Blockchain, academic verification use case

Contributors: Federico Bond, Franco Amati, Gonzalo Blousson.

Date: 2015-08-31.

Abstract. To verify the authenticity of academic certificates we propose employing a digital signature scheme and timestamps using blockchain technology, because of its greater transparency, less maintenance and lower cost than traditional alternatives. Based on conversations held on July 31, 2015 on the stage of the first Bitcoin forum organized by the government of Ciudad de Buenos Aires [1-2].

1. Introduction

To unequivocally demonstrate having an academic certificate (university degree, doctorate, or any studies certification) is a process that changes in each country or educational institution.

Some academic centers allow verifying the authenticity of their certificates by a quick and simple online query without even asking who is requiring that information [3-4]. Other delegate the task to third parties [5-6] (either by choice or because of regulations requiring it [7]) or market the service [8]. Finally, there are times when there is no alternative but to directly contact the academic secretary's office at the educational institution, so that we can confirm whether or not a diploma or qualification is valid.

Meanwhile, academic certificate fraud is a reality [9] and comes both by counterfeiting [10-12], and through the complicity of institution’s authorities and staff [13-14]. The frequency of these events is even enough for companies dedicated to detect it to emerge [15].

2. Counterfeit/falsification: digital signature

Detecting a fake academic diploma or degree requires an inquiry to the educational institution that allegedly issued it, using any of the already mentioned methods. In this regard, a more professional, direct and safe alternative is using a digital signature scheme.

Each diploma could include a digital signature to verify unequivocally if it was issued (signed) by the appropriate academic institution (using PKI [16] or simply by posting their public key on their website). The signature ensures the authenticity, integrity and non-repudiation of it.

A variant could be using a digital signature but on a public blockchain [17], this way the academic certificate is not signed, but a cryptographic hash function [18] is applied on it and the result is recorded [19] in the blockchain in a transaction signed by the private key of the

educational institution. Since the blockchain cannot be modified, authenticity, integrity and non-repudiation of the certificate is guaranteed. The disadvantage is that while often inexpensive, recording in blockchains has a cost, while traditional digital signatures don't.

We could also create a data format for academic use, signing and recording the information directly in the blockchain for later reference (no need then to use a cryptographic hash that requires the original diploma). In general blockchain storage capacities are small [20], but depending on the length of our data, the selected blockchain, and the acceptable cost, it may be an option.

Finally, the digital signature scheme can be more specific by adding the signature of several authorities of the educational establishment. In this case, using a blockchain also allows to demand certain requirements, such as minimum number of authorized signatures (P2SH [21]) or any other programmed condition [22].

3. Internal fraud: timestamp

The fraud consists of adding to the academic records of an educational institution to people who actually did not graduated or certified successfully. Often, though not necessarily be so, with the complicity of someone who is part of the academic organization.

If the fraud takes place on the same date of the alleged graduation or certification, technology does not provide a clear solution when the person involved has control over the private keys needed in a digital signature scheme. But if someone tries to show as graduated in the past to whom is not, a solution is to use a timestamp next to the digital signature of each diploma.

Thus, if a person claims to have obtained a university degree a decade ago, then the digital signature with its timestamp has to indicate that it was indeed a decade ago. In this way, the generation of fake degrees in the future by editing university records or databases is prevented.

The problem with traditional timestamp technology (RFC 3161 [23]), besides its cost, is that it requires availability and trust in third parties (Time Stamping Authority) certifying the date. Then its legal use is not universal but up to each jurisdiction, and the possibility of bankruptcy, closure or negligence of who is certifying.

On the other hand, the risk of bankruptcy, closure or negligence can be mitigated by chaining timestamps (RFC 4998 [24]), but this additional complexity not only does not solve the problem at all (trust is still required), but involves an eternal maintenance to preserve the validity of the certified timestamp.

A simpler, economical and straightforward solution to correct the mentioned drawbacks is the use of decentralized blockchains [25-26]. While the time accuracy is far from perfect in many of today's blockchains, it is more than enough where a date is required (not the exact

minute or second in which the certification was signed). In this way, no trust or ongoing maintenance/payments are required to have a valid timestamp.

The method using a blockchain is the already mentioned. A cryptographic hash function is applied on the diploma and recorded in the public blockchain with a transaction that is digitally signed by the academic institution. Given the decentralized nature of a blockchain, the date the information was recorded cannot be altered and is publicly verifiable without intermediaries requiring our trust.

4. Real-world example

An example where either side in conflict could prove the validity or otherwise of a certification happens in Argentina. There, citing government control over the National University of La Plata (UNLP) [27], the press and many lawyers have disputed the existence of a law degree from the President Cristina Fernandez de Kirchner [28-31].

Beyond that the technology of that time made it impossible, have a blockchain been used in the aforementioned manner, the dispute could not exist. On the one hand, it would be easy to prove if a title was truly issued by the UNLP. On the other, it would not be possible to issue fraudulent title decades later because the timestamp would not coincide with the year of graduation.

5. Privacy

The legality, for reasons of personal data and privacy, of recording academic information in a public blockchain changes according to each jurisdiction, data used (names, qualifications, etc.) and certification type (university degree, tertiary diploma or others).

Educational institutions are responsible of knowing the specifics of each case, and this is already seen when requesting a certification verification on many of them [32], which provide information only if they have the explicit consent of the graduate.

However, it is useful to make clear that:

- The result of applying a cryptographic hash function to a diploma does not provide details on the degree neither does it make it publicly accessible. It works as proof of authenticity, if we have the diploma we can verify if the hash recorded publicly corresponds to it, but the other way around is not possible (from the hash we can't know about the diploma).

- If a hash is not used, but a data format is created and the academic details are directly recorded in a blockchain, it is possible to use an encryption algorithm to not publicly expose the information.
  By adding a code to the academic certification to locate and decode the content, we can prevent third parties from knowing what is recorded in the public blockchain

(there are already existing alternatives [33], without the explained advantages, that request a code included in the diploma to check for their authenticity).
Another point of consideration, since there is no possibility of changing the encryption once recorded, is the risk that the chosen cryptographic algorithm gets compromised in the future. In this case, if the data format is not too large (for example, identification, name and degree obtained), using a one-time pad [34] is a possible solution.

6. Conclusion

A digital signature scheme and timestamp solve most of the potential problems with counterfeits and frauds in academic certificates. But it is through a public and decentralized blockchain that these two technologies are combined enhancing their traditional implementations.

The outcome provides greater transparency, lower maintenance and fewer costs than any other existing alternative.

References

[1] http://panampost.com/belen-marty/2015/08/04/buenos-aires-bitcoin-forum-finds-rare-ally-in-city-hall/
[2] https://www.reddit.com/r/Bitcoin/comments/3fimcd/bitcoin_argentina_buenos_aires_gov_forum_310715/
[3] http://registrar.utexas.edu/students/degrees/verify
[4] http://www.itba.edu.ar/es/la-universidad/graduados/buscador-de-graduados
[5] http://www.studentclearinghouse.org
[6] https://www.hedd.ac.uk
[7] http://www.pagina12.com.ar/diario/universidad/10-180464-2011-11-04.html
[8] http://www.ox.ac.uk/students/graduation/verification
[9] http://uknaric.org/2015/06/19/fraud-a-growing-problem-in-education-and-how-to-guard-against-it/
[10] http://www.bbc.com/news/uk-england-32194976
[11] http://www.nytimes.com/2015/05/28/world/asia/axact-chief-executive-arrested-in-pakistan-over-fake-diplomas-scandal.html
[12] http://www.lanacion.com.ar/65882-la-uba-investigara-los-titulos-fraguados
[13] http://indiatoday.intoday.in/story/agra-university-awarded-thousands-of-fake-degrees-reveals-sit/1/457232.html
[14] http://edant.clarin.com/diario/2007/08/15/um/m-01478656.htm
[15] https://www.qualificationcheck.com
[16] ftp://ftp.rsa.com/pub/pdfs/understanding_pki.pdf
[17] https://www.bbvaresearch.com/wp-content/uploads/2015/07/150710_US_EW_BlockchainTechnology.pdf
[18] http://www.unixwiz.net/techtips/iguide-crypto-hashes.html
[19] https://en.bitcoin.it/wiki/Script#Provably_Unspendable.2FPrunable_Outputs
[20] https://github.com/bitcoin/bitcoin/pull/5286
[21] https://github.com/bitcoin/bips/blob/master/bip-0016.mediawiki
[22] http://szabo.best.vwh.net/smart_contracts_idea.html
[23] https://tools.ietf.org/html/rfc3161
[24] https://tools.ietf.org/html/rfc4998
[25] http://www.gipp.com/wp-content/papercite-data/pdf/gipp15a.pdf
[26] https://www.proofofexistence.com
[27] http://www.unlp.edu.ar
[28] http://chequeado.com/ultimas-noticias/icfk-no-tiene-titulo-de-abogada/
[29] http://www.mendozapost.com/nota/16088/
[30] http://www.clarin.com/politica/Sabsay-vuelve-Presidenta-muestre-abogada_0_1236476616.html
[31] http://www.perfil.com/politica/Denuncian-ante-la-Justicia-a-Cristina-por-el-titulo-de-abogada-20141028-0014.html
[32] http://www.cambridgestudents.cam.ac.uk/your-course/graduation-and-what-next/verification-cambridge-degrees
[33] http://sicer.siu.edu.ar/sicer/2.6/consulta.php
[34] http://www.cryptomuseum.com/crypto/otp.htm