Response to the Blockchain Position Paper

In the last issue of the GDN newsletter, a short overview of feasibility and usability of blockchain in education written by Mr. Andy Dowling from Digitary was published. While the article covered most of the current landscape in blockchain based credentialing solutions there were some points made about the underlying technology itself which I find needing further clearing up. I would like to comment on the points specifically isolated by mister Dowling as the key takeaways from the article.

"#1: Learners do not need to "own" their record in order to share it with others, they only need access to it."

It can be argued that a person should "own" his or her credentials and not only that but that the credentials in question should also be verifiable without direct connection with the issuing institution. Institutions can be shut down or records destroyed in wartime and natural disasters. If the credential is exclusively stored by the institution, then that record ceases to exist with the institution.

"#2: While self-sovereignty is empowering for the learner, it puts a burden on the learner to keep their records and keys safe and secure, for life."

While it is true that the concept of self-sovereignty places the ownership of the data in the hands of the learner this does not mean that a copy of that record is not also being kept by the issuing institution. From a security standpoint self-sovereignty is about taking digital information offline and handing it over to the user because as long as that information is being hosted it can be compromised. Also it is difficult to verify the identity of a user online, especially in countries which do not have universal national identification numbers. Issuing institution can give its alumni an authentication number or login information but this also represents information which the learner has to keep safe and secure for life.

"#3: Blockchain does not remove the need for an issuer to maintain a repository of records."

The purpose of the blockchain is to remove the need for credentials to be accessible online all the time and with it the organizational and maintenance overhead. It is natural that the institution will have its own copy for legal and archival reasons.

"#4: Blockchain can provide the learner with a secondary verification method in the event that the issuers repository becomes unavailable, provided that the learner keeps their copy of their record."

If the learner loses his or her copy they can always request a new copy from the issuing institution provided it has not been closed down and the learner can lose login information for whatever other digital solution the issuer uses. The key benefits of a blockchain are self-sovereignty and disintermediation.

"#5: By design, blockchain cannot tell if a credential issuer is who they claim to be;"

This is a serious issue with today’s blockchain credentialing solutions and the current solution to it requires the issuing institution to host its public keys on its website which in a way defeats the purpose of a blockchain solution since the closure of the institution also invalidates all issued certificates. There are proposals for using distributed identities as mentioned by mister Dowling but
as of yet there is still no practical way of linking issuers with issued documents in case of issuers closure.

"#6: Blockchain verification is actually more complex and less complete than more established online methods."

It is difficult to understand how a verification against a public ledger can be considered more complex compared to a centralized system with user identity management, customer support, different interfaces for institution, employer and user access, hosting requirements and constant security monitoring.

"#7: Blockchain does not necessarily guarantee the long-term immutability of hashed records."

This is in fact the only thing which the blockchain does guarantee and as the advances in cryptography progress so will the underlying consensus method the same way in which older cryptographic methods have become deprecated in the past. Even in the unlikely scenario that the blockchain becomes cryptographically compromised, the institution can take a copy of the chain created thus far and host it as a private database of hashes, something that would require the hardware infrastructure of a raspberry pi compared to monolithic centralized systems.

"#8: Verifying a record "at source" with the issuer is safer than computing hashes and comparing them to hashes on a public blockchain."

The cryptography used in a blockchain is the same cryptography used in all other forms of secure digital communication and to question the validity of comparing cryptographic hashes would bring into question every other use case for them including digitally signed PDF files.

"#9: Disintermediation is strategically costly to education providers."

The strategic cost described here can be considered a benefit if viewed from the perspective of the learner. Higher education institutions have had alumni organizations even before the advent of the Internet and will continue to have them, what they do not need is the ability to track their alumni throughout their career without their consent. It is also important to take into consideration different concepts of privacy in the US, Canada, Australia and in the EU.

"#10: The financial cost of writing a transaction to a public blockchain can be highly volatile."

Cost of writing to a blockchain has peaked during December of 2017 at about 55 USD and is as of this writing around 0.3 USD (see [https://bitinfocharts.com/comparison/bitcoin-transactionfees.html](https://bitinfocharts.com/comparison/bitcoin-transactionfees.html)). Both of these fees are negligible in case of writing final degree certificates. If the use case requires daily issuance of transcripts or other types of records a sidechain would be used for day to day operation with only the final settlement being committed to the blockchain. This would also make transaction fee costs negligible as in the first case.

Mirko Stanic
Agency for Science and Higher Education
Croatia