Identification of technologies used for recognising and verifying open credentials

(O3A1)

OEPASS

Authors

Anthony F. Camilleri

Contributors

Denes Zarka, Ildiko Mazar, Ira Sood, Svenja Wiechmann

Editors

Ildiko Mazar

Layout

Tara Drev

Copyright

The Oepass Consortium

Duale Hochschule Baden-Württemberg Heilbronn	DHBW	DE
Stifterverband	SV	DE
European Distance and e-Learning Network	EDEN	UK
Budapest University of Technology and Economics	BME	HU
Lithuanian Association of Distance and e-Learning	LieDm	LT
Knowledge Innovation Centre	KIC	MT
National Distance Education University	UNED	ES
Tampere University of Technology	TUT	FI

This project has been funded with support from the European Commission. This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Table of Contents

1 Scope and Introduction

The scope of this paper is to give an overview into different technologies used for awarding credentials.

2 Paper Certificates

Most records are still issued on paper or other physical formats, although digitisation efforts by governments and industries are proceeding all over the world (Cheng et al., 2016). There is no ‘perfect format’ for certificates, with many countries using hybrid-certificates whereby paper certificates are backed up by digital databases.

However, the significant limitations of each system clearly show a need for a better, more robust certification technology.

2.1 Limitations of Paper Certificates

Paper certificates are still the most widely used, seen in many quarters as being the most secure form of certification, since they are:

- difficult to forge due to security features built into the certificates themselves;
- (usually) held directly by the recipient, who thus has full control over their certificate;
- relatively easy to store securely for prolonged periods of time, e.g. by keeping them in a safe;
- they can be presented by the recipient anywhere, to any person for any purpose.

Furthermore, having been the standard for hundreds of years, paper certificates are built into institutional, regulatory and legislative workflows for practically all use-cases of such certificates.

However, paper certificates also have significant disadvantages:

- while being hard to forge, no certificate is immune from the risk of forgery. Thus, the issuer is obliged to retain a central register of issued certificates that may be used to verify certificate authenticity;
- certificate registries can be significant points of failure: if problems emerge within the registry, although the certificates may remain valid, the ability to verify them could be lost;
- keeping such a register of claims, and answering queries as to the validity of certificates is a manual process, which requires a considerable amount of human resources and time;
- security features in the physical certificate derive exclusively from the difficulty level and expertise required to create the document. The more secure the certificate, the more expensive it is to produce;

- there are no limitations on the ability of the issuer to fraudulently state the timestamp or other details of the certificate;
- once issued, there is no way to revoke a certificate without having the owner relinquish control of it;
- If a third-party needs to interact with the certificates, e.g. to verify claims made in CVs, they need to read and verify each certificate individually and manually, a significantly time-consuming process.

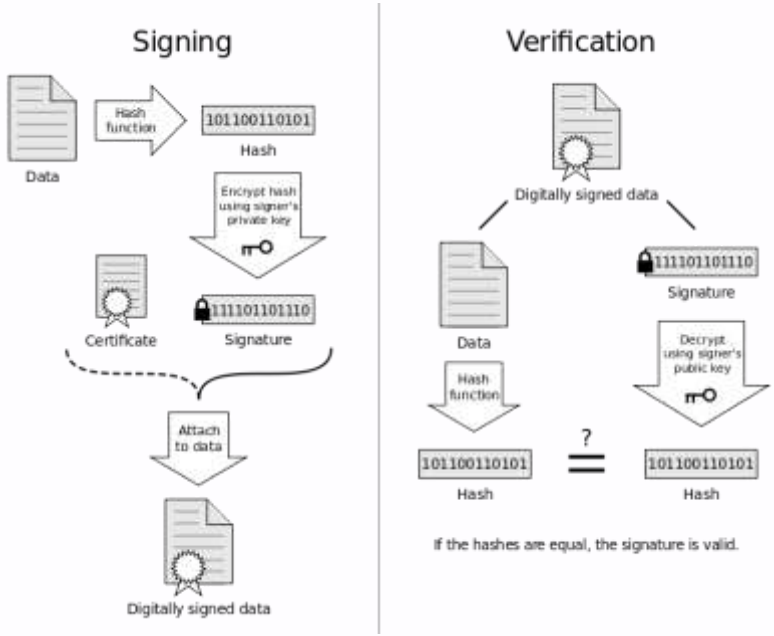
3 Digital Certificates

At a high-level, digital certificates may take three forms, namely:

- Reproductions of paper certificates - these are usually scanned versions or photographs of paper certificates. For many low-security applications, these are considered to be equivalent to paper certificates. These are typically not considered ‘true’ digital certificates, and are not further discussed in this section;
- Unsigned digital certificates - these consist of digital documents such as a PDF or a Word Document. These documents are extremely easy to edit, forge and reproduce at scale - as such their use is not recommended for any trust-based applications;
- Digitally-signed digital certificates - which are both computer-readable and tamper-proof. The security of the certificate derives from the security of cryptographic protocols, which ensure that the certificate is cheaper to produce than its paper equivalent but extremely expensive to reproduce by anyone except the issuer;

Digital certificates hold many advantages over paper certificates in that they require less time and far fewer resources to issue, maintain and use, since:

- the veracity of certificates can be checked against the registry automatically, without human intervention;
- where a third-party needs to use the certificates, these can be automatically collated, verified and even summarised if they are issued in a standardised format;
- digital certificates can be revoked by the issuer;
- they can be multilingual;
- certain types of issuer-fraud, such as changing the timestamp or changing the certificate serial, can be made impossible depending on the design of the system



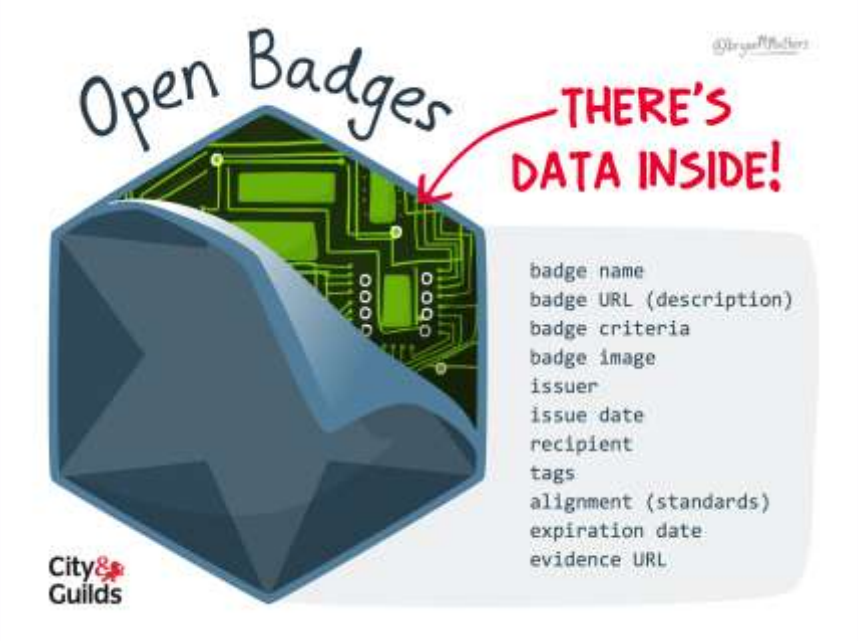
A digital signature is a digital code (generated and authenticated by public key encryption) which is attached to an electronically transmitted document to verify its contents and the sender's identity

Disadvantages associated with digital certificates could be that:

- without the use of digital signatures (i.e. a digital code - generated and authenticated by public key encryption - which is attached to an electronically transmitted document to verify its contents and the sender's identity), they can be easy to forge;
- where digital signatures are used, these require the involvement of third-party certificate providers to guarantee the integrity of the transaction – these third parties have significant control over every aspect of the certification and verification process, which, theoretically, can be abused;
- there is no universally-used open standard for digital signatures, leading to certificates that can only be verified within the context of specific software ecosystems;
- just like paper certificates, electronic records can also be destroyed – keeping them safe requires sophisticated, multi-tier backup systems which are prone to failure;
- should the registry fail, the certificates themselves become worthless since unlike paper certificates, they hold no intrinsic value without the registry;
- registries of digital certificates are prone to large-scale data-leaks.

3.1 Open Badges as Digital Certificates

An open badge is a special digital certificate comprised of a digital image and some metadata. The data can be baked into the badge, meaning that it is embedded into the image file. The individuals and organizations who issue badges create the badge metadata - which is designed to support verification of badges, so that an earner's badges can be checked for authenticity. This Developers Guide provides a set of technical resources to guide through the processes of creating, issuing and displaying Open Badges.



The Open Badge anatomy by Bryan Mathers, City and Guilds
The badge metadata includes information about the learning content, earner and issuer

The Open Badge Standard was originally developed by the Mozilla Foundation with funding from the MacArthur Foundation. Although the standard officially transitioned to the IMS Global Learning Consortium in January 2017, the so-called Mozilla Backpack, a decentralised badge aggregator/repository site where earners can collect and store their badges, is still operational. There are many similar aggregators of open badges in the world like the Open Badge Factory, Credly and others.

The Open Badge Standard is under constant development, in October 2018 the latest version is 2.0. Some consequential updates to this structure are coming with the next version of the Specification, particularly enabling embedding of complete BadgeClass and Issuer Profile documents into an Assertion (and into baked badges). See current issues in progress for details on Github.

The OBI (Open Badge Infrastructure) is a set of software tools and specifications to support people and organizations who want to adopt badging. The OBI is the core underlying technical scaffolding for the badge ecosystem.

The OBI supports a multitude of issuers, including education and training providers, who confer badges into the ecosystem, as well as many displayers and earners using badges to share their competencies and achievements. Anyone can earn badges across many issuers, collect them in one place tied to their identity, then share them with various websites and audiences (including career sites, social networks or personal portfolios).

The OBI aims to support badge issuing, collection and display. This involves:

- allowing earners to tie badges to their identity and carry their badges with them wherever they go

- displaying badges to parties the earner cares about (e.g. employers, college admin, peers)
- allowing earners to manage collections of badges and control visibility of those collections
- All of this is supported within a framework that is open and decentralized to facilitate badging across sites and sources.

Thus, advantages include that:

- badges are easy to collect and display
- granularity of open badges offers a way to acknowledge smaller achievements
- empowering for students in the sense that it acknowledges an achievement
- a combination of badges may help students to self direct their efforts in the right direction
- they can be shared easily
- they capture the learning which might otherwise never be recognized (Devedzic and Jovanovic, 2015)

While open badges have several advantages, including the potentials listed above, they also have limitations. As open badges can be awarded to acknowledge any achievement, including any level of learning of any type (from formal to informal), the quality is determined by the developer. Therefore, when it comes to assessing achievement in learning, the developer has to make sure to assess learner performance properly.

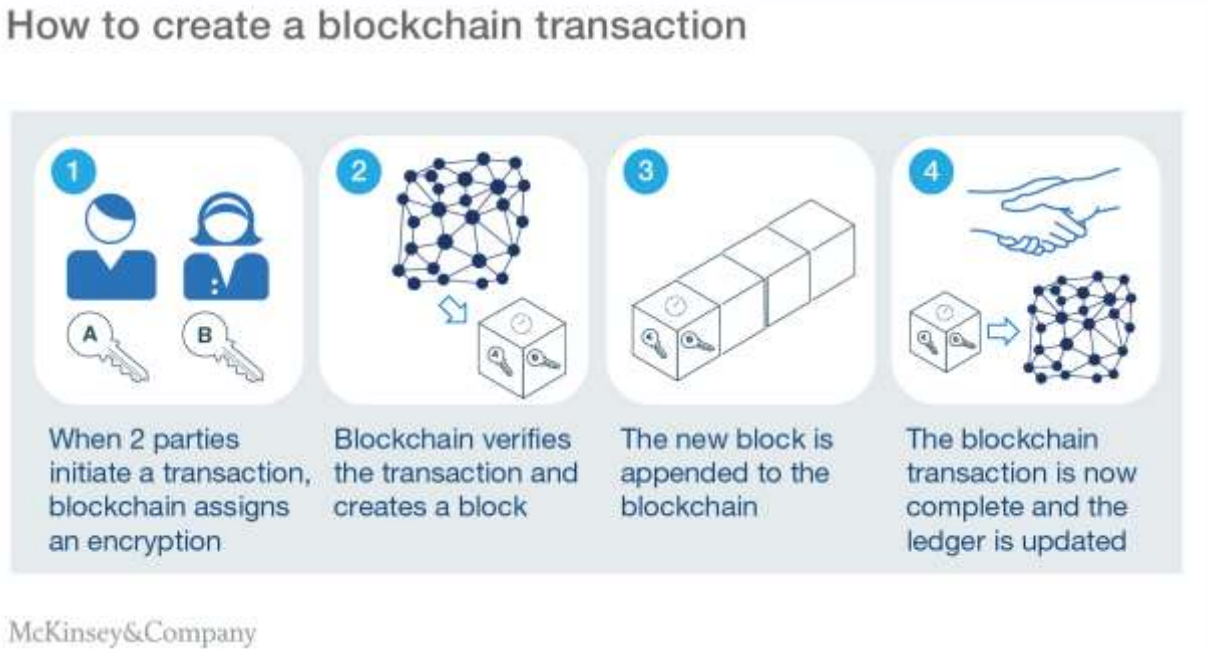
Typical criticism on open badges include:

- The long history of physical badges in military and quasi-military settings might encourage similar hierarchical relationships when employed online.[1]
- Badges are a type of extrinsic motivator that could compete with an individual's intrinsic motivation for accomplishment and mastery.
- Validity: whether they can be viewed as "trusted credentials". In particular:
  - It is difficult to evaluate the real value of a badge
  - Badges are hard to exchange across different institutions, highlighting the problem of commonality
  - It only provides a vague evaluation for the skill, highly subjective in nature and can be interpreted in different ways
- Carpet badging: the fear that too many badges will undermine their value.

Critically, badges are still not successful and acceptable as an educational currency.

[1] Halavais, Alexander (2012). "A genealogy of badges: Inherited meaning and monstrous moral hybrids". *Information, Communication & Society*. **15** (2): 354–373.

3.2 Digital Certificates using Blockchain Technology



Blockchain technology is ideal as a new infrastructure to secure, share, and verify learning achievements (Smolenski, 2016). In the case of certifications, a blockchain can keep a list of issuer and receiver of each certificate, together with the document signature (hash) in a public database (the blockchain) which is identically stored on thousands of computers around the world.

Despite the above listed disadvantages and challenges, digital certificates which are secured on a blockchain could still hold significant advantages over 'regular' digital certificates, in that:

- they cannot be forged – it is possible to verify with certainty that the certificate was originally issued by and received by the same persons indicated in the certificate[2];
- verification of the certificate can be performed by anyone who has access to the blockchain, with easily available open source software – there is no need for any intermediary parties;
- because no intermediary parties are required to validate the certificate, the certificate can still be validated even if the organisation that issued it no longer exists or no longer has access to the issued record;
- the record of issued and received certificates on a blockchain can only be destroyed if every copy on every computer in the world hosting the software is destroyed;
- the hash is merely a way of creating a 'link' to the original document, which is held by the user. This means that the above mechanism allows for the signature of a document to

[2] Note that while this allows for the certificate to be definitively matched to an issuer or receiver, it does not protect against either the issuer or receiver impersonating another person or institution. Preventing identity fraud will likely require public key registries which serve as verified lists of which persons own which public keys, which will likely be maintained by vendors and public institutions as a service.

be published, without needing to publish the document itself, thus preserving the privacy of the documents.

3.2.1 Ideal Characteristics for Recipient

Blockchains address the following ideal requirements for a certificate from a recipient's perspective:

- **independence**: the recipient owns the credential, and does not require the issuer or verifying third-party to be involved after receiving the credential;
- **ownership**: the recipient may prove ownership of the credential;
- **control**: the recipient has control over how they curate credentials they own. They may choose to associate credentials with an established profile they own, or not;
- **verifiability**: the credential is verifiable by third parties, like employers, admissions committees, and verification organisations;
- **permanence**: the credential is a permanent record

3.2.2 Ideal Characteristics for Issuer

Blockchains address the following ideal requirements for a certificate from an issuer's perspective:

- the issuer may prove they issued the credential;
- the issuer may set an expiration time on the credential;
- the issuer may revoke the credential;
- the credentialing system is secure and imposes minimal ongoing burden to remain so.

3.2.3 Other Characteristics

For the actual credential to have meaning and utility, a third-party verifier, such as an institution receiving the credential as part of an application, must be convinced of a certificate's veracity. The following are standard requirements:

- **integrity**: the content hasn't been tampered with; that is, it matches what the issuer originally intended.
- **authenticity**: confidence that the issuer is who the certificate claims, and has not been forged.

3.2.4 Challenges to Blockchain Use

Blockchain is not in itself a panacea to all potential disadvantages of credential systems. In particular, the design of a system would need to take into account:

- How to create a balance between full user control and ownership over data, and protecting the user from mistakes such as password loss;
- How to manage permissions for a ledger - who should have access to do what under what conditions?

- What kind of blockchain to use to reach a balance between security and efficiency (in particular as regards energy and storage costs)
- Interoperability between systems - no global standard currently exists for educational certificates, let alone blockchain certificates;
- How to reconcile the immutability requirement of blockchains with the requirements for the GDPR
- Whether to build incentive schemes for partners running nodes into the chain architecture (mining)

4 Initiatives for Digital Credentials

The following is a list of different European Initiatives for digital credentials:

- Open Badges on the Blockchain - Open University UK, Knowledge Media Institute
  Introduction of OpenBadges data related to the OpenLearn web access into a set of Ethereum Smart Contracts, allowing to store the certificates from different sources in the same place.
  http://kmi.open.ac.uk/review/pdf/kmi-review-issue-10-2017.pdf
  https://openbadges.org/about/
- UNIC's Blockchain Initiative for academic certificates - University of Nicosia
  Use of Bitcoin blockchain technology to issue electronic PDFs verifiable through UNIC's website verification tool or by replicating UNIC's open-source instructions (available at block.co).
  https://block.co/blockchain-certificates/
- Blockchain in education pilots - Government of Malta
  Implementation of a nation-wide pilot project for academic credentialing and professional certifications using Blockcerts open standards, defined by the Malta Qualifications Framework (MQF) and adapted to the European Qualifications Framework (EQF).
  http://connectedlearning.edu.mt/malta-first-nation-state-to-deploy-blockchain-in-education/
  https://www.gov.mt/en/Government/Press%20Releases/Pages/2017/September/15/PR172070.aspx
- Recipient-owned credentials - The University of Melbourne
  Issuance of a Teaching Certificate using the Learning Machine issuing system based on Blockcerts open standards.
  http://newsroom.melbourne.edu/news/university-melbourne-issue-recipient-ownedblockchain-records
- Infrastructure to issue digital certificates - Aristotle University of Thessaloniki PKI
  Issuance of Qualified Certificates for e-Signatures following European Regulation 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS).
  https://pki.auth.gr/index.php.en
- Digital Badge Academy - Sussex Downs
  Use of Digitalme's Open Badge Academy to showcase skills in a "digital and verifiable way" through endorsements by experts, educators and peers.
  https://www.openbadgeacademy.com/sussexdowns

- Teacher's badges - Oulu University, partners, and the Ministry of Education of Finland
  Creation of a new system to be applied across educational sectors which will consist of a shared structure, model, and awarding criteria for badges to recognise the competences of teachers.
  http://www.digital-competences-for-teachers.eu
  http://www.oppiminenonline.com/
- Digital Certificates Project - MIT Media Lab Learning Initiative and Learning Machine
  Development of a system to ensure the management, ownership, transferability, longevity and trust of certificates through tools, software and strategies related to the bitcoin blockchain technology.
  http://certificates.media.mit.edu/
- Blockchain for education - Fraunhofer Institute for applied information technology
  Creation of a platform to facilitate certificates management through smart contracts in the Ethereum blockchain.
  https://www.fit.fraunhofer.de/en/fb/cscw/blockchain.html
- Edubadges - SURF
  Issuance of micro-credentials that cover both formal and non-formal learning and exploration of the use of blockchain in combination with the Edubadges infrastructure.
  https://www.surf.nl/en/innovationprojects/customised-education/edubadges-and-microcredentialing.html
  https://www.surf.nl/binaries/content/assets/surf/en/knowledgebase/2016/whitepaper-onopen-badges-en-micro-credentials.pdf
- Lifelong learning competencies on the blockchain - VDAB & GO!
  Linkage of competencies to individuals through a "bring-your-own-standards" blockchainbased online platform, through which future employers will be able to consult candidates' diplomas but also their skills.
  https://medium.com/wearetheledger/bring-your-own-standard-426da33034ca
- Badgr - Concentric Sky
  Use of a free and open source achievement recognition and tracking system to issue, organise, and share Open Badges offered as a service or as an open source.
  https://badgr.com/
- Digital Badges - Acclaim
  Issuance of badges compliant with the Open Badge Infrastructure (OBI) metadata, allowing users to store and share their badges in their profile or in other OBI-compliant badge wallets.
  https://www.youracclaim.com/
- Credentials Dashboard - Accredible
  Issuance of certificates and badges that are verified in the platform through third parties or by using blockchain technology.
  https://www.accredible.com/
- IndiaChain - Government of India, Niti Ayog
  Implementation of a blockchain-based solution linked to IndiaStack, a government identification database.
  http://indiastack.org/
  https://www.newsbtc.com/2018/02/06/indiachain-governments-blockchain-basedcertification-for-education-degrees/

5 Bibliography

Cheng, S., Daub, M., Domeyer, A., and Lundqvist, M., (2016). Using Blockchain to improve data management in the public sector. Available at: http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/using-Blockchain-to-improve-data-management-in-the-public-sector

Devedzic, V., & Jovanovic, J. (2015). Developing open badges: a comprehensive approach. Educational Technology Research and Development, 63, 603–620. doi:10.1007/s11423-015-9388-3.

Grech, A. and Camilleri, A.F., 2017. *Blockchain in Education* (No. JRC108255). Joint Research Centre (Seville site). http://publications.jrc.ec.europa.eu/repository/bitstream/JRC108255/jrc108255_blockchain_in_education%281%29.pdf

Openbadges-Backpack: Mozilla Open Badges Backpack. JavaScript. 2011. Reprint, Mozilla, 2017. https://github.com/mozilla/openbadges-backpack.

Smolenski, N. (2016a). Academic Credentials in an era of digital decentralisation. Learning Machine Research.

https://en.wikipedia.org/wiki/Digital_badge

Description of the report

An ‘open credential’ could be defined as a credential which is fully transparent and which can be used for a multitude of purposes. These might include accumulation towards a qualification, as evidence of skills for employment or as a means of transferring evidence of expertise between countries. Such an open credential would fit seamlessly into European recognition frameworks, and would be instantly verifiable at the click of a button, and would include all necessary information about the learning it represents. It would also allow collection by various software systems to create online CVs, backpacks etc. Initial work has already been done in this area by MIT and by the Open University (UK).

This report is based research into technologies used for awarding credentials including digitally signed documents, blockchain, open badges, etc. The aim of the exercise was to map the field in such a way as to assess the adequacy of current technological solutions for issuing credentials, and identify any factors which are preventing them from being mainstreamed.

Co-funded by the
Erasmus+ Programme
of the European Union