Certificates on Blockchain

Preprint · May 2018

CITATIONS
0

READS
115

2 authors, including:

Rohit Sharma
Indian Institute of Technology Gandhinagar
7 PUBLICATIONS **4** CITATIONS

SEE PROFILE

Journal of Universal Computer Science

Certificates on Blockchain

Rohit Sharma
(Indian Institute of Technology, Gandhinagar)
rohit.sharma@iitgn.ac.in

John R. Black
(University of Colorado, Boulder)
jrblack@cs.colorado.edu

Abstract: This report introduces the fundamental principles of the Blockchain leading to a design of a system on its potential for the creating digital certificates which overcomes limitations of Paper Certificates and (non-Blockchain) Digital Certificates. It explains how this technology may both disrupt institutional norms and empower learners of issuing and verifying certificate and gives a new idea to generate certificate in most secure and tamperproof ways using blockchain technology.

Keywords: Blockchain , Certificate , Cryptography , hash , SHA-256 , Consensus , Homomorphic Encryption

Categories: E.3.2, E.3.3, E.3,K.6.5

1 Introduction

This idea investigates the feasibility, challenges, benefits and risks of current technology of issuing and verifying digital certificates(credentials) and how we can improve them with Blockchain. The application of blockchain to education is extremely new – with little peer-reviewed published literature in the area. The architecture build by us in the research shows how blockchain technology can be adopted in current system and beyond to provide ultimate security and reliability to human credentials and digital certificates

2 Blockchain – An introduction

"Blockchain" is rapidly becoming part of the technology vernacular, and yet it remains very much misunderstood. The following high-level definition[8] provides a quick introduction to the subject:

Simply put, a blockchain is a distributed ledger that provides a way for information to be recorded and shared by a community. In this community, each member maintains his or her own copy of the information and all members must validate any updates collectively. The information could represent transactions, contracts, assets, identities, or practically anything else that can be described in digital form. Entries are permanent, transparent, and searchable, which makes it possible for community members to view transaction histories in their entirety. Each update is a new "block" added to the end of a "chain." A protocol manages how new edits or entries are initiated, validated, recorded, and distributed. With blockchain, cryptology replaces third-party intermediaries as the keeper of trust, with all blockchain participants running complex algorithms to certify the integrity of the whole.

There have been experiments with blockchains since the early 1990's, but it was only in 2008, with the release of a white paper by an individual or group of individuals operating under the pseudonym of Satoshi Nakamoto[9] , that blockchains gained wide adoption. The first well-known blockchain was the Bitcoin blockchain, which is also the name of the first widely-used, decentralised cryptocurrency[10] . "Bitcoin" also refers to the network protocol underlying the cryptocurrency. In terms of the popular vernacular, the Bitcoin blockchain is automatically associated with 'the Blockchain' when in practice, there are other blockchains of significant importance, such as the Ethereum blockchain and Hyperledger Fabric.

2.1 Ledgers

Ledgers are tools by which one can determine the owner of an asset at any point in time.From a technical perspective, a ledger is simply a list of sequential, time-stamped transactions structured as follows:

Figure 2: Typical Ledger entry

TRANSACTION NO.	DATE & TIME	SENDER	ASSET	RECEIVER
#	dd-mm-yy hh:mm	Person 1	Description of asset transfered e.g. a unit of currency, a deed toa property or a certificate.	Person 2
#	dd-mm-yy hh:mm	Person 1	Description of asset transfered e.g. a unit of currency, a deed toa property or a certificate.	Person 2

http://publications.jrc.ec.europa.eu/repository/bitstream/JRC108255/jrc108255_blockchain_in_education%281%29.pdf

2.1.1 Blockchains as Public Ledgers

Blockchains are therefore ledgers recording groups of transactions, otherwise known as blocks, which are linked together cryptographically in a linear temporal sequence. Other key properties associated with a blockchain - security, immutability, programmability - depend on the architecture of the blockchain and the character of the consensus protocol it runs by that blockchain. Some blockchains are structured to facilitate peer-to-peer transactions across non-hierarchical nodes; this is known as a "distributed" network structure. Some blockchains, like the Bitcoin blockchain, also ensure the immutability of their ledgers through their unique consensus protocol. To identify who owns a specific asset, a party needs simply to consult the ledger to check who is its most recent owner.

2.1.2 Identity

The cryptography at the core of blockchain technology promises to address identity lacunae and 'wrestle' the ownership and control of personal data back to the individual user. People, businesses and institutions can store their own identity data on their own devices, and provide it efficiently to those who need to validate it, without relying on a central repository of identity data. Blockchain technology does not just provide a new way of digitising bits of paper which have an intrinsic value,

such as our credentials – it provides us with the means to take control of our identity online and manage it appropriately

2.1.3 Trust

Blockchain technology might provide a viable alternative to the current procedural, organisational, and technological infrastructure required to create institutionalised trust.[15] The improved trust between stakeholders is associated with the use of decentralised public ledgers as well as cryptographic algorithms that can guarantee approved transactions cannot be altered after being validated. The distributed ledgers contribute to trust by establishing a fact at a given point in time, which can then be trusted. They achieve this by automating the three roles of the trusted third-party: a) validating; b) safe guarding transactions; and c) then preserving them.[16]

2.1.4 Transparency and Provenance

Blockchain technology provides an indisputable mechanism to verify that the data of a transaction has existed at a specific time. Moreover, because each block in the chain contains information about the previous block, the history, position and ownership of each block are automatically authenticated, and cannot be altered. A single, shared ledger provides one place to go to determine the ownership of an asset or the completion of a transaction.

2.1.5 Immutability

An immutable record is an unchangeable record whose state cannot be modified after it is created.The immutability of blockchains means that it is essentially impossible for changes to be made once established: this in turn increases confidence in the integrity of the data and reduces the opportunities for fraud. For a transaction on a blockchain to be considered valid, all participants in the transaction must agree on its validity nodes or “peers” running the blockchain protocol must come to consensus on the transaction’s validity. The mechanism by which this happens differs from blockchain to blockchain but is generally distributed to some extent, meaning that no one actor can be an arbiter of truth in the network. No participant can tamper with a transaction after it has been recorded to the ledger. If a transaction is in error, a new transaction must be used to rectify the error, and both transactions are then visible in the ledger. Blockchain resilience stems from its structure, since it is designed as a distributed network of nodes in which each one of these nodes stores a copy of the entire chain. Hence, when a transaction is verified and approved by the participating nodes, it is virtually impossible for someone to change or alter the transaction’s data. Attempts to change data in one location will be interpreted as fraudulent and an attack on integrity by other participants, with the result that it will be rejected.

2.1.6 Disintermediation

By replacing middlemen with mathematics, blockchain also can go some way towards maintaining trust (Piscini et al. 2016). Participants on a blockchain are linked together

in a marketplace where they can conduct transactions and transfer ownership of valued assets with each other in a transparent manner and without the assistance or intervention of third-party mediators or intermediaries. A value network operates without a defined central authority. With blockchain technology, peer-to-peer consensus algorithms transparently record and verify transactions without a third-party - potentially reducing or even eliminating cost, delays, and general complexity. For instance, blockchains can reduce overhead costs when parties trade assets directly with each other, or quickly prove ownership or authorship of information --> a task that, is otherwise currently next to impossible without either a central authority or impartial mediator. Moreover, blockchains' ability to guarantee authenticity across institutional boundaries is likely to help parties focus on new ways of authenticating records, content, and transactions in new ways. Greater decentralisation of the internet would place more control in the hands of the user-->or more specifically, the user's devices-->instead of relying on clouds platforms operated by the likes of Google or Amazon.

3 Certification

3.1 What is Certification?

Broadly speaking, certification describes any process by which a certificate is issued as verification of a claim.
Certification is used in many scenarios – for instance, as evidence of:

a] achievement of learning outcomes, irrespective of the form of learning;
b] the competence of a teacher;
c] a learning process undertaken by a learner, irrespective of the form of learning;
d] an educational organisation or course meeting certain quality criteria;
e] an accreditation body being authorized to issue certifications.

As Schmidt (2017a) observes, outdated credential systems limit our ability to create new pathways to education, in particular for those who lack access and need it most. One challenge for people without formal education is to translate their learning into jobs because they often lack credentials affirming their skills and experience. Moreover, existing credential systems vastly favour formal education over other learning experiences, making it harder to develop valuable after-school and after-work education programs – this, despite the clear merits of lifelong learning and informal and non-formal education. Smolenski adds, "The credential has emerged as a transnational, interdisciplinary signal of capability and skill in an environment where other characteristics – language, nationality, religious identity – cannot be presupposed" (Smolenski, 2017). Credentials not only determine who can pass on knowledge, but they also help us identify members of a community who have certain skills (Schmidt, 2017b).

3.2 Ontology of Certification

3.2.1 Components of a Certification

Certification, in its most essential form, is the issue of a statement from one party to another that a certain set of facts are true. Thus, any certification involves the following elements:

1. **The claim** - the statement that "this set of facts is true". Examples within an educational context might include, "a learner has acquired a skill", "a teacher has sufficient knowledge to teach", or "a student has completed an assignment".

2. **An issuer** - a body that has checked and validated the facts, and is certifying that the claim is true

3. **Evidence** backing up the claim, usually including the procedure by which the claim is verified and some additional information about the claim.

4. **A recipient -** the person who is addressed by the claim – the learner acquiring skill, the teacher who has enough knowledge to teach or the student who has completed an assignment

5. **A certificate** - a document that attests the identity of the issuer, the identity of the recipient, the claim and refers to the evidence as necessary

6. **Signature** - A certificate will include a signature which is a unique symbol, stamp, image or code which can only be affixed by the issuer, thus confirming their identity.

3.2.2 Processes Involved in Certification

Certification involves three distinct processes:

1. **Issuing:** this is the process of recording the claim, issuer, evidence, recipient and signature onto a certificate. Often, this data is recorded: in a centralized database of claims; on a certificate issued the user.

2. **Verification**: this is the process by which a third-party verifies the authenticity of the certificate. There are three modalities for doing this:
a) verification using security features built into the certificate itself: this could include measures like checking the authenticity of a seal, special security paper, signature etc.;
b) verification of the certificate with the original issuer, whereby the third-party contacts the original issuer, asking them whether they really did issue the certificate. (Here the original issuer might consult their centralized database of claims, or check the security features built into the certificate themselves);
c) verification by comparison with a centralized database of claims. Here the issuer may have listed all the certificates issued in a third-party database, which would allow

anyone to consult this database to see copies of all certificates issued and compare the two.

3. **Sharing:** this is the process by which the recipient of a certificate shares that certificate with a third-party. There are three ways to share certificates:
a) directly transferring the certificate (or a copy of the certificate) to the third-party, e.g. by e-mailing it, or by showing it to the third-party in person;
b) storing the certificate with a custodian, who is authorized to share only with certain people at your demand (e.g. in the case of a private will, a notary is authorized only to share the contents of the will with the beneficiaries, after a person's death);
c) publishing the certificate, by putting it in a public registry or store, where everyone may consult it.

3.3 Limitations of 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 hybridcertificates 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.

3.3.1 Limitations of Paper Certificates

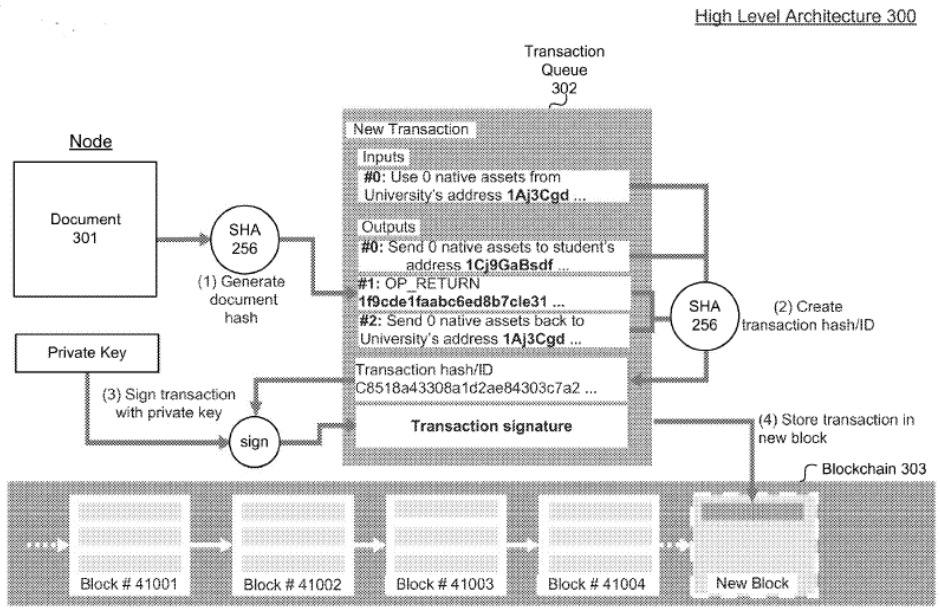
Paper certificates are still seen in many quarters as being the most secure form of certification, since they are:
--> difficult to forge due to security features built into the certificates themselves;
--> (usually) held directly by the recipient, who thus as full control over their certificate;
--> 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.
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 are single points of failure: while the certificates may remain valid, the ability to verify them is lost;
--> keeping such a register of claims, and answering queries as to the validity of certificates is a manual process, which requires significant human resources;
--> security features in the physical certificate derive exclusively from the difficulty level and expertise required to author the document. The more secure the certificate, the more expensive it is to produce. Single secure certificates such as passports routinely cost 1-50
--> 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 use the certificates, e.g. to verify claims in CV, they need to read and verify each certificate individually and manually, a significantly timeconsuming process.

3.3.2 Limitations of (non-Blockchain) Digital Certificates

Digital certificates hold many advantages over paper certificates:
--> they require far fewer resources to issue, maintain and use, since: o the veracity of certificates can be checked against the registry automatically, without human intervention; o 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 for format; o the security of the certificate derives from the security of cryptographic protocols, which ensure that the certificate is cheap to produce but extremely expensive to reproduce by anyone except the issuer;
--> certificates can be revoked by the issuer;
--> 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 However, digital certificates also have significant disadvantages, namely that:
--> without the use of digital signatures, they are extremely 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 can be abused;
--> in many countries, 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;
--> it is easier to destroy electronic records – 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.

4 Proposed Solution: 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. Digital certificates which are thus secured on a blockchain 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
--> 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 be published, without needing to publish the document itself, thus preserving the privacy of the documents.

4.1..1 Ideal Characteristics for Recipient

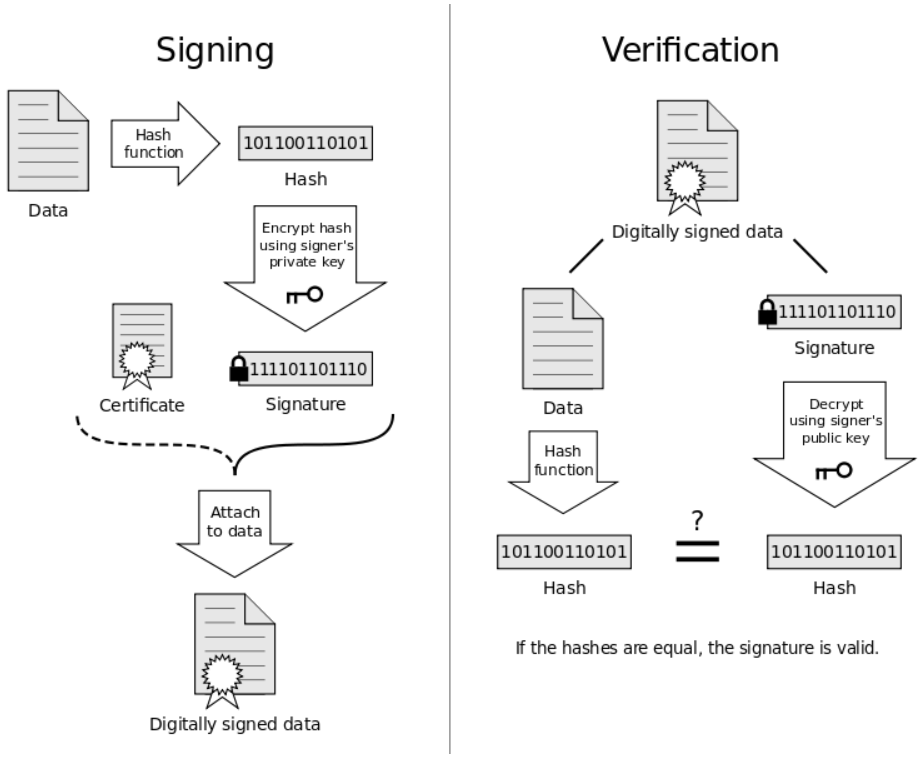
Blockchains address the following ideal requirements for a certificate from a recipient's perspective:
--> independence: the recipient owns the credential, and does not require the issuer or verifying third-party to be involved after receiving the credential;
--> ownership: the recipient may prove ownership 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

4.1..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.

4.2 Issuing Certificates Directly using a Blockchain with Digital Signatures

Pragmatically speaking, a degree certificate holds very little information. It contains the date, awarding institution, awardee and title of degree. Thus, it might read that the University of Colorado, Boulder issued a Bachelors in Technology(Hons.) to Rohit Sharma on 15th June 2017. This is tiny amount of information lends itself well to being stored in a ledger, and would take up little space on the chain. Thus, it could be published on a blockchain either: in plain text, if the purpose is to create a publicly available database of degrees awarded; as a hash of the certificate (using a system such as Blockcerts) if the purpose is to secure the digital certificate awarded to the student. This information can run into several pages, and while it is well suited to storage in a database, it is not well suited to storage in a ledger. Furthermore, it would be prohibitively expensive to store that level of information directly on a blockchain. Therefore, qualifications together with their diploma supplement could be published on a blockchain either: in plain text including a timestamp, awarding institution, awardee, title of degree and link to the full text of the diploma supplement which is held offchain as a hash of the certificate (using a system such as Blockcerts) if the purpose is to secure the digital certificate awarded to the student



A digital signature is different from an electronic signature, which is simply a traditional signature drawn onto an electronic document (for example with an electronic pen), or a scanned physical signature. Electronic signatures are easily copied or forged, and provide no mechanism for verification or standardisation. On the other hand, digital signatures can be used to verify that a specific document was indeed signed by a specific person.
A digital signature provides a way to issue certificates by allowing a person to:
--> mark a document with a stamp that only they can generate
--> ensure the document cannot be tampered once it has been signed. For digital signatures to work they require that each person signing a document be issued with an identity number (a public key) and a linked password (a private key).

Note that : We are applying Hash of the certificate and then applying homomorphic encryption to the Hashed file rather than the whole pdf because calculating SHA-256 is fast but encrypting and decrypting a data depends on the size and is much slower than SHA-256 calculation so instead of digitally signing the whole data issuer will only sign the Hash of the certificate.

4.2.1 Components of a Digital Signature

A digital signature is made up of four components:
a) an SHA-256 hash, which is a type of hash function
b) a public Key;
c) a private Key;
d) a timestamp lists the precise time the certificate was issued.

6.3.2 How to digitally sign a Document (Homomorphic Encryption)

A document is signed by combining the hash of a document with a person's private key to create a new unique code. The resultant signature is then 'stamped' or combined into the document together with the timestamp. Since the signature is a combination of these two components, it:
--> is unique to this specific document, since it was created from the hash of the document;
--> can only have been created from the person who holds the private key. It should be noted that:
--> since the signature is stamped into the digital document, the 'signed' digital document has a different hash value to the unsigned digital document;
--> should even a single letter of the document be changed after signing, this would again have a completely different hash value. Additionally, the signature cannot be reverse-engineered to discover a person's private key. To verify a Digital Signature If a third-party wishes to verify a digital signature, it needs to know the public key of the person who signed the document. Since public keys are effectively just ID codes, they

can usually be looked up in public directories, similar to phone books. Verification software works by inputting the document and the public key, and checks two things:
--> that the signature on the document matches the hash of the original document;
--> that the signature of the document is mathematically related to the public key of the person who claims to have signed the document with their private key. The verification software is able to do this, without ever revealing the private key.

5 Method to issue a certificate

1. A digital file is created that contains some basic information, such as the name of the issuer and recipient, the name of the issuer (MIT Media Lab), an issue date, the credential, which is structured according to the IMS open badges standard, etc.
2. The Issuer then cryptographically signs the contents of the certificate using a private key to which only the issuer has access.
3. The Issuer appends that signature to the certificate itself.
4. The Issuer creates a cryptographic hash of the credential file – the short string of letters and numbers that can be used to verify that nobody has tampered with the content of the certificate. As stated before, there is exactly one possible combination of letters and numbers that corresponds to a digital file, and any change to the file would result in a different hash.
5. Finally, the Issuer uses its private key again to create a record on the Bitcoin blockchain that states we issued a certain certificate to a certain person on a certain date.

The digital credentials themselves can be stored by a user on a hard drive or in a mobile wallet, from where they can easily be shared with others, or even printed out on paper. It is therefore possible for a user to verify who a certificate was issued to, by whom, and validate the content of the certificate itself. 48 The data needed to verify the integrity and authenticity of a certificate is stored on a blockchain. Thus, for example, to validate credentials, an employer (or a company offering verification services) will essentially follow the process above backwards to ensure that the hash corresponds to the original file and that the keys used by the issuer point back to the right institution. Where a permissionless (or public) blockchain is used issuing or receiving certificates, this means that anyone can use the blockchain to ensure that the signatures and verification mechanism are available in perpetuity, as long as at least one copy of the database is running. Verification occurs by comparing the hash of the document being verified with the publicly recorded hash on the blockchain. If they match, the document is authentic. It further means that anyone who receives a certificate that has been signed on the blockchain can verify its authenticity, even if the issuer of the certificate no longer exists. Where a permissioned (or private) blockchain is used, this means that only people who are allowed access into the specific blockchain network would be able to issue, receive or verify signatures on the blockchain.The process looks like this

ISSUER OF CERTIFICATE	HASH / DOCUMENT SIGNATURE	RECEIVER OF CERTIFICATE
1CytUYMWr439wms5MYjryCg5uM-sEhNHYW7	1b3793716c610c1a521d71b2f52c37e4c435d4cd990247ac0cd90a093f5d8fc8	1EUGqyEHbzGQ7hpvkPwm4XJG-FXC3duFvAn
1LSQXVvokuvBfRQUf8Q3rdkhVajK-gwHqoZ	d2bddd4516dd51e617fbb575a8384a1444a009b86d8d5c2440a28ed8d2db3790	1CytUYMWr439wms5MYjryCg5uM-sEhNHYW7
1b3793716c610c1a521d71b2f52c37e4c435d4cd990247ac0cd90a093f5d8fc8	1b3793716c610c1a521d71b2f52c37e4c435d4cd990247ac0cd90a093f5d8fc8	1b3793716c610c1a521d71b2f52c37e4c435d4cd990247ac0cd90a093f5d8fc8

6 Conclusions

The following conclusions can be withdrawn from the above model

- ➔ Only ‘fully-open’ blockchain implementations can reach the real goals and promise of blockchain in education. By this, we mean solutions whose fundamental components include: a) recipient ownership; b) vendor independence and c) decentralised verification. If those aren't all being achieved, using a blockchain is likely to be a waste of effort and resources for all stakeholders.
- ➔ the adoption of digital certificates has been held back by the ease with which they may be forged. The blockchain provides a way for organisations to issue immutable digital certificates which are valid in perpetuity, since their authenticity can be verified against the blockchain. Where certificates are transferred as tokens on a blockchain, even the certificates themselves can be made available in perpetuity.These advantages over current systems significantly increase the value proposition of digital certificates, and will likely push digital certification into the mainstream.
- ➔ Since certificates issued on the blockchain can be automatically verified, educational organisations will no longer need to commit resources to this task, significantly reducing their administrative load, and practically eliminating the ‘after-sales support’ they need to provide to learners following the end of courses88. However, since many organisations also offer this service at a profit, it may also mean that institutions will need to adapt their business models accordingly.
- ➔ Blockchain technology has the potential to revolutionise the management of intellectual property. Depending on the policy choices made, it could be used to increase openness or to close intellectual property
- ➔ By publishing hashes of documents onto a blockchain, a person can provide proof of first publication without actually needing to share the document or invention being published. This turns conventional notions of copyright and patent law on their heads, allowing the possibility for a far more restrictive system whereby knowledge could be protected without being shared.
- ➔ With practically daily news of major data breaches around the world, adopting digital technologies for record keeping has implied a social contract: increased efficiency and effectiveness at a price: less security, privacy and permanence.
  Properly implemented blockchain technology significantly improves all three of these criteria, allowing digital records to have far fewer unwanted side-effects.

Acknowledgements

This study benefited from the input and collaboration of stakeholders and experts throughout Europe and elsewhere, to whom the project team would like to express its gratitude. We are particularly grateful to:
--> Michael J. Casey, Senior Adviser, Digital Currency Initiative - MIT Media Lab
--> Brian Canavan, Senior Associate Registrar – MIT
--> Cédric Colle, Co-founder - Gradbase
--> Alberto De Capitani, Co-founder- Gradbase
--> John Domingue, Director, Knowledge Media Institute - The Open University
--> Daniel Gasteiger, CEO - Provicis
--> George Giaglis, University of Nicosia
--> Patrick Graber, Head of Business Development - Provicis
--> Dan Hughes, President, Learning Machine
--> Chris Jagers, CEO – Learning Machine
--> Darco Jansen - EADTU
--> Soulla Louca – University of Nicosia
--> Ioannis Maghiros - Head of Unit B4, European Commission, JRC
--> Theo Mensen - Stichting ePortfolio Support
--> Kamalesh Dwivedi – Ex CIO, TeleTech
--> Natalie Smolenski, VP Business Development – Learning Machine
--> Colin Tuck, Director, European Quality Assurance Register
--> Philipp Schmidt, Director of Learning Innovation - MIT Media Lab

References

Web

Aglietti, A. (2017a). Proof-of-Knowledge: same Blockchain, different story. Available at:

https://tail.aqquadro.it/proof-of-knowledge-efc138f2a17c

Aglietti, A. (2017b). GROWBIT @ International Open Recognition Day. Available at:

https://tail.aqquadro.it/growbit-international-open-recognition-day-a39281072a6c

CNBC. What is Blockchain? Available at:

https://www.youtube.com/watch?v=8o9QxMxhTp8

Government Office for Science, UK (2016). Block chain technology. Available at:

https://www.youtube.com/watch?v=4sm5LNqL5j0&feature=youtu.be

Wong, J.I. (2017). Microsoft thinks Blockchain tech could solve one of the internet's toughest problems: digital identities. Available at:https://qz.com/989761/microsoftmsft-thinks-Blockchain-tech-could-solve-one-of-the-internets-toughest-problems-digitalidentities

Witthaus, G., Inamorato dos Santos, A., Childs, M., Tannhäuser, A., Conole, G., Nkuyubwatsi, B., Punie, Y. (2016). Validation of Non-formal MOOC-based Learning. An

Analysis of Assessment and Recognition Practices in Europe (OpenCred). JRC Science for Policy Report.

Thompson, Stephen. "The preservation of digital signatures on the blockchain." See Also: the UBC iSchool Student Journal. 3 (2017). Available at: http://ojs.library.ubc.ca/index.php/seealso/article/view/188841/186526

Gupta, M., (2017). Blockchain for Dummies, IBM Limited Edition. Available at: https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=XIM12354USEN&

IBM (2017). Blockchain basics: Introduction to distributed ledgers. Available at: https://www.ibm.com/developerworks/cloud/library/cl-blockchain-basics-intro-bluemixtrs/index.html

Jagers, C. (2017b). Digital Identity and the Blockchain. Available at: https://medium.com/learning-machine-blog/digital-identity-and-the-Blockchain10de0e7d7734

Jagers, C. (2017a). Blockchain-Based Records and Usability. Available at: https://medium.com/learning-machine-blog/Blockchain-based-records-and-usability179a4eeaeb6e

Videos

ASU GSV Summit, (2017). Trust but Verify: Block Chain – Knowledge as a Currency. Available at: https://www.youtube.com/watch?v=x6TDCTiUO9M

Brownworth, A. (2016). How Blockchain works. Available at: https://www.youtube.com/watch?v=_160oMzblY8

Clark, D. (2016). OEB2016 Blockchain for Education. Available at: https://www.youtube.com/watch?v=0ZYnPDirJmA

CNBC. What is Blockchain? Available at: https://www.youtube.com/watch?v=8o9QxMxhTp8

De Filippi, P. (2017). Blockchain Revolution. Meetup Dassault Systemes. Available at: https://www.youtube.com/watch?v=3ukEXQ66_ss

Government Office for Science, UK (2016). Block chain technology. Available at: https://www.youtube.com/watch?v=4sm5LNqL5j0&feature=youtu.be

Future Thinkers (2017). 19 Industries the Blockchain Will Disrupt. Available at: https://www.youtube.com/watch?v=G3psxs3gyf8

Text

(8) Adapted from Piscini et al. (2016).

(9) The original white paper, “Bitcoin: A Peer-to-Peer Electronic Cash System”, was published on 31 October 2008. It described the Bitcoin network protocol and its distributed architecture and followed by a reference implementation a year later. These documents became the foundation for the Bitcoin cryptocurrency.

(10) This study provides a short overview of the technology, ensuring reference to rather than duplication of the JRC 2015 Study "On Virtual and Cryptocurrencies: a general overview from the technological aspects to financial implications".

(15) Government Office for Science, UK (2016)

(16) Piscini et. Al (2016)