educational institutions, standardisation bodies and governmental authorities on the other hand need interoperable standards and the means to verify and validate such certificates efficiently. All this shows that the challenges for stakeholders in the educational ecosystem are interconnected.

How does the status quo compare to this observed shift?

Currently, job applicants often still have to request transcripts from their universities or governmental bodies, which can be costly. Employers still need to contact the issuing authority to ensure that a certificate is indeed authentic or pay for an educational credential evaluation service. This makes the whole process cumbersome, costly and slow. Besides, if certification systems are not working well, there can be far-reaching consequences for some individuals such as, for instance, refugees who are unable to provide a diploma of completed study and are thus prevented from getting a job or – in the worst case scenario – residence rights in their host country. – If processes around verification and validation of certificates fail so bad this can instigate fraudulent and corrupt behaviour.

With the diversification of educational offers comes a need to bring the underlying infrastructures for issuing and verification up to the task of fostering trust in certificates. The following challenges will need addressing to develop an open, globally accessible infrastructure for verification:

- **Harmonise the valuation of educational standards**. – This task involves creating equivalence between increasingly diverse forms of qualification. It is mainly the field of international standardisation bodies, learning consortia and education associations.

giz Deutsche Gesellschaft
für Internationale
Zusammenarbeit (GIZ) GmbH

THE LAB

- **Increase interoperability between systems for verification.** – This highlights the need for open certification schemes and technical standards that any system provider can build upon to interact with the verification infrastructure. Fostering interoperability will a) provide a level playing field for competition around the provision of solutions for digital certification issuance and management and b) provide the preconditions to grant learners more control over their certificates because portability between systems becomes possible.
- **Raise efficiencies in verification processes.** – At the moment, issuing institutions present bottlenecks in the process of verification. Blockchain technologies present an opportunity to rethink roles and responsibilities in a way that dissolves this centralised gatekeeper structure in favour of a distributed one that empowers certificate holders.
- **Foster trustworthiness, reliability and robustness of verification infrastructures.** – This refers to the need that the system's architecture, governance and operations model must be suitable to justify the user expectation to have sustainable global access.

Leveraging distribution

While not being a silver bullet, blockchain technology can indeed provide a solid basis to tackle some of these challenges. Its distributed nature supports protection against counterfeits, the need for global access and secure management of certificates even if the issuing authority no longer exists, and automation of monitoring processes for certificates with a time-limited validity. This would not only benefit learners but a wide range of beneficiaries, including academic institutions, governmental bodies, corporate entities, and hiring consultants.

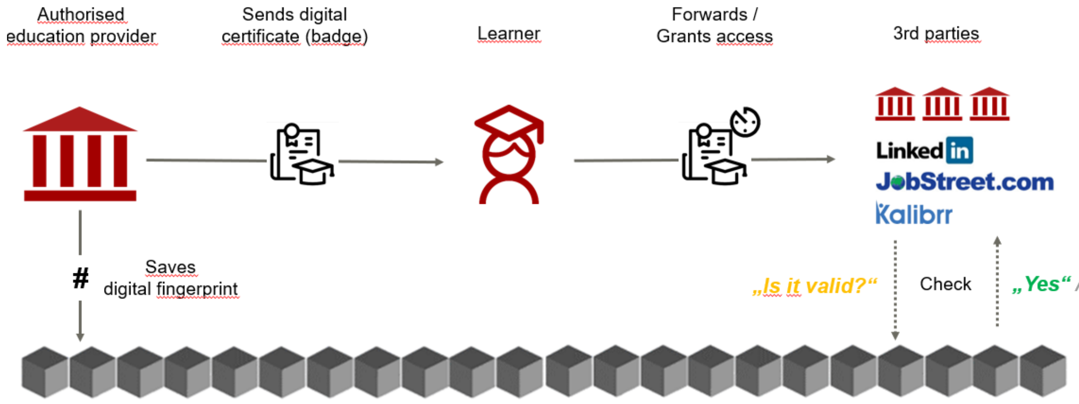
Blockchaining education credentials – how does it work?

In a nutshell, education credentials that are blockchain-based come with tamper-proof registration and global accessibility. The most basic design of such a credential architecture is fairly simple.

In a first step, a trusted certifier admits accrediting institutions, for the sake of this example universities, to the system by registering their unique, digital fingerprint. These digital fingerprints are based on so-called public-key cryptography where they publicly identify with their unique signature, but exclusively remain in control of the corresponding private key. This private key enables an accredited institution to validate and add credentials to the blockchain.

In a second step, each accredited authority can comprise all information that an education credential contains – qualification or title, name of the certifier, name of the student, and issue and possibly expiration date – into a dataset, also called a badge. This dataset is then signed by the university. Through a so-called hash function, the dataset is reduced to a hash – a short, arbitrary sequence of symbols that can be seen as a digital fingerprint. This digital fingerprint does not contain any personal information and cannot be converted back into the dataset, given that hash-functions are one-way. Students' private data or the corresponding metadata reflecting the education programme is kept separately from the public blockchain and managed securely by the accredited institution. By hashing the dataset, a transaction that contains its digital fingerprint is automatically sent to the blockchain, thus making the credential immutable[1].

Concurrently, the graduate receives a digital copy of the badge (so the complete dataset before it has been hashed) from the accredited institution, which gives her or him full control over the badge. This transmission may occur via email or via an account-



Picture 1 Stakeholders and processes

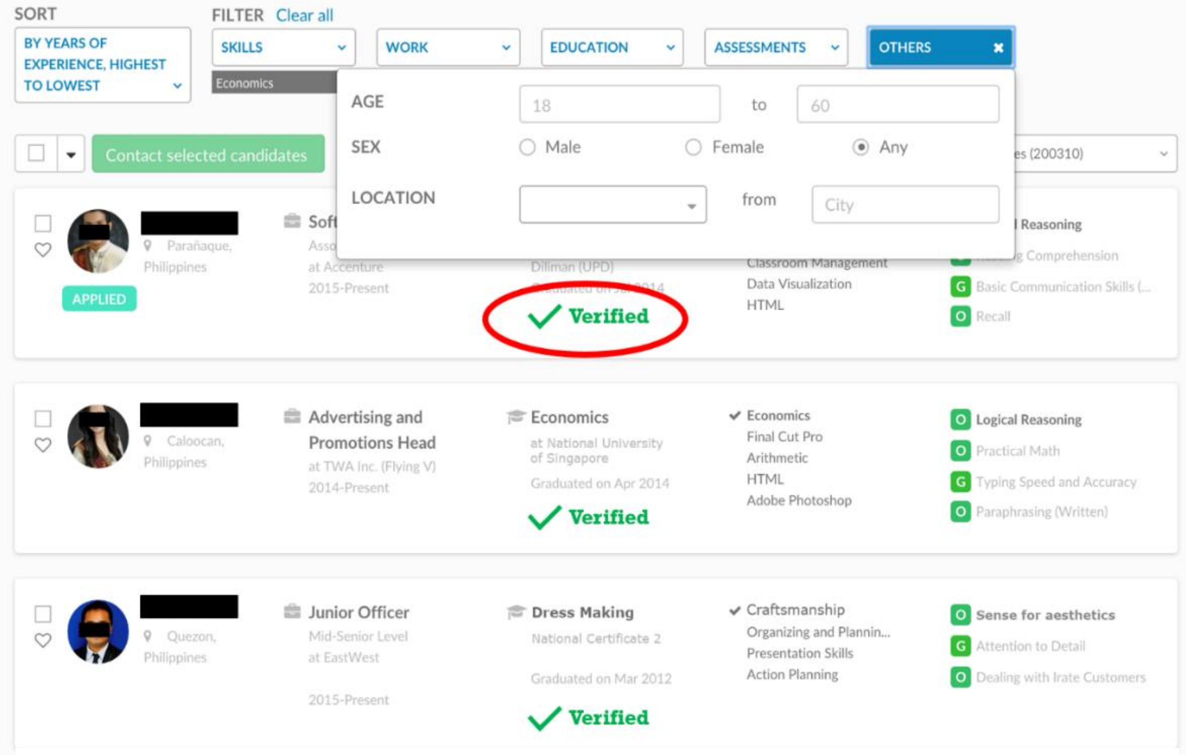
[1] Among blockchain professionals, the word „immutability“ is contested, as arguably no technical can be 100% immutable while blockchain comes as close as no technical system before. We certainly agree with this argument. Yet we choose to use the term 'immutable' for the sake of simplicity and to reflect the objectives and vision of our system and blockchain more widely, which is constantly maturing and tends to become increasingly resilient, secure and at least quasi-immutable.

based web platform, administrated by the accredited institution. Now, whenever a hiring entity or administration asks for proof, the graduate can choose to send a digital copy of the academic achievement to such entities. They can upload the badge to a website which checks the smart contract on the blockchain and returns a warning if the badge has been tampered with. This process generally just requires a browser and can be done on desktop or mobile as long as there is a basic internet connection, allowing employers and administrations to automatically and from anywhere in the world review the certificate's authenticity. The blockchain therefore makes it possible to verify at any given time and place who a certificate was issued to, by whom, and validate the content of the certificate itself.

Taking this concept a step further, one can even think of integrating such a blockchain-enabled system into lifelong learning activities. Let's imagine that a distributed platform of achievement, affiliation, and authorization is created that offers a more detailed picture of people's learning experiences throughout their life, such as participation in conferences and workshops, official certification, community involvement, and all the other competences people develop outside of formal credentialing systems. Such "lifelong learning passport" could be shared in job applications and be issued and verified by anyone with the proper profile.

Conveniently, access to the blockchain-based verification service could also be offered via an API for already existing third-party platforms such as LinkedIn, XING, JobStreet, or Kalibrr.

In order to maximise integration with external services the credentialing system would ideally use the most widespread and open standards for badges, e.g. the OpenBadges[2] standard.



SORT

BY YEARS OF EXPERIENCE, HIGHEST TO LOWEST

FILTER Clear all

SKILLS | WORK | EDUCATION | ASSESSMENTS | OTHERS ×

Economics

AGE 18 to 60

SEX ○ Male ○ Female ● Any

LOCATION from City

□ Contact selected candidates

es (200310)

□ ♡ [redacted]
Parañaque, Philippines
APPLIED
Soft
Asso
at Accenture
2015-Present
Diliman (UPD)
Graduated on Jul 2014
✓ Verified
Classroom Management
Data Visualization
HTML
Reasoning
Comprehension
G Basic Communication Skills (...
O Recall

□ ♡ [redacted]
Caloocan, Philippines
Advertising and Promotions Head
at TWA Inc. (Flying V)
2014-Present
Economics
at National University of Singapore
Graduated on Apr 2014
✓ Verified
✓ Economics
Final Cut Pro
Arithmetic
HTML
Adobe Photoshop
O Logical Reasoning
O Practical Math
G Typing Speed and Accuracy
O Paraphrasing (Written)

□ ♡ [redacted]
Quezon, Philippines
Junior Officer
Mid-Senior Level
at EastWest
2015-Present
Dress Making
National Certificate 2
Graduated on Mar 2012
✓ Verified
✓ Craftsmanship
Organizing and Plannin...
Presentation Skills
Action Planning
O Sense for aesthetics
G Attention to Detail
O Dealing with Irate Customers

Picture 2 Mock-up of API-powered verification on professional social network platform

Potential challenges

Even though a blockchain-based solution facilitates the transfer of reliable information to potential employers, the technology cannot be a warranty for the skills and abilities, whose validation remains centralized in the accrediting entities which have a reputation often ratified by national authorities. Furthermore, privacy and data protection considerations will have to be taken into account. Certificates are only useful if they can be linked to a person holding them. Yet, this means that some personal data of the learners has to be collected for the system to function – data that might be misused. Technical solutions to this challenge such as zero-knowledge proofs are in the making, their implementation is however far from straightforward.

From the viewpoint of education policy, the necessary formalisation of educational evidence creates the risk of overemphasizing skills that are easy to measure in a standardised way.[3]

Finally, a distributed system architecture that puts learners in full control of their certificates also means that learners bear the responsibility of preserving their

[2] https://openbadges.org/

[3] See Barabas & Schmidt (2016) - http://rooseveltinstitute.org/wp-content/uploads/2016/08/The-Promises-and-Challenges-of-Digital-Credentialing.pdf

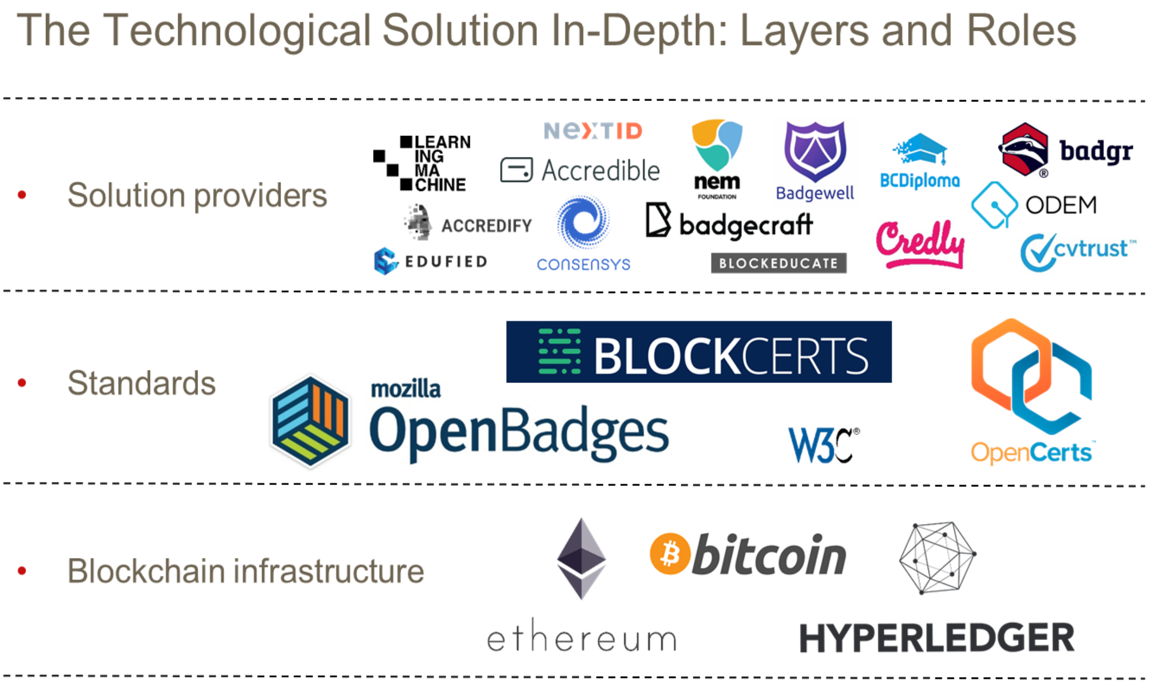
digital certificates (remember: the certificates are not saved on the blockchain, just a hash). While there are many ways of backing up data, this can present a challenge in scenarios with very low digital literacy.

Ideal application context

The stakeholder landscape of a blockchain-based platform for education credential includes

i. a trusted certifier,
ii. issuing institutions,
iii. learners, and
iv. third parties such as administrations or employing entities or even web intermediaries such as online job networks, which want to verify the validity of the certificates in question.

In terms of concrete application contexts for which such a solution would create benefice, several scenarios can be imagined: In the first scenario we talk about a context in which endemic credential fraud is prevalent and therefore the sound development of education is impeded, while the labour market fails to recruit duly graduated students. In such circumstances, reliable education data could improve trust from employers, limit administrative burden and truly reward merit among students who obtained certified diplomas. Another interesting scenario is where the learners do not have the financial means to get their certificates validated by the issuing authority which demands high fees for this services. In these situations, the blockchain-based system would give students back ownership about their achievements without any monetary implications. A third scenario is where the long and cumbersome administrative processes of certificate access and verification impedes on the success of learners' job applications and hiring entities search for suitable employees alike. In these situations, blockchain-based education credentials can significantly streamline the process for all actors involved. Finally, it goes without saying that an ideal application context can also encompass a combination of two or even all three of these scenarios.


The Technological Solution In-Depth: Layers and Roles

- Solution providers
- Standards
- Blockchain infrastructure

Picture 3 Layered view of the emerging ecosystem for blockchain-based education credentials

Choosing a solution design

There is no standard blockchain-based credentialing solution yet. Developers still explore various architectural approaches, which have different features and lead to different trade-offs.

In order to still get a rough understanding of how the building blocks of such a solution come together, it helps to think in terms of layers.

The base layer of any blockchain system is the internet. On top of that runs the blockchain infrastructure. The broad middle layer consists of standards for data models and syntax to express the claims. On the top layer, solution providers offer – currently mostly proprietary – applications that provide interfaces and methodologies for issuers, learners and other end-users (such as employers) to interact with the blockchain through the standards.[4] So modules on higher layers make use of functionality that is provided to them by the layer below.

Without going into all the technical details, the questions below may help decision-makers to interrogate the different credentialing solutions with

[4] A technical description of how two exemplary systems work can be found in the Appendix.

regard to their suitability in the context of sustainable software development.

- Is the solution open source and based on open standards?
- Is the underlying technology sufficiently mature?
- Is the underlying technology appropriately maintained,
  e.g. by a sophisticated open source community?
- Are there existing implementations and references we can learn from?
- Are there public repositories and templates we can reuse and adapt?
- Does the solution allow for a scalable, sustainable mode of operation?

Current initiatives

Several universities, research institutions and blockchain companies are experimenting with blockchain-based education credentials for their students and employees. Notable for the German context, in May 2019 an international consortium has launched a "Digital Credentials" initiative. Partners include Hasso-Plattner-Institut, TU Munich, TU Delft and several US universities such as Harvard University, MIT and UC Berkeley.[5] In this context of higher education, the Verifiable Credentials for Education Task Force has been introduced. It seeks knowledge exchange and serves to coordinate development internationally https://w3c-ccg.github.io/vc-ed/

In practice, for two credentialing solutions, core building blocks have been open sourced. These are the Blockcerts and the OpenCerts standards. Both initiatives provide extensive code repositories and documentation publicly online, allowing third-parties to adapt the solution to own needs. For both projects, commercial solution providers exist offering customisation and operations through a Software-as-a-Service (SaaS) business model.[6] Motivated by the desire to safeguard education providers against possible lock-in effects from such licensing models, GIZ and its partners at Manila-based learning specialists SEAMEO Innotech joined forces and created Auther[7]. Auther is a free to use, fully operational open source implementation of Blockcerts for the Ethereum Blockchain, extended by application interfaces and templates. It makes use of the OpenBadges standard for certificate representation.

For a long-term view, one should also pay attention to work at the World Wide Web Consortium (W3C), which is the leading international community to develop web standards. In an attempt to ultimately mainstream standardised and open digital credentialing applications across sectors and across the web, the W3C's "Verifiable Claims Working Group" has published a data model for verifiable credentials. This model is now at the verge of becoming an official W3C recommendation. That said, protocols and supporting infrastructure for this data model are still lacking so that this work needs to be regarded as early stag

[5] https://hpi.de/meinel/security-tech/secure-identity-lab/blockchain/digital-credentials.html

[6] Please refer to the document "Solution-mapping_GIZ.xlsx" (GIZ internal) for a detailed analysis of the two open source projects Blockcerts and OpenCerts as well as an overview over commercial service providers.

[7] http://auther.org

Published by:
Deutsche Gesellschaft für
Internationale Zusammenarbeit (GIZ) GmbH

Registered offices
Bonn and Eschborn, Germany

Blockchain Lab
Friedrichstr. 246
10969 Berlin, Deutschland
T +49 61 96 79-0

E blockchain@giz.de
I www.giz.de/blockchain

Berlin 2020

Author/responsible, etc.:
Theodor Beutel/Dr. Uta Meier-Hahn/Franz v. Weizsäcker; Berlin

Design/layout etc.:
Lars Wannemacher, Berlin

Photo credits/sources:
Brett Andrei Martin, unsplash.com

URL links:
Responsibility for the content of external websites linked in this publication always lies with their respective publishers. GIZ expressly dissociates itself from such content.

GIZ is responsible for the content of this publication.