Decentralized verification infrastructure for documents anchored to blockchain

Mirko Stanić[1], Matija Pužar[2]

[1]Agency for Science and Higher Education, Donje Svetice 38, Zagreb, Croatia, mirko.stanic@azvo.hr
[2]Unit – Directorate for ICT and joint services in higher education and research, Fridtjof Nansens vei 19, 0369 Oslo, Norway, matija.puzar@unit.no

Keywords
digital documents, digital credentials, blockchain, education, distributed ledger

1. SUMMARY

Digitizing student credentials presents several unique problems. Traditionally the issuers must provide infrastructure for hosting digital documents or chose to outsource it to a third party. In this solution, dangers of potential data breach can never be fully mitigated and the validity of these documents is automatically tied to the existence of the institution that issued them. With the advent of blockchain technology it has become possible to store proofs of existence on a distributed database thus eliminating the need for hosting complex infrastructure as well as rendering data breaches impossible and enabling ownership of the documents to be efficiently managed in the digital space.

2. INTRODUCTION

In order for any digital data exchange format and/or protocol to gain traction, it needs something which can be best described as “display infrastructure”. Software that can read and/or process received files. In use cases which go beyond record exchange between institutions, such as admissions, diplomas etc., it is unreasonable to expect that every stakeholder who wants to verify validity of a document will have the ability or even the desire to host a dedicated verification software. Such an endeavor would require time and resources and also expose the stakeholder to potential data theft. Some countries solve this by means of centralized web portals through which a user with an account can give access to their records to another user. Ignoring the potential data breach of such a solution there are the many other costs included, be they of financial or resource based nature. One also needs to take into account the need for user authentication. This is again sometimes solved through centralized eID systems that are in some cases run by for profit corporations, thus introducing further issues of user tracking and data harvesting. Even in countries where both the eID system and the central data repository are government owned, there is the problem of sharing data with someone in another country. The concept of issuing educational certificates on the blockchain is based on publishing digitally signed hashes of XML, PDF, JSON or other files, containing information about the certificate. The published hash has a twofold purpose, to provide an immutable timestamp of when was the document issued and to ensure that the digital file issued to the user has not been tampered with. In this use case, a person is issued a file whose digital fingerprint is recorded in a transaction on the blockchain. It is important to note that the system being presented here is completely independent of the actual software implementation of the blockchain and that it would be wrong to cater towards one specific blockchain architecture since the only property that is of actual benefit is its immutability. We state that full vendor independence must be observed when implementing long term projects in the digital area to mitigate against potential obsolescence of certain implementations.

3. DOCUMENT ISSUING

We recognize that the ownership of any document is shared between the issuing institution and the receiving individual, and that in some cases, such as credentials, the issuing institution reserves the right to revoke the document. With this in mind, documents would be hashed and the hash would be cross-signed with the institution’s private key to verify their origin and with student’s public key to confer ownership. The institution would use a different private-public key pair for each document derived from a single master seed key in what is known as a hierarchical deterministic key pool. The resulting data would then be broadcast to the rest of the network and added to the blockchain. This scheme allows the issuing institution to revoke the document but denies it the ability to display it. The student on the other hand controls to whom and when he or she will show his or her document.

4. DOCUMENT VIEWING

The display of document would be done by checking the hash of the individual file against the one stored on the blockchain through a smart contract which would check the validity of both keys that were used for signing. The actual physical display of the document represents the most difficult problem in the process. Current solutions rely almost exclusively on smartphone apps which bring a whole set of problems with them. From modification of viewer apps and display of false documents to the theft of users' secret keys by malicious apps or by transmitting touch inputs. The loss of phone or simple hardware failure is also a problem. Our solution does not tie the document to a user derived private-public key pair thereby decoupling the verification infrastructure from the display infrastructure. In order for any digital format to become widely accepted, the cost of viewing/consuming/verifying content has to be minimal. Moreover, if someone wants to verify the validity of a digital document, they should not be required to host and maintain their own verification software. Verification is handled through web based display and verification software. This software can be hosted by anyone and it is only important for the verifier to trust the institution hosting the software. For example, if a university hosts it on its public website that can be considered a trustworthy host, software can also be hosted by other trustworthy stakeholders such as ministries, accreditation agencies, recruitment agencies, companies etc.

5. REFERENCES

Zyskind, G, Oz N. (2015). *Decentralizing privacy: Using blockchain to protect personal data.* Security and Privacy Workshops (SPW), IEEE.

Crosby, M, et al. (2016). *Blockchain technology: Beyond bitcoin.* Applied Innovation 2, 6-10.

Lewenberg, Y, Sompolinsky, Y, & Zohar, A. (2015). *Inclusive block chain protocols.* International Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg

Grech, A, Camilleri, A.F. (2017). *Blockchain in Education.* No. JRC108255. Joint Research Centre (Seville site)

Skiba, D.J. (2017). *The potential of Blockchain in education and health care.* Nursing education perspectives 38.4 220-221.

6. AUTHORS' BIOGRAPHIES

Mirko Stanić

Mirko Stanić has a Master's Degree in Information and communication technology from University of Zagreb (2010). He has worked in Central Applications Office since 2011 as the lead software developer on the Croatian Higher Education Admissions system (NISpVU2). His work is divided between working as a developer in software projects and working as a consultant on specialist projects.

Matija Pužar

Matija Pužar is a Senior Security Specialist and developer from Unit, a directorate under the Norwegian Ministry of Education and Research. Matija received his PhD in 2010 from the University of Oslo, where he also worked as a researcher. Matija has more than 15 years of experience in developing web applications, both back end and front end. In his current position, his focus is on information security and integration services. Matija has been involved in the architectural design and implementation of the EMREX and Erasmus Without Paper solutions.