Blockchain in Education

Technical Report · December 2017

2 authors:

Alex Grech
University of Malta
6 PUBLICATIONS   **274** CITATIONS

SEE PROFILE

Anthony Camilleri
Knowledge Innovation Centre
23 PUBLICATIONS   **498** CITATIONS

SEE PROFILE

Some of the authors of this publication are also working on these related projects:

RadioActive101 View project

ISO 21001 View project

Blockchain in Education

Alexander Grech
Anthony F. Camilleri

Editor: Andreia Inamorato dos Santos

2017

Contact information
Name: Andreia Inamorato dos Santos / Yves Punie
Address: European Commission JRC, Calle Inca Garcilaso, 3 - 41092
Edificio EXPO - Seville, Spain
Email: andreia-inamorato-dos.santos@ec.europa.eu / yves.punie@ec.europa.eu

JRC Science Hub
https://ec.europa.eu/jrc/en/open-education

How to cite this report: Grech, A. and Camilleri, A. F. (2017) *Blockchain in Education.* Inamorato dos Santos, A. (ed.) EUR 28778 EN; doi:10.2760/60649

Title
Blockchain in Education

Abstract

This report introduces the fundamental principles of the Blockchain focusing on its potential for the education sector. It explains how this technology may both disrupt institutional norms and empower learners. It proposes eight scenarios for the application of the Blockchain in an education context, based on the current state of technology development and deployment.

Contents

Table of Figures

Acknowledgements

Foreword

This *Blockchain in Education* study has been designed and supported by the European Commission's Joint Research Centre's (JRC) unit B4 – Human Capital and Employment. It is an exploratory study located within the Open Education[1] research area in the JRC, contributing to research carried out in the domain of the **recognition dimension** of the Open Edu Framework[2]. This previous research was a study on recognition of MOOC-based learning, of which the outcome was the OpenCred[3] report.

Further research was deemed necessary to understand what can facilitate both the process of issuing and recognising credentials in an increasingly digitised world. The *Blockchain in Education report* aims to fill in this gap. It highlights the growing need for learner empowerment when it comes to handling one's own learning and learning portfolio, tapping into the benefits that openness and decentralisation of processes can bring.

This report has been primarily written for policy makers, education institutions, educational researchers, teachers and learners, and anyone from a non-technical audience who is interested in understanding blockchain and its potential in education.

JRC overall research on [Learning and Skills for the Digital Era](#) started in 2005. The aim was to provide evidence-based policy support to the European Commission on harnessing the potential of digital technologies to encourage innovation in education and training practices; improve access to lifelong learning; and impart the new (digital) skills and competences needed for employment, personal development and social inclusion. More than 20 major studies have been undertaken on these issues resulting in more than 120 different publications.

Recent work on capacity building for the digital transformation of education and learning, and for the changing requirements for skills and competences has focussed on the development of digital competence frameworks for citizens ([DigComp](#)), educators ([DigCompEdu](#)), educational organisations ([DigCompOrg](#)) and consumers ([DigCompConsumers](#)). A framework for opening-up Higher Education Institutions ([OpenEdu](#)) was also published in 2016, along with a competence framework for entrepreneurship ([EntreComp](#)). Some of these frameworks are accompanied by (self-) assessment instruments. Additional research has been undertaken on Learning Analytics, MOOCs ([MOOCKnowledge](#), [MOOCs4inclusion](#)), Computational thinking ([Computhink](#)) and policies for the integration and innovative use of digital technologies in education ([DigEduPol](#)).

More information on all our studies can be found on the JRC Science hub: https://ec.europa.eu/jrc/en/research-topic/learning-and-skills.

Yves Punie
Deputy Head of Unit
DG JRC Unit Human Capital and Employment
European Commission

---

[1] https://ec.europa.eu/jrc/en/open-education

[2] bit.ly/openeduframework

[3] bit.ly/opencredreport

Executive Summary

Blockchain is an emerging technology, with almost daily announcements on its applicability to everyday life. It is perceived to provide significant opportunities to disrupt traditional products and services due to the distributed, decentralised nature of blockchains, and features such as the permanence of the blockchain record, and the ability to run smart contracts. These features make blockchain technology-based products or services significantly different from previous internet-based commercial developments and of particular interest to the education sector – although education, with some minor exceptions, is not currently perceived to be high on the agenda of most countries with national blockchain initiatives. In addition, currently stakeholders within education are largely unaware of the social advantages and potential of blockchain technology. This report was produced to address this gap.

Context

Blockchain technology is forecast to disrupt any field of activity that is founded on time-stamped record-keeping of titles of ownership. Within education, activities likely to be disrupted by blockchain technology include the award of qualifications, licensing and accreditation, management of student records, intellectual property management and payments.

Key Advantages of Blockchain Technology

From a social perspective, blockchain technology offers significant possibilities beyond those currently available. In particular, moving records to the blockchain can allow for:

— **Self-sovereignty**, i.e. for users to identify themselves while at the same time maintaining control over the storage and management of their personal data;

— **Trust**, i.e. for a technical infrastructure that gives people enough confidence in its operations to carry through with transactions such as payments or the issue of certificates;

— **Transparency & Provenance**, i.e. for users to conduct transactions in knowledge that each party has the capacity to enter into that transaction;

— **Immutability**, i.e. for records to be written and stored permanently, without the possibility of modification;

— **Disintermediation**, i.e. the removal of the need for a central controlling authority to manage transactions or keep records;

— **Collaboration**, i.e. the ability of parties to transact directly with each other without the need for mediating third parties.

Key conclusions

This report concludes that blockchain applications for education are still in their infancy, though quickly picking up steam. It describes case studies of implementations at the Open University UK, the University of Nicosia, MIT and within various educational institutions in Malta: each of these implementations is in a piloting phase. However, even from these early pilots it is pertinent to conclude that blockchain could probably disrupt the market in student information systems and loosen the control current players have over this market.

While many of the applications of blockchain technology cannot yet be imagined, we find that within the educational sphere, the following areas are most likely to be impacted by the adoption of blockchain technology in the near future:

(a) Blockchain technology will accelerate the end of a paper-based system for certificates. Any kinds of certificates issued by educational organisations, in particular

qualifications and records of achievement, can be permanently and reliably secured using blockchain technology. More advanced blockchain implementations could also be used to automate the award, recognition and transfer of credits, or even to store and verify a complete record of formal and non-formal achievements throughout lifelong learning.

(b) Blockchain technology allows for users to be able to automatically verify the validity of certificates directly against the blockchain, without the need to contact the organisation that originally issued them. Thus, it will *likely remove* the need for educational organisations to validate credentials.

This ability to issue and then reliably validate certificates automatically can also be applied to other educational scenarios. Thus, one can imagine certificates of accreditation being issued to institutions by quality assurance bodies, or licences to teach being issued to educators, with all of these being publicly available and verifiable by any user against a blockchain.

It can also be applied to intellectual property management, for the tracking of first publication and citations, without the need of a central authority to manage these databases. This enables, e.g. the possibility of automatically tracking the use and re-use of open educational resources.

(c) We find that the ability of blockchain technologies to create data management structures where users have increased ownership and control over their own data could significantly reduce educational organisations' data management costs, as well as their exposure to liability resulting from data management issues.

(d) Finally, we find that blockchain-based cryptocurrencies are likely to be used to facilitate payments within some institutions. The ability to create custom cryptocurrencies is also likely to mean that blockchain will find significant use in grant or voucher-based funder of education in many countries.

We further conclude that the benefits mentioned above are only achieved through open implementations of the technology, which (a) utilise open source software, (b) use open standards for data and which (c) implement self-sovereign data management solutions. This said, many of the solutions being proposed by blockchain solution providers, of which there are already hundreds, fail on at least one of these three criteria, since it is easier to build a business case around keeping control of the software, data or standards. We recommend that further development of the technology in the educational field should be considered as a shared competence of the market and of public authorities, to ensure an appropriate balance of private sector innovation coupled with safeguard of the public interest.

For all this to come to be, regulation and standardisation will determine the extent and speed of progress either forward or backward.

Main recommendations

Considering that blockchain technology clearly benefits from a network effect when applied transnationally, but also that it affects many areas that are the exclusive competence of Member States, we believe that any policy work linked to the blockchain needs to be of shared competence between the EU and Member States, in line with the principles of subsidiarity and proportionality laid out in the treaties.

To ensure development of open blockchain implementations we recommend that the EU in collaboration with Member States consider creating and promoting a label for 'open' educational records, which enshrines the principles of recipient ownership, vendor independence and decentralised verification – and only supports or adopts technologies in compliance with such a label.

We further recommend that policymakers consider investigating and supporting the application of blockchain technology to specific educational use cases, such as those described above, in particular by organising and supporting innovation pipelines to lead to their implementation.

Taking advantage of any technology offerings innovations linked to educational records cannot progress without commonly agreed digital meta-data standards for such records. We therefore recommend that Europe urgently supports standardisation activities in this area.

From a research perspective, we recommend that an expert consultative committee be formed to keep policymakers abreast of developments and their implications on policy while at the same time financing specific implementations and/or projects of interest.

The main beneficiaries of the adoption of blockchain- based technologies in education are likely to be networks of educational organisations and learners. To this end, we suggest outreach to the networks to help them understand the benefits of blockchain technology, and the incorporation of the principles behind the technology into digital competence education for learners.

Related and future JRC work

The OpenCred[4] report of the JRC has previously explored recognition of non-formal, MOOC-based learning. This *Blockchain in Education* report also taps into recognition of learning but from a perspective of certification and credentialisation of both formal and non-formal learning, and argues that globally, governments, enterprises, and start-ups are exploring the blockchain technology/market fit in a wide variety of use cases and for a wide variety of requirements and regulatory demands. However, there is still much that is unknown about the development of trustworthy blockchain-based systems. Further research is required to improve our knowledge about how to create blockchain-based systems that work, and how to create evidence that blockchain-based systems will work as required.

---

[4] bit.ly/opencredreport

1 Introduction

This study investigates the feasibility, challenges, benefits and risks of blockchain technology[5] in education, with a focus on the application of the blockchain to formal and non-formal credentials[6]. It is an exploratory study which is aimed at policy makers and a non-specialist audience

The application of blockchain to education is extremely new – with little peer-reviewed published literature in the area. This study represents an exploratory review of blockchain for education, focusing on the state-of-the-art of the field in Europe. Its primary target audience are policy-makers, educators, strategists and researchers with an interest in securing:

a) A foundation knowledge of a new digital infrastructure which is widely touted in specialist and technical media for its potential to disrupt established sectors;

b) A pragmatic understanding of those areas most likely to be impacted by the uptake of the technology by EU Member States and education institutions currently experimenting with the technology.

The study therefore necessarily bridges desk research with an assessment of early movers in the field, bearing in mind that what is architected in the early days of technology adoption will determine the foundations and vulnerabilities of the future.

---

[5] In this report, we use "Blockchain technology" when referring to the concept of the blockchain; and "a blockchain", when talking about specific use cases of writing a piece of information to a specific blockchain.

[6] Recognition of non-formal learning and new accreditation models are key objectives of the 2012 Council recommendation on validation of non-formal and informal learning which asks Member states to have national arrangements for validation.

2 Purpose, Scope and Objectives

Blockchain technology is a growing area of interest for many industries and universities in Europe and beyond. As a relatively recent innovation in computer science, blockchain is a global, cross-industry and disruptive technology which is forecast to fuel the growth of the global economy for the next several decades[7].

This exploratory study addresses the value decentralized ledgers, in particular those based on blockchain, may bring to stakeholders within the educational sector, with a particular focus on its potential for digital accreditation of personal and academic learning.

Figure 1: Educational stakeholders likely to utilise blockchain technology

EDUCATIONAL STAKEHOLDERS WITH INTEREST IN THE BLOCKCHAIN

BLOCKCHAIN

— Accreditors
— Validators
— Testers

— Employers

— Students

— Teachers
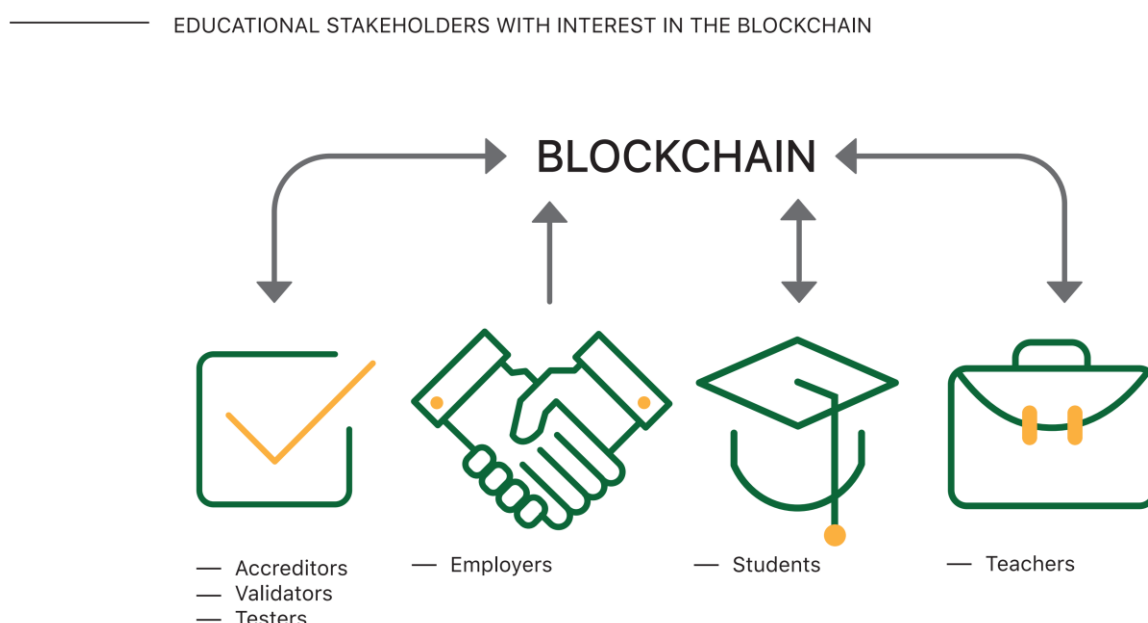
This study focuses on the feasibility, challenges, benefits and risks of the Blockchain as applied to formal and non-formal education credentials. Europe needs to overcome challenges on many fronts where educational credentials are concerned, related to:

a) the need for continuous professional development and re-skilling of its workforce;

b) the facilitation of the recognition of non-formal learning based on individual's portfolios – this being particularly pertinent for open learners and migrants; and

c) the standardisation and scaling up of the process of credentialing issuing and recognition, as well as their access by interested parties.

In this sense, the Blockchain also represents an opportunity for third parties, such as employers, to independently and privately verify that shared records are authentic and unadulterated. This study explores a number of areas that reflect the rapidly-changing socio-political and technical landscape in relation to the subject.

---

(7)   The World Economic Forum (2015) estimates that by 2025 at least 10% of the world's GDP (USD 100 trillion) will be managed via Blockchain technologies, and half of that will be in the form of a crypto-currency.

Furthermore, this study also examines the implications of blockchain technology for management of intellectual property (in particular open educational resources), for management of educational grants, and for enhancing the control of learners over their own data.

The primary objectives of the study are to:

1. provide an introduction to blockchain technology and its core social value proposition;

2. identify and engage with the key issues which are influencing policy-makers and other key stakeholders in considering the use of blockchain technology as a value-added proposition within an education landscape;

3. explain how education institutions and learners can use the technology as a transparent, trusted system for securing, sharing and verifying academic achievements in Europe;

4. determine if the technology is fit-for-purpose for the recording of academic achievements within the short-term, and the likely take-up by European universities and higher education institutions should it be deployed as an open standard;

5. discuss how blockchain technology may help bridge the legitimate need for academic institutions to safeguard their brands and reputations when issuing academic credentials and the aspirations of individuals to maximise their learning portfolio;

6. identify a set of clear opportunities and challenges for the take-up of blockchain technology in higher education institutions. The study also engages with issues relating to interoperability of technology; and how the centralized nature of accreditation and the decentralised nature of the Blockchain could be reconciled

7. make a set of recommendations that may support EU efforts to open up education in Member States by maximising the potential for blockchain technologies. The study will recommend how the EU can play a strategic role in introducing blockchain technology, so it can improve access to educational formal, informal and non-formal opportunities; improve transparency of qualifications; and contribute towards improvements in the education and European employment sector.

This study is primarily aimed at policy-makers in the EU and EU Member States, educators and researchers. It may also be of interest to a more general readership with an interest in an emerging technology, and its deployment within a wider socio-economic context.

3 Methodology

This study is based on qualitative research methods, using desk research, literature review, interviews and case studies to generate evidence. With an emerging technology such as blockchain, with almost daily industry announcements and posts on specialist media, the use of qualitative methods currently represents a pragmatic approach in engaging with the subject at a time when research on the subject is at an embryonic stage, and where case studies involving the blockchain and education are exploratory and / or pilot initiatives.

To this end our research approach involves:

Literature review of any published literature on:

Applications of blockchain technology to education

Non-financial applications of blockchain technology more generally

Digital methods for storing, securing, sharing and verifying academic credentials

Desk Research utilising primary sources covering:

Technical specifications of major blockchain implementations, in particular Bitcoin and Ethereum

Technical specifications of products released by vendors offering products built on top of blockchain technology, as well as of their governing structure, operations and intellectual property arrangements.

Interviews with a sample of researchers, experts, industry representatives, educators, accreditors, testers and learners of relevant stakeholders in the blockchain and educational fields.

3.1 Limitations of the Study

This study is subject to several limitations which are indicative of an early stage, exploratory research area.

1. Blockchain technologies are under active development globally, and there may be recent advances that impact our findings. To mitigate this, we have endeavoured to follow advances in blockchain technologies by monitoring international technology conferences, published academic papers, and grey literature (such as white papers, and blogs).

2. We have used only a small number of use cases. This is factored into the overall exploratory, qualitative approach employed in this study. We do not make claims that rely on statistical evidence about the populations of use cases.

3. The selected use cases may not adequately cover nor be representative of optimal approaches to the blockchain in education. We have made extensive use of our professional networks to secure interviews with leaders in the industry and with researchers and experts. The use case studies were identified and developed as a direct result of this iterative process.

4. The candidates for our use cases may not be optimal in their contribution to the development of blockchain technologies in education. It is possible that alternative case studies exist that better address the dynamic context and requirements for relevant use case studies. We have mitigated this risk by seeking broad input from the literature and from our interviews with industry insiders and policy-makers. We believe we have secured enough relevant and first-hand information for the use cases to conduct an evaluation of the risks and opportunities blockchain-based systems afford to a set of domains likely to influence the decisions and behaviours of the primary stakeholders in the education sector and the target readership for this study.

5. The design analysis we have performed may not be valid, relevant or rigorous enough, since they are yet to be widely-identified, used and studied for blockchain-based systems. However, we believe that the high-level qualitative approaches we employ have been previously used in a variety of other technology domains, so we believe it is reasonable to use them to support the indicative qualitative findings in our study. We believe that the conclusions and recommendations of our study are grounded in an appropriate analysis at this stage in the evolution of blockchain technologies and the very limited take-up by education stakeholders; and that these in turn reveal risks and opportunities that may be commonly encountered in this early stage of blockchain technology development.

6. Our technical descriptions of blockchain technology are intentionally simplified to allow for comprehension by a non-technical audience. Thus, this paper contains no discussion of the cryptographic techniques which underpin blockchain technology, or of the mechanisms of consensus-validation and mining employed by different blockchains.

4 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 (See Annex 3 for an overview of the major blockchains.

4.1 Ledgers

Ledgers are tools by which one can determine the owner of an asset at any point in time. They perform this function by serving as a central authoritative list of transfers of the asset in question.

> In a system or society that has agreed to use a ledger to determine ownership of a particular asset, all that is required to transfer ownership between two parties, is to make an entry in the ledger indicating that this has happened.

From a technical perspective, a ledger is simply a **list of sequential, time-stamped transactions** structured as follows:

---

[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". Also see https://blockgeeks.com/guides/what-is-cryptocurrency for a quick guide to the origins and underlying principles of cryptocurrencies.

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

This simple concept of keeping an authoritative list of transfers of an asset, enables the systematic transfer and accumulation of capital, and as such has been referred to as the essential technology that makes capitalism possible (Windjum, 1978; Yamey, 1949).

The person or organisation that physically owns or controls a public ledger (including the server where the ledger resides, in the case of an online public ledger) is in a position of significant power and influence. Specifically, the owner of the ledger may:

— decide whether to record a transaction, which in turn provides this person with the ability to:

  o impose conditions for individuals to have their transactions recorded; and

  o decide on the system of controls to be applied to check the accuracy of those transactions;

— modify or delete transactions already in the ledger;

— destroy the ledger entirely, or allow it to be destroyed.

Since under such a system, writing, modifying or deleting a transaction in the ledger also changes the ownership of the object, the person or organisation controlling such ledgers also wields significant influence by effectively controlling who owns what - simply by being the custodian of the list of transactions.

The responsibility of keeping accurate ledgers has traditionally been assigned to a variety of institutions: governments control ownership of land by controlling ledgers of property; banks control the world's monetary system by holding the ledgers for currency; while stock exchanges control large shares of the business world by holding ledgers for business -ownership. Since capitalist societies are built around the concepts of sale and ownership (the transfer and accumulation of capital), there are great responsibilities associated with the custodianship of ledgers.

Specifically, these central authorities are trusted to:

provide **witness** – that is, to certify identity and ensure that the persons being recorded in the ledger are who they say they are, and that the assets being transferred exist;

be honest and **transparent** in all transactions – that is, not to divest users of their assets by creating fake transactions or illegitimately modifying transactions after they have been created;

be **secure** – that is, ensure that unauthorized third parties cannot read or write to the ledger (hacking);

not abuse their monopoly by imposing unfair/exceptional costs on their services;

allow persons to **transact** – that is, give access to everyone with a legitimate interest to conduct transactions by listing them on the ledger.

The corollary is that these institutions may individually or collectively cause significant harm or even social chaos by abusing the trust placed in them to accurately keep and maintain these ledgers. The inference is that these institutions have the power to use or abuse their control over the ledgers and exert significant control over individuals and societies within their immediate remit.

4.1.1 Blockchains as Public Ledgers

The most widely-known application of a blockchain is as a **public ledger** of transactions for cryptocurrencies, such as Bitcoin and Ether. As in the case of other public ledgers, the blockchain ledger provides the record of the provenance and transfer of ownership of an asset. The transactional structure of blockchain protocols facilitate not only the transfer of cryptocurrency, but of other digital assets. An asset can be tangible, such as a house, a car, cash, land, or intangible like intellectual property, such as patents, copyrights, or branding. Virtually anything of value can be tracked and traded on a blockchain network, reducing risk and cutting costs for all involved (Gupta, 2017). Since they are designed to record and preserve transactions, all blockchains have traditionally had a digital currency of some kind associated with them as the most basic asset transacted across the network. This has also incentivized the adoption of that blockchain's protocol by paying contributors to the network in its own cryptocurrency.

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.

When describing the blockchain, it is important to understand both a set of social principles that underpin its core ethos and philosophy (its 'social value proposition') – and the characteristics of its underlying architecture to support its social utility (its 'technical characteristics'). The following chapters address these important considerations.

4.2 The Social Value Proposition of Blockchains

In engaging with a subject area like blockchain, the tendency is to first focus on issues relating to digital disruption, the digital economy, knowledge industries and the innovation system. This allows us to understand the context for digital disruption. However, typically it is not only the digital technology that matters: the socio-economic

drivers that create demand for technology (or change in response to it) may be equally, if not more, important. The digital business models that work best have understood people first and digital technology second (Christensen, Clayton M 2003).

Adapting the core arguments in Byrne (2017), Gupta (2017), Hanson et. al (2017), Morabito (2017) and Piscini et al. (2016), it is possible to propose a set of principles that underpin the social value proposition of blockchain technology[11] as a primer to understanding the specific affordances of blockchain technology to the education sector.

4.2.1 Self-Sovereignty and Identity

The early literature on blockchain makes frequent references to 'self-sovereignty', and the individual's ability to own and control his or her own identity online (Lilic, 2015; Allen, 2016; Smolenski, 2016b). According to Au (2017) and Lewis (2017), public blockchains facilitate self-sovereignty by giving individuals the ability to be the final arbiter of who can access and use their data and personal information. Within an educational context, the term is on its way to becoming synonymous with the empowerment of individual learners to own, manage and share details of their credentials, without the need to call upon the education institution as a trusted intermediary.

This can also be thought of as citizens acquiring significant 'self-authority' over the way personal data and identity is shared online, and being able to choose to release all or parts of it in return for access to services they want – *without the need of constant recourse to a third-party intermediary* to validate such data or identity.

> *Identity is… [the basis for] trust and confidence in interactions between the public and government; it is a critical enabler of service delivery, security, privacy, and public safety activities; and it is at the heart of the public administration and most government business processes. How identity information is collected, used, managed, and secured is of critical interest to leaders in the public sector" (Government of Canada)*

Identity is complicated territory for citizens and those who need to verify it: it is the assessment of verifying personal attributes, personal history, relationships and/or transactional histories[12]. Digital identity is verging on a human right. Yet there has yet to be a fail-safe method to deal with one of the flaws of the internet - identifying people or machines online[13]. When citizens are obliged to, or agree to divulge their online identity, new problems are created, such as the use of private algorithms to maximise the commercial use of users' personal data on social media.

Technology is fundamentally changing our ability to represent ourselves. At the same time the nature of our connected world is changing our perception of identity and trust.

([11]) Different blockchain implementations address these principles in different ways and to different extents. Not all the blockchains and / or the applications over different types of blockchains will embrace the entire set of principles underpinning the social value proposition of blockchain technology. There is debate about which is the most likely blockchain to embody the entire set of principles; however, a strong case can be made that, as a public blockchain with a highly distributed consensus protocol, the Bitcoin blockchain is at the top of the list.

([12]) According to Hanson et. al (2017), the assessment of identity is used to minimise any perceived gap in trust. This gap is proportional to the measure of risk, which reflects the perception of the identity and any potential losses. *The trade-off is often a loss of privacy in exchange for access to high value transactions.* The downside has historically been the loss of privacy where the transaction is asymmetrically of moderate to minimal value to the individual being vetted compared to the risk presented to the other party. In order to verify certain attributes of their identity to complete the transaction they also expose other attributes of their identity they may not wish to disclose. This disclosure places all of their attributes, on that document, at risk of further unwanted disclosure or illegal use.

([13]) See https://qz.com/989761/microsoft-msft-thinks-blockchain-tech-could-solve-one-of-the-internets-toughest-problems-digital-identities/

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 (see section 5 for further information on the affordances of the Blockchain to credentials and certification).

In fact, some have argued that full digital self-sovereignty may eventually depart from the sharing of anything like a permanent "identity," but instead become a system of verifying claims. In other words, rather than soliciting extraneous information, querying parties will instead request only information that is immediately pertinent to the transaction at hand: Is the individual over the age of 18? Did they receive a PhD in Neuroscience from MIT? Are they a citizen of Italy? Once verified satisfactorily, claims can then be retracted by the subject[14].

4.2.2 Trust

An influential UK Government study[15] suggests that trust is a risk judgement between two or more people, organisations or nations; and that in cyberspace, it is based on two key requirements:

a) **authentication** – *prove to me that you are who you say you are*;

b) **authorisation** – *prove to me that you have the permissions necessary to do what you ask.*

If one of the parties is not satisfied with the response, they may still choose to allow the other party to proceed, but they would be incurring risk. However, there is no viable relationship unless the parties trust one another. In this sense, being trustworthy in a society is analogous to being creditworthy.

This basic concept of trust remains unchanged in the digitised world where we have to rely upon many actors, whom we will never meet, to act in good faith and on our behalf: trust is often granted only for a very specific application, within a specific context, and for a set period of time. In a global, digital economy, the challenges of maintaining trust - with the resultant checks and balances – are becoming increasingly expensive, time-consuming, and inefficient[16].

Blockchain technology might provide a viable alternative to the current procedural, organisational, and technological infrastructure required to create institutionalised trust. 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.

The hope is that in the same way that the Internet reinvented communication and impacted social behaviour, blockchains may similarly help address the current lacunae in transactions, contracts, and trust – key underpinnings of business, government, and society.

---

[14] See Andreas Antonopolous in the "ADISummit: Self-Sovereign Identity Panel." Available at:
https://www.youtube.com/watch?v=DZbyiJqKT8c

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

[16] Piscini et. al (2016)

4.2.3 Transparency and Provenance

Ease of sharing and visibility are essential features of a blockchain; the lack of one or the other of these features in current systems is often a central driver of blockchain adoption. They become particularly critical in transactions in which more than one organisation is making blockchain entries.

Blockchains empower participants with information on the origins of each asset or record and how its ownership has changed over time. However, this transparency only functions if blockchain transactions are linked to an identifier. Without a public identifier, such as a linked document or serial number, blockchain transactions cannot be decoded and tracked. In this way, blockchains—even "public" blockchains—are private by default, but can also be used to track transactions of specific individuals over time via linked "off-chain" data.

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.

4.2.4 Immutability

An immutable record is an unchangeable record whose state cannot be modified after it is created.

Immutability is interlinked with security, and its classic properties of confidentiality, integrity and availability. Immutability is also about resilience and irreversibility. Blockchain data cannot be easily changed because it is continually replicated across many different locations. With private and public key cryptography as part of blockchain's underlying protocol, transactional security and confidentiality become virtually unassailable.

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.

4.2.5 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.

4.3 Types of Records stored on Blockchains

Blockchains are typically used to store **records** of:

1. asset transactions;

2. smart contracts;

3. digital signatures and certificates.

4.3.1 Asset Transactions

Records of transactions of assets typically take two forms:

— Money, expressed in **units** of a **currency**: each single unit of the same currency has an identical value as every other single unit at any one time. Currencies are also intra-convertible at an exchange rate. The most common form of currency built using blockchain technology is Bitcoin.

— Documentary evidence of ownership rights, legally known as **title deeds.** These are commonly used to represent immovable property such as land, or intangible property such as intellectual property rights.

4.3.2 Smart Contracts

Smart contracts are effectively small computer programmes stored on a blockchain, which will perform a transaction under specified conditions. Thus, a smart contract is typically a declaration such as "*transfer X to Y if Z occurs*". Unlike a regular contract where after reaching an agreement, parties must execute the contract for it to take place, a smart contract is **self-executing** - that is, once the instructions are written to a blockchain, the transaction will take place automatically when the appropriate conditions are detected, with no further actions required by the parties to the transaction or other third parties.

The promise represented by smart contracts is that after an industry's important digital records are verifiable, a whole new ecosystem of technical automation will start to evolve to produce a new social fabric that enables civic efficiencies, personal mobility, and institutional transformation. Within this context therefore, smart contracts represent an automated view of the future[17].

---

[17]   Also see https://github.com/Azure/azure-blockchain-projects/blob/master/bletchley/AnatomyofASmartContract.md

4.3.3 Certificates and Digital Signatures

In its most essential form, certification is the **issue of a statement from one party to another that a certain set of facts are true** (see section 6).

Signatures are proofs that the statement was issued from and to the said parties.

Blockchains can be used to either store cryptographic hashes ("digital fingerprints") of the certificates, or to store the claims themselves[18]. Thus, a blockchain can take on the function of a public certificate registry.

4.4 High-Level Overview of Blockchain Architecture

A blockchain is a ledger linking sequential "blocks" of transactions whereby:

— Every person who wishes to trade any asset across a private or public network requires access to the network. This access occurs via a software application that mediates between user and blockchain. The software application, often called a "wallet," can be installed directly on a device or accessed via a web browser. Depending on how it is designed, a blockchain wallet can be used to send and/or receive digital assets. Some wallets allow for direct transacting without a mediating third-party, while other wallets are run by third parties who maintain custodianship of users' digital assets on their behalf.

— Those users wishing to participate in validating transactions through consensus must generally to install the blockchain software on their device. This is used to write to the ledger, store an entire copy of the entire ledger and keep all the copies of the ledger perfectly synchronised. Because public blockchains allow anyone to install the software and have a copy of the entire ledger, anyone can transact directly on the Blockchain within the network, and no third parties can impose conditions for access. In permissioned blockchains, a centralized authority determines who has access to run a node and participate in the consensus process.

— The transaction-records, or blocks, in a blockchain are linked together cryptographically, rendering them tamper-proof. Unlike records in digital databases, which can be altered, once a transaction is recorded and time-stamped on the Blockchain, it is impossible to alter it, or delete it.

— The blockchain records the fact of the transaction, that is, what has been transferred, the parties involved, as well as structured information (metadata) related to the transaction and a cryptographic hash ("digital fingerprint") of transaction content. This unique signature is used to verify transactions later: if someone alters the transaction content, its resulting unique code no longer matches the version that is on the chain, and the blockchain software will highlight the discrepancy.

— All parties involved in a transaction, and *only those parties*, must provide their consensus before a new transaction record is added to the network. All other nodes in the network will *only* verify that the two parties have the appropriate capacity to enter into the transaction. Thus, as soon as one party agrees to send the asset, and the other party agrees to receive the asset, and the nodes verify that each party has the capacity to conduct the transaction, it is completed.

— All computers in the network continually and mathematically verify that their copy of the blockchain is identical to all the other copies on the network. The version running on the majority of computers is assumed to be the 'real' version, so the only way to 'hack' the records would be to take control of over half of the computers on the network. For a blockchain running on thousands (or even, in the

---

[18] This is a particularly true where the claims can be expressed in terms of tokens, such as the acquisition of credits

future, millions) of computers, as public blockchains like Bitcoin and Ethereum do, this would-be a near-impossible task. Destroying the ledger entirely would require deleting every copy of it in the world.

5   Certification

5.1 What is Certification?

Broadly speaking, certification describes any process by which a certificate is issued as verification of a claim.

In education, certification is used in many scenarios – for instance, as evidence of:

- achievement of learning outcomes, irrespective of the form of learning;
- the competence of a teacher;
- a learning process undertaken by a learner, irrespective of the form of learning;
- an educational organisation or course meeting certain quality criteria;
- 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).

5.2 Ontology of Certification

5.2.1 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. Thus, for example if an institution certifies that a student has received 1 ECTS worth of learning, the ECTS manual sets out how the components and procedure of verification of that claim. In this example, the procedure involves testing the student on the achievement of a specified set of learning outcomes, which have been achieved through approximately 25 hours of learning

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. 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.

5.2.2 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.

5.3 Enablers for a Trusted System of Certification

While any person can issue a certificate to any other person, attesting to anything, the objective of a system of certification is for certificates to be widely accepted by third parties. This requires the third parties to have significant **trust** in the system and its processes.

Trust within the context of certification is created through the following methods and processes:

5.3.1 Method for Identity-Verification

This involves creating trust by verifying who is involved in the transaction. Since a certificate involves **the issue of a statement from one party to another**, it is important to be able to verify the identity of both the issuer and of the certificate holder. Identity is typically verified using identity-documents, which themselves are certificates attesting to a person's identity.

Where verifying identity documents can be complex, often third parties are involved to verify the identities of either of the parties.

5.3.2 Standardised Processes for Issue & Certification

Solely knowing the identity of the parties in a transaction would mean that third parties would need to have complete trust in the former. Since these circumstances rarely come about, it is necessary to also have trust in **how** the certificates are released, specifically by showing the methodology by which the issuer has arrived at the conclusion stated in the claim.

It is also necessary to ensure that all certificates within a system are issued **predictably** and **equitably**, i.e. that a certificate will be issued to any person once they meet a certain set of criteria, and only when they meet that set of criteria. This requires that the methodology be documented in a standard[19], which is adhered to by all issuers.

Where a system of certification has multiple issuers, and each issuer applies individual or proprietary standards to issue certificates, the inevitable result is the creation of multiple sub-systems. These would, in turn, need to be individually and independently understood and verified to create trust. Therefore, in a system with multiple issuers, the higher the level of standardisation in place across the network, the higher is likely to be the level of trust inherent in that system of certification.

5.3.3 Mechanisms for Regulation and Assurance

Once a standardised system of certificates is established, one must still trust that each of the parties in the system acts in good faith and applies those standards in line with their requirements. Thus, a system of certification that includes a mechanism to verify that the parties are acting in good faith, and to expose (and possibly remove) parties that do not, leads to a higher level of trust in the entire system.

5.3.4 Security Features

A third-party wishing to verify the authenticity of a claim in a certificate must be able to ensure that such certificate is not forged. There are two ways to prevent such forgeries:

— through physical anti-forgery mechanisms such as signatures, watermarks, special designs incorporated into the certificate itself, which ensure that only the issuer could have made that specific certificate;

— through a database of issued claims, held either by the issuer or in a centralized database known as a *registry,* whereby a third-party can check that the claim has indeed been issued.

5.3.5 Accessibility

The final element for trust in a certificate is for the claim to be easily accessible. This implies that:

— the recipient of the certificate should be able to hold a copy of the certificate;

— third parties who require access to the certificate should be granted it easily either by the holder, the issuer or a registry;

— the certificate should contain information as to how to verify the claim, and the standards and processes used to make the claim and issue the certificate;

— the information in the certificate should be clear, legible and easy to use. Ways to do this include:

   - standardising the content of the certificate itself;

   - ensuring that the certificate is machine-readable.

([19]) Standards may be open, proprietary or statutory.

5.4 Uses of Certification in Education

5.4.1 Uses of Certificates issued to Learners

Certificates are used widely throughout education, for a variety of purposes. Certificates are typically issued to learners to recognise:

— the completion of a specific learning experience. Examples of this might include a school-leaving certificate in formal education, a certificate of attendance/participation in non-formal education, or a certificate attesting a mobility experience;

— the totality of learning achieved in a specific area, example for a certificate attesting the award of a degree;

— discrete units of learning, through the achievement of specific learning objectives, for example through the award of ECTS credits in Higher Education;

— specific experiences which contribute to learning, such as certificates attesting the completion of an apprenticeship, or of another kind of work-experience;

— the acquisition of specific skills, such as through certificates awarded in procedures for the recognition of prior learning;

— the achievement of certain excellence criteria, for example by winning certain prizes for achievement, or graduating '*with honours*';

— the specific level of competence achieved in specific areas, through the issue of examination certificates or grade-cards.

Typically, certificates issued to learners are used by stakeholders interested in the **evidence of an individual's learning**. For instance: educational institutions are interested in this for determining an individual's suitability to progress to another level of education; recruiters and potential employers are interested to determine suitability of a candidate for open employment opportunities.

Literature also points to the uses of certification as a motivational tool in education, through the gamification of learning by awarding certificates for the achievement of specific intermediate learning goals (Gibson et al, 2015; Abramovich, Schunn, & Higashi, 2013). This ongoing formative assessment and certification has been shown to improve concentration, recall and overall learning outcomes.

5.4.2 Use of Certificates for Accreditation

Accreditation is a procedure by which an authoritative body gives formal recognition that a body or person is competent to carry out specific tasks (ISO/IEC 18009:1999). Accreditation is usually attested by means of a certificate. Multiple forms of accreditation are used in education:

— educational organisations are accredited, to be licenced to operate. Examples of such accreditation includes accreditations issued by governments to universities or schools; and accreditation issued by software companies to training centres to teach specific software packages;

— specific educational programmes are accredited, to be allowed to be taught within accredited educational organisations;

— teachers are often accredited for a specific skill-set to be allowed to claim that they are teachers, and teach in specific schools;

— agencies that accredit schools and teachers are themselves accredited by high-level supervisory agencies, which ensure that they issue their accreditation according to set rules. An example of such an accreditation is that awarded by the European Quality Assurance Register (EQAR).

Many of these certificates and accreditations are typically linked into accreditation chains. Thus, for example a student may be awarded a certificate attesting a degree only if it has been issued for an accredited programme, which was in turn issued by an accredited university, which in turn was accredited by an accredited quality assurance agency. An example of such an accreditation structure, typical for European Higher Education is displayed below:

Figure 3: Outline of a Trust & Recognition Structure for Qualifications in Europe

OUTLINE OF A TRUST AND RECOGNITION
STRUCTURE FOR QUALIFICATIONS IN EUROPE
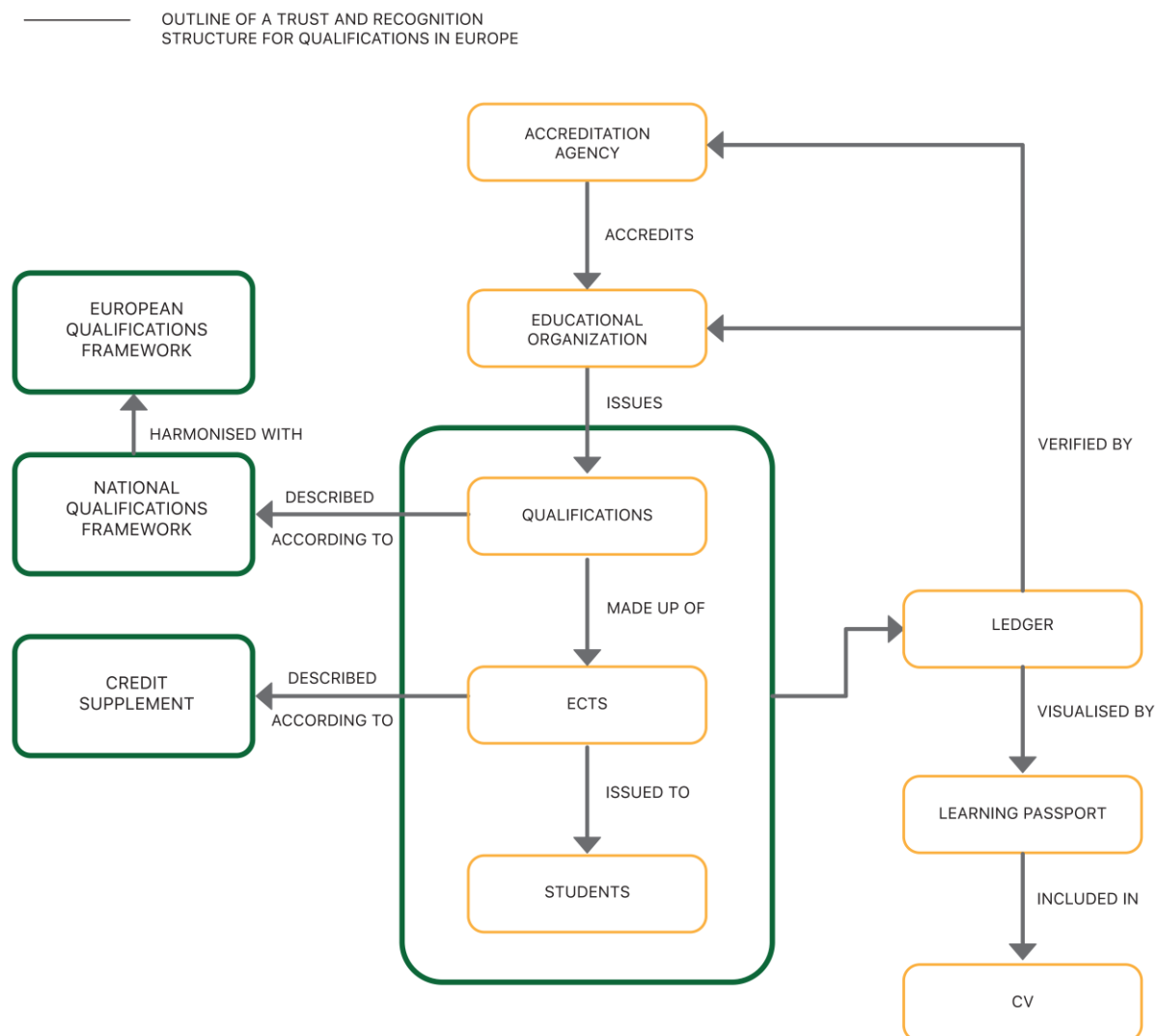
Source: Camilleri, Anthony (2017): Outline of a trust and recognition structure for qualifications in Europe. See https://doi.org/10.6084/m9.figshare.5372758.v1

5.4.3 Uses of Certificates for Tracking Intellectual Property

Registering and tracking intellectual property is a key part of all academic systems. Intellectual property creates value and in turn its use may apply costs.

To this end, a host of central authorities are used to manage intellectual property of various kinds. In particular:

— research journals certify that a piece of research is new, and that the research has been conducted in line with rigorous scientific standards – this information is used to determine *scientific truth*;

— Data companies certify the number of times a piece of research or an open educational resource (OER) has been used. This is used to determine the *significance of the research or the OER*, and often to compensate the author accordingly;

— patent offices certify the first inventor of an invention, and award them a monopoly to market and profit from that invention for a number of years.

5.4.4 Uses of Certificates for Financial Matters

Certificates are also used extensively for financial reasons, including to track:

— receipts of payment;

— award of student grants;

— award of student loans;

— waivers and/or modifications to student loans.

5.5 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 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.

5.5.1 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 €20-€150;

— 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 time-consuming process.

5.5.2 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.

5.6 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[20];

---

[20] 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.

— 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.

5.6.1 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 (subject to the limitations discussed in 10.3)

5.6.2 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.

5.6.3 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.

5.7 Certifying Identity using a Blockchain

From a technical perspective, a person's identity is made up of the sum of all their personally-identifiable information (PII).

When a person wishes to confirm their identity to another person or institution, they will share much of that personally-identifiable information. Therefore, for example a prospective student might confirm their identity to a university admission's office by providing their name, address, government identification number, gender and grades. Typically, the admissions office will keep all this data in a centralised database, requiring the user to trust them to care for the safety of their data. However, due to the value of such data, it is extremely susceptible to risks such as abuse, fraud and theft, as demonstrated by a recent spate of high profile big data thefts from governments and corporations around the world. Currently, every time a person needs to conduct a transaction with a new person or organisation, they again need to hand over their data and give yet another person control over how that data is safeguarded and shared.

Blockchain technology enables a new concept of **self-sovereign identity**, whereby a user stores their own personally identifiable information on a personal device such as a smartphone, and only shares it with third parties as necessary. This is the digital equivalent of keeping your paper certificates in a safe at home, and displaying them to a third-party to prove your identity, but keeping control over whether these third parties can copy such documents or not. Blockchain technology furthermore allows for the user to certify their identity without needing to share the underlying data that makes up that identity.

5.7.1 Using a Certified Self-Sovereign Identity

Once a person has a fully-complete self-sovereign identity:

— their personal data is digitally stored on a device to which only they have access, and which they control, such as a device-level wallet;

— a hash of that data, whether consisting of claims or digital documents, may be stored on the blockchain;

— the truthfulness of that data is certified by third parties, such as an issuing or verifying institution where the certificates are also:

  o stored on the secure device with the rest of the person's data;

  o hashed on a blockchain.

With these elements, a person can securely identify themselves to any party who also trusts the verifying institution, simply by proving that they are the owner of the public key associated with the certificate claim, and without the need to share any piece of personally-identifiable information – not even their name.

Thus, to continue our example, once the student at the university has received a scholarship, they might need to identify themselves as a scholarship recipient to other parts of the university to receive services. For example, they might be entitled to free books from the university bookshop. Traditionally, the university bookshop would need to hold the data of which students are entitled to scholarships and free books to be able to offer this service. Thus, to receive free books, the student would need to allow a bookshop to hold extremely sensitive information from which one could infer the student's financial situation and that of their family. With a verified self-sovereign identity, the bookshop would not need to hold any data. The student would simply turn up, present the "scholarship recipient" claim (stored on their phone or another device), then prove that they are the owner of that certificate claim by entering their password or scanning their fingerprint on their phone. Since the bookshop owner trusts the certificate issuer (i.e. the admissions office) to have verified the identity appropriately, and can trust the certificate due to the security and immutability of the blockchain, they could give the student books, without the need to store any piece of information whatsoever about the student.

5.8 Issuing Certificates Directly using a Blockchain

Wherever a certificate can have a measurable value, it can be represented as a token, and traded directly on a custom blockchain. Thus, for example on a blockchain for:

— school-leaving certificates, a single certificate might be considered as one token;

— educational credits, 1 ECTS would equal one token;

— tracking references to journal papers, one reference might equal one token.

Thus, certificates could be transferred from one person to another, simply by transferring a token on the blockchain. Additional information on the certificate could be stored either:

— directly on the blockchain; or

— by linking to it from the blockchain entry.

Thus, it is possible to design a database where some information would be private and held by the user, while other information would be held publicly on a blockchain.

The advantage of issuing certificates directly on a blockchain is that the certificates themselves, rather than just the proof of their signing, become immutable and permanent.

The disadvantage is that any general purpose blockchain used in this manner would grow significantly in size, which means that it would lead to low performance and high resource usage. Thus, such a model could only be implemented as a private/permissioned blockchain (See Section 10.2 for a further discussion of resource usage of blockchains).

Issuing a Diploma Supplement on a Blockchain

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 Malta issued a Bachelors in Science (Hons.) to Jane Doe 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.

Graduates in the European Higher Education Area, have the right to receive a diploma supplement along with their qualification which additionally indicates:

- its level and function of the qualification;

- the contents and results gained;

- certification of the supplement;

- details of the national higher education system concerned;

- any additional relevant information.

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 off-chain

- as a hash of the certificate[21] (using a system such as Blockcerts) if the purpose is to secure the digital certificate awarded to the student.

---

[21] Remember that the hash of the document will always be the same length, irrespective of the length of the document.

6 Technical Characteristics of Blockchain Technology

This chapter describes the technical underpinnings of blockchain technology. Readers who wish to understand *how* blockchain technology accomplishes the claims made in the previous chapter should read on. For those who wish to take these claims at face value, without delving into the technical architecture, we recommend skipping the chapter.

6.1 Principles of Blockchain

6.1.1 From Centralisation to Distribution

A centralised ledger is a single, authoritative list of transaction records. An example of these might include a national land registry. In computer terms, a centralised database is stored and executed on a single central node.

A variation of a centralized ledger, with an element of distribution, involves several parties sharing responsibility for different parts of the single authoritative ledger. Thus, consider a national land registry which is administered by regional offices, each of which only process and store transactions within their jurisdiction - but all of which ultimately form a single database of national land transactions. In a computerized implementation of this, each node only stores its part of the database and executes its part of the code.

If the central computer (server) goes down, access to its ledger is prevented.

Decentralising and distributing a ledger involves the removal of the central controlling authority entirely by creating a system whereby:

— Several persons keep copies of the entire ledger;

— Writing or making changes to the ledger requires consensus from the persons who have copies;

— Each addition or change is recording in each copy of the ledger – thus each copy is equally authoritative (Peters & Panayi, 2016).

A distributed, decentralised network will only go down if every single node goes down, rendering it virtually always available.

Figure 4: Distributed Ledger Taxonomy

DISTRIBUTED LEDGER TAXONOMY

HOW MANY COPIES OF THE LEDGER?

ONE

TRADITIONAL LEDGER EG A PERSONAL BANK ACCOUNT

MANY

WHO CAN USE THESE COPIES?

OWNER GROUP

PERMISSIONED, PRIVATE SHARED LEDGER EG BACKCHAIN, A CLEARING AND SETTLEMENT NETWORK

ANYONE

WHO MAINTAINS INTEGRITY OF THE LEDGER?

TRUSTED LEDGER OWNERS OR ACTORS, BY VALIDATION

PERMISSIONED, PUBLIC SHARED LEDGER (IE A DISTRIBUTED LEDGER) EG RIPPLE, A GLOBAL FINANCIAL TRANSACTION SYSTEM

ANY USER, BY UNTRUSTED CONSENSUS

UNPERMISSIONED, PUBLIC SHARED LEDGER EG BITCOIN, A CRYPTOCURRENCY

Source: Adapted from Distributed Ledger Technology. Beyond Blockchain; A Report by the UK Government Chief Scientific Adviser

6.1.2 Hashing

A hash is a short code of defined length which serves as a **fingerprint for a digital document**. A program called a hash-generator allows a user to upload any string of text

and create a unique ID. Every time the same string of text is run through the hash-generator, it will give the same document-ID. The contribution of hashing as an anti-tampering device is significant: if a single letter in a document is changed, it will automatically generate a completely different ID.

Hashes are one-way. This means that the hash-generator can be used to generate a hash from the document, but it is mathematically impossible to generate a document from a hash.

Figure 5: Cryptographic Hash Function
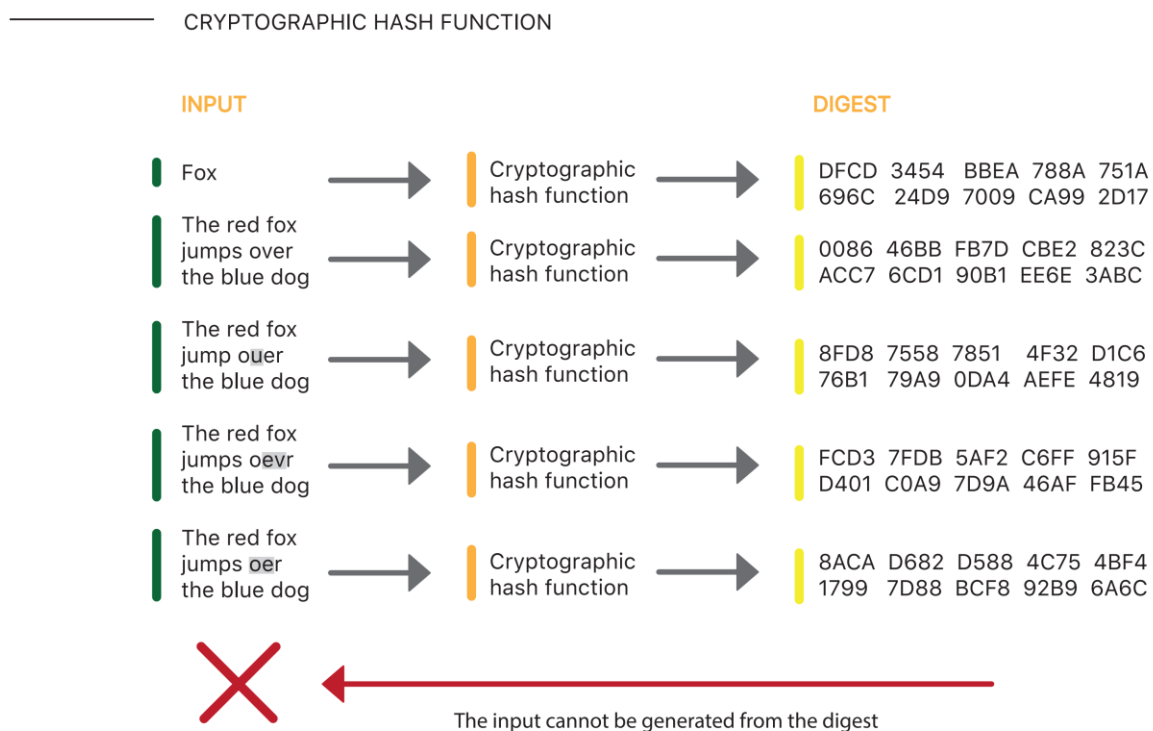
Source: Adapted from: https://commons.wikimedia.org/wiki/File:Hash_function.svg

In a blockchain, each block of transactions is secured by including a hash of the information block, as well as of the previous block, thus allowing all parties to guarantee that none of the transactions has been modified or tampered with.

6.1.3 Public and Private Keys

A **public key** is effectively a **publicly available ID-number** which can be used to identify a person.

A **private key** is effectively a **password**, which has been **mathematically linked to the public key**.

When using public/private key pairs, a user can authenticate that they are truly the 'owner' of a public key by entering their private key details into the software; this will, in turn, check if the two keys are truly mathematically linked.

This function cannot be practically run in reverse – that is, it is nearly impossible to generate the private key if one only has information about the public key

6.2 Architecture of a Blockchain

6.2.1 A Decentralised Digital Network for trading Assets

As a network oriented software implementation, a blockchain shifts the risk and responsibility of code execution and data storage from centralized machines to decentralised networks.

A blockchain is used to record the trading of digital assets. The most basic asset whose transactions are built into the functioning of most blockchain protocols is cryptocurrency in the form of tokens (such as Bitcoin, Ether, Litecoin, etc.). However, they can also be used to exchange other assets, such as land titles or ID documents (see section 4.3).

Every blockchain network has different rules regarding what kind of assets it trades, and under which conditions trading takes place. These rules are encoded into its software.

Each device running the blockchain software is known as a **node** and is connected to the network of nodes running that software. When anyone can set up a node and transact directly with any other node on the network, this is known as a **public blockchain network**.

However, if the device is connected to an intranet, that is, a private network which only specific devices have access to, then trades can occur between a select group of persons who have been given access to that network. This is known as a **private blockchain network**.

The architecture of blockchain software ensures that only identical copies of the blockchain software may interact with each other[22]. Therefore, if anyone changes a copy of the software, they effectively create an entirely new blockchain. This is known as a "fork." There have been multiple forks of blockchain software since the introduction of the Bitcoin protocol in 2009: August 2017 saw a fork of the Bitcoin blockchain into a new blockchain called Bitcoin Cash.

Protocol identity ensures that all devices on the network trade under exactly the same conditions without the need for a central authority to verify that the rules are observed.

---

[22] This is done by hashing the entire software code of the program. If even a single letter of code of two versions of the software is different, the hashes will not match, and the programs will refuse to communicate with each other.

HOW A BLOCKCHAIN WORKS

1 — A wants to send a digital asset to B

2 — The transaction is represented online as a "block"

4 — Those in the network approve the transaction is valid

3 — The block is broadcast to every party in the network

5 — The block then can be added to the chain, which provides an indelible and transparent record of transactions

6 — The digital asset moves from A to B
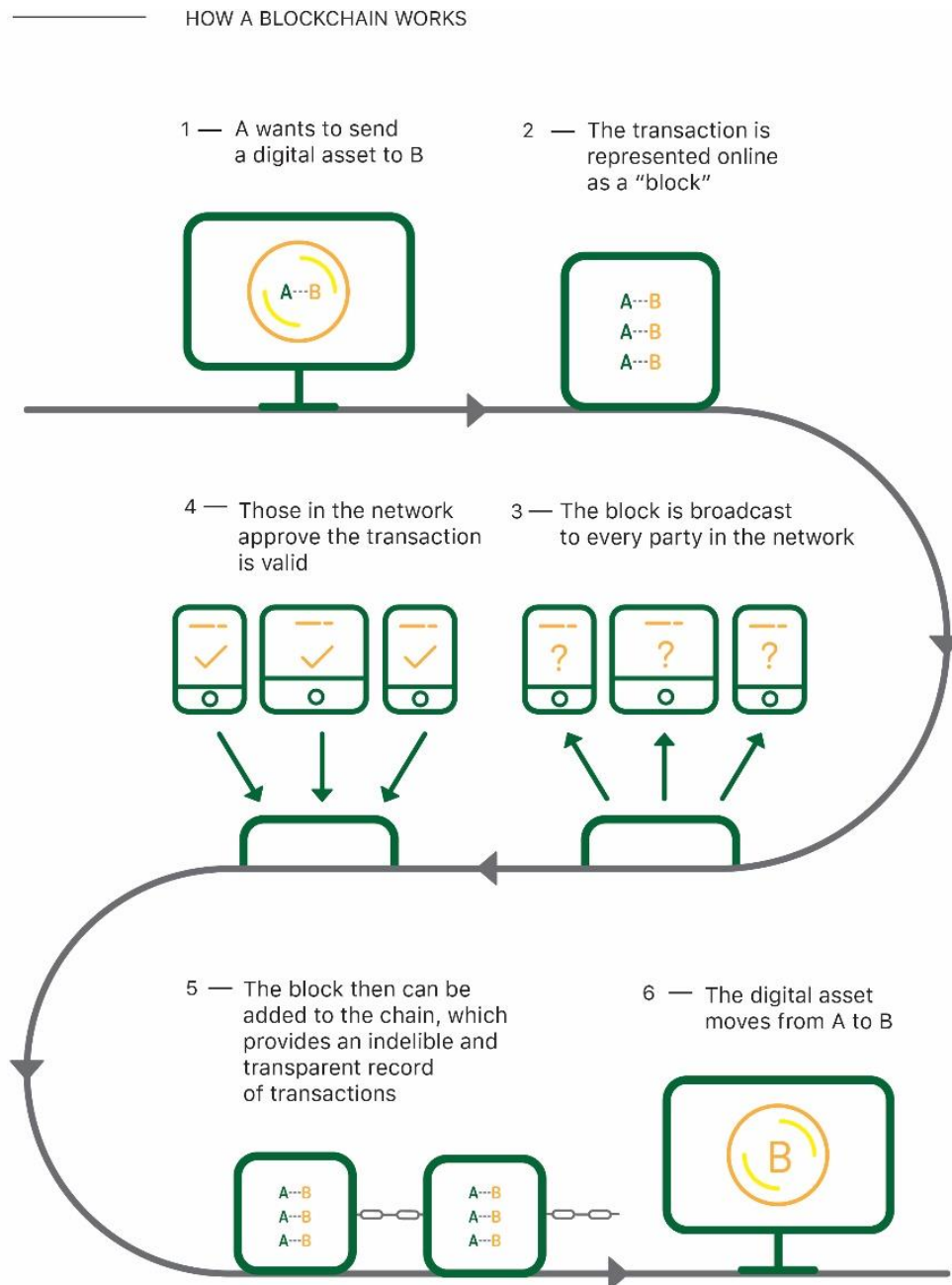
Adapted from Ryan (2017)

6.2.2 A Decentralised, Distributed Ledger

At its core, a blockchain is a transparent and autonomous decentralised ledger. Each copy of blockchain software:

— stores a complete copy of the ledger;

— writes new entries to its ledger when it receives consensus from the rest of the network;

— broadcasts transactions made by its user to the rest of the network, for verifying by consensus and recording;

— regularly checks that its copy of the ledger is identical to the ones across the rest of the network.

6.2.3 A System for anonymously verifying Identity and Ownership

Transactions are listed on a blockchain in the following manner:

Figure 7: Transactions on a blockchain

The blockchain software can issue a person with a bitcoin address which is linked to their unique public key, and its cryptographically linked private key.

To write a new transaction to a blockchain – that is, to transfer an asset associated with a bitcoin address – a user must enter the secret private key associated with that public key/bitcoin address which was issued to them when it was created.

Ownership of assets which have been transferred to a specific bitcoin address/public key are verified by knowing the private key.

Thus, both the parties involved in a transaction as well as the public can see that a transaction has taken place, and can identify who owns what, without knowing the identity of the parties in the transaction (Nakamoto, 2013).

Each of those parties in the transaction can then make use of their assets by simply entering their private key into the bitcoin software, without needing to prove or expose their identity to any third-party or intermediary.

Figure 8: Signing a Transaction on a blockchain
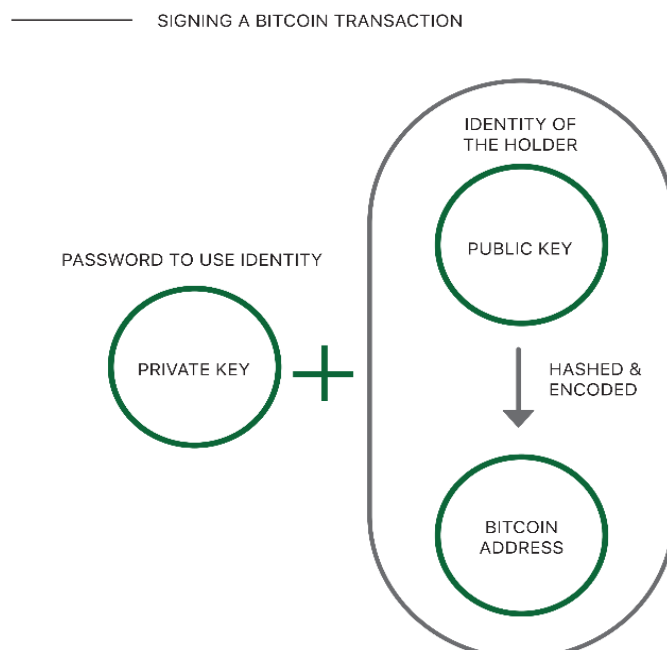
6.2.4 A System for ensuring Permanent Indestructible Records

> The ledger in the Bitcoin blockchain is 'append-only' – which means that transactions can only be added, and *cannot* be edited or deleted.

Thus, each new transaction is added to a block, while each block is chained to the previous block forming a **chain** (see figure 10).

Figure 9: Building a Blockchain
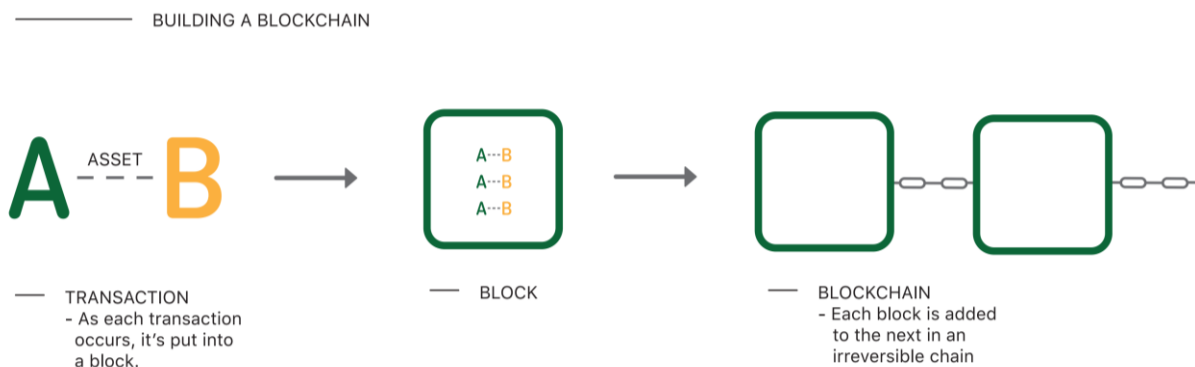
As shown in Figure 10, the *integrity of the chain* is assured using two sets of hashing:

— All transactions within a block are compressed and anchored to the block by using a special hash function called a **Merkle root**. That hash is included in the header of the block.

— The header of each block also includes the hash of all the information in the previous block.

Were someone to try to edit one of the transactions in the chain, it would immediately invalidate the hash of every subsequent block.

Thus, hacking the chain would require *not only changing the transaction, but also recalculating and changing the header information of every block created since that transaction, and doing so on over half the computers on the network* – a highly impractical proposition.

For larger blockchains it becomes effectively impossible to change any transactions because:

a) it would require impractically-large amounts of computer processing power to do so; and

b) as the number of blocks on the chain is ever-increasing, the amount of computing power required to make such a change is also always increasing.

This is an important consideration: advances in computing power will *not* suddenly compromise or make the security of the blockchain obsolete.

Figure 10: Simplified Structure of a Blockchain

Source: Adapted from https://www.slideshare.net/arcatomia/anatomy-of-a-blockchain/7

43
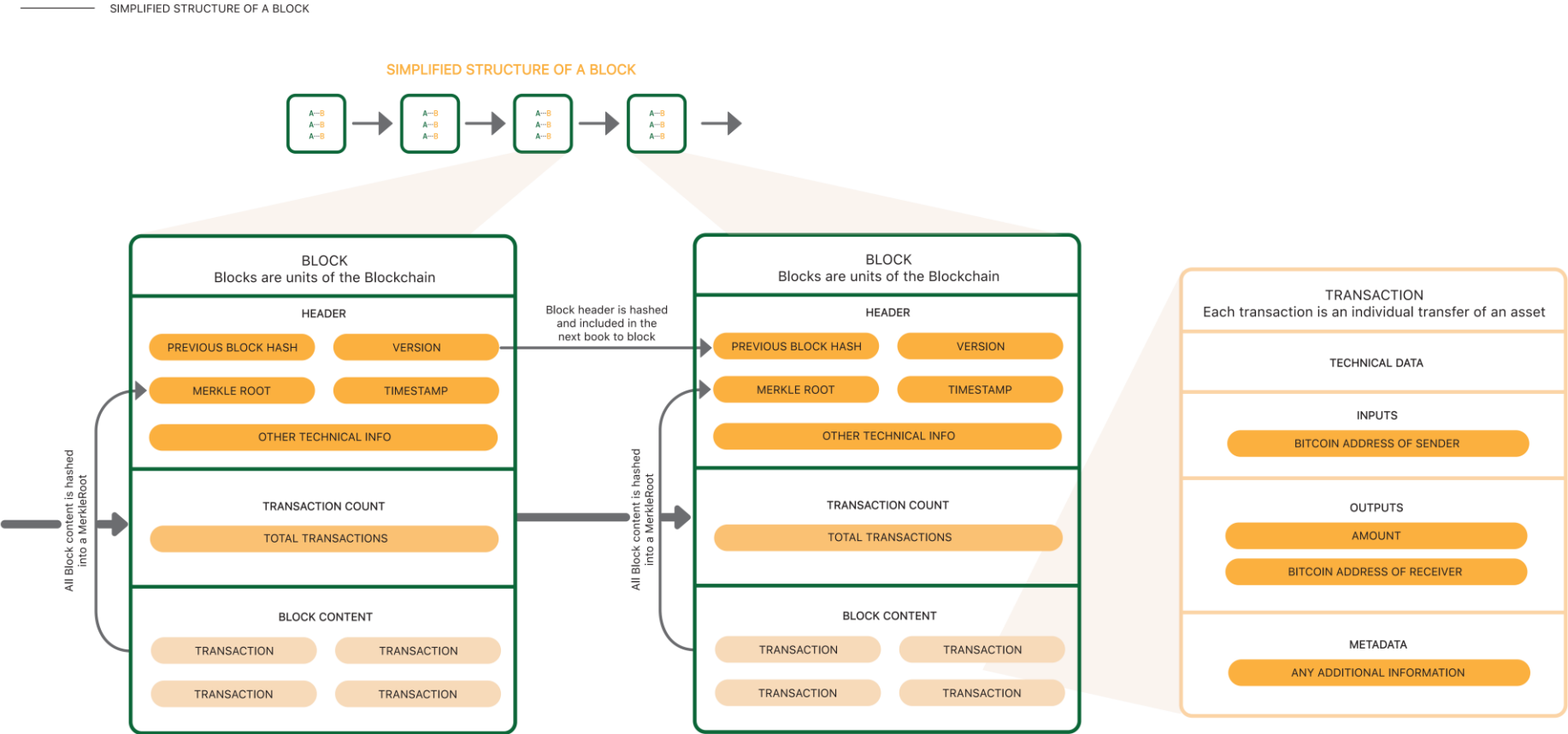
6.3 Issuing Certification using Digital Signatures

All solutions for digital certification use a system of digital signatures to issue certificates.

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.

Figure 11**:** Anatomy of a Digitally Signed Document

Adapted from: https://www.docusign.com/how-it-works/electronic-signature/digital-signature/digital-signature-faq
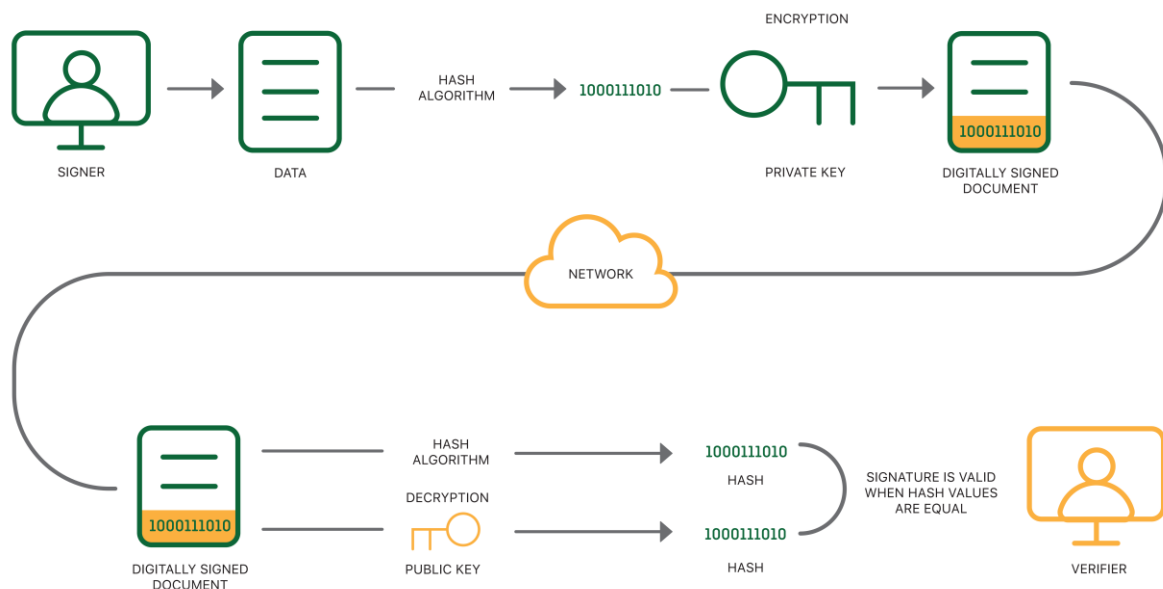
A digital signature provides a way to issue certificates by allowing a person to:

— 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).

6.3.1 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 (See section 5.2.1);

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

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.

6.3.3 How 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*.

6.3.4 Systems for Digital Signatures

6.3.4.1 Public Key Infrastructures

In public key infrastructures, trusted bodies known as certification authorities, centrally manage the system by:

— issuing the linked private and public keys;

— running a server to timestamp each signature;

— running the verification software.

Usually, the certification-authority embeds the public key in a certificate that contains a set of additional meta-data to facilitate usage. This offers several advantages:

— certification authorities can verify the identity of persons to whom keys are issued, thus linking public-keys to real-world identities;

— everyone can have confidence of the date of signature, since the 'clock' is maintained only by the certification authority.

However, public-key infrastructures also create a central-point of control and failure. Most critically, should the certification authority hosting the verification software close down (say, due to bankruptcy, civil unrest, restructuring etc.), it would effectively

invalidate any document signed through it. This provides a significant problem for certificates such as birth, marriage or educational achievement which should last a lifetime. Furthermore, the certification authority may abuse the trust placed in them, in any of the ways already discussed under section 4.1.

If a private key is leaked, there is nothing to prevent an attacker from issuing fake records and backdating content. Even if an issuer publicly revokes those records, an independent verifier would not know the difference between a valid and invalid record unless there were some additional authority attesting to when the transaction took place[23].

6.3.5 Digital Certificates using Blockchain Technology

6.3.5.1 The Value-Added of Blockchain-Secured Digital Certificates

Blockchain technology is ideal as a new infrastructure to secure, share, and verify learning achievements (Smolenski, 2016). **In blockchain, PKI replaces the central authority with a more robust decentralised network.** This decentralised structure enhances the longevity of the network because duplicates of the blocks, on which the signatures are stored, are so numerous. The decentralisation of the blockchain gives it a further advantage in that no third-party can alter or erase the transactions stored in the blocks without undoing the proof-of-work requirement that had verified them.

Beyond removing the dependence upon any certificate authority or trusted third-party, blockchains provide **independent time stamping**, which creates significant security benefits. A reliable timestamp is clearly important in cases where credentials expire, but it is also critical for a practical reason — the issuer must be able to rotate issuing keys on a regular basis, both as part of security best practices, but more critically in response to a key leak. To determine that a record was issued by a specific issuer when the issuing key was valid requires knowledge of an independent timestamp.

Unlike many PKI systems, signatures on a blockchain are also file-format independent: the same software can be used to sign any kind of file, irrespective of the (proprietary) standards with which it was created (Thompson, 2017).

6.3.5.2 Architecture of Blockchain-Secured Digital Certificates

In the case of certifications, a blockchain keeps 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.

---

[23] See: https://github.com/blockchain-certificates/cert-schema/wiki/Why-the-blockchain

Figure 12**:** Digitally Signed Documents on a Blockchain

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

Schmidt (2015, 2017) describes issuing a certificate in such a manner using Blockcerts (see section 7.1.1) as a relatively simple process:

> 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.

Figure 13: Issuing a Blockchain-Secured Certificate
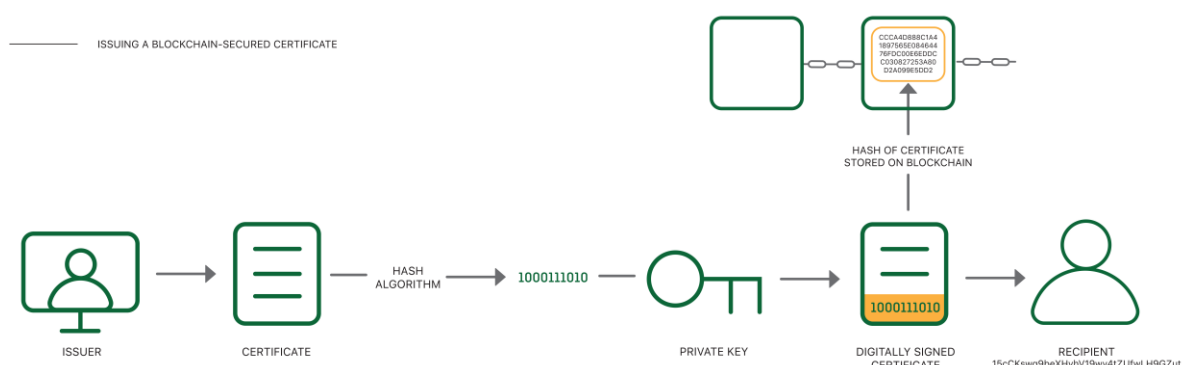
The digital credentials themselves can be stored by a user on a hard drive or in a mobile wallet, from where they can easily be shared with others, or even printed out on paper. It is therefore possible for a user to verify who a certificate was issued to, by whom, and validate the content of the certificate itself.

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.

6.3.6 Self-Sovereign Identities using Blockchain Technology

6.3.6.1 Creating a Self-Sovereign Identity on the blockchain

> *The recording of a transaction of money is similar to the award of a certificate in that it has value. The certificate notarised on a blockchain is time-stamped, in a chain, and makes it easy for the identity of issuers and recipients to be verified (Jagers at ASU GSV Summit, 2017).*
>
> *The ownership and control of a diploma reside in the same place - which means that they are shared equitably between the institution and the student. That is already a game-changer*
>
> *(Gray, 2017 at ASU GSV Summit).*

New models for identification are emerging, although their implications are not necessarily clear at this time. The model of a singular state-issued credential evolved into an augmented and networked approach that uses the state issued credential as a start. Now the current evolution is towards knowledge-based aggregations of attributes of identity, often much more under the user's control. This includes things like reputation scores from social media, peer-to-peer sharing, and gig economy platforms.[24]

As with digital signatures, in a blockchain-based self-sovereign identity system, a person is identified by their public key. They prove they are the owner of their public key by entering their secret private key. In most self-sovereign identity systems, this private key is linked to a piece of biometric identifiable information such as a fingerprint.

To create the self-sovereign identity, the person simply needs to record their personally identifiable information and associate it with their public key. This is done using custom software, typically residing on their smartphone, which they can log into using their private key / biometric data. The software encrypts their private data on the device, and uploads a hash of that information to a blockchain.

---

[24] Hanson et al. (2017)
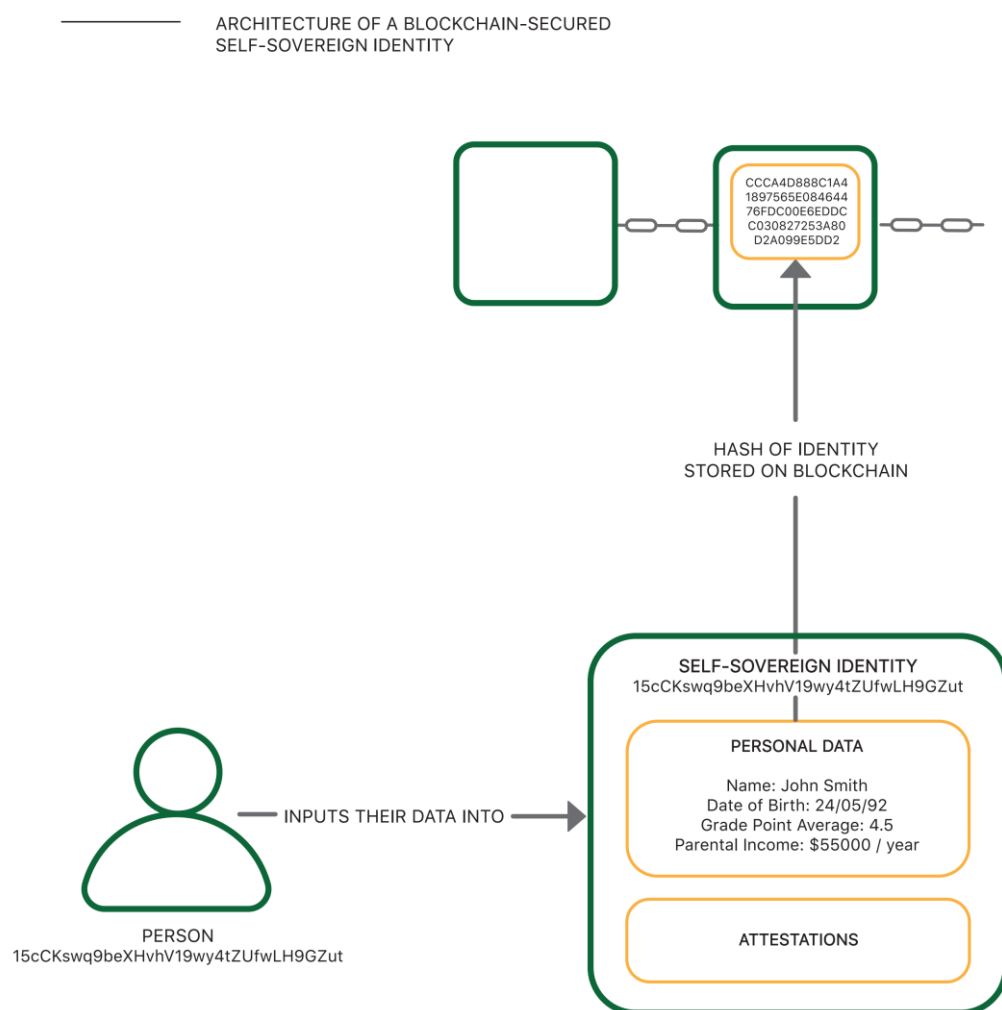
Source: Camilleri, Anthony; Grech, Alex (2017): Architecture of a Self-Sovereign Identity. See: https://doi.org/10.6084/m9.figshare.5371510.v1

6.3.6.2 Certifying ta Self-Sovereign Identity

Should a third-party need to certify that a person's data is true, they would require:

- the person to share the data in question,
- evidence that that data is true.

Having checked the data, the third-party could then issue a certificate certifying the information as true with a statement such as "I have certified that the information with this hash is true". If this statement is uploaded to a blockchain, it provides a public attestation that the person's identity details are true, without needing to reveal any information about the person whatsoever, aside from their public key.

Thus, to continue our example, if our university applicant wished to obtain a scholarship, the admissions office would likely ask for proof of their identity in the form of a passport or birth certificate, proof of their grades, and of their financial situation. If, having checked this information the admissions office finds it suitable, they might issue a certificate saying that the person qualifies for a scholarship. The hash of this certificate can in turn be stored on the blockchain, while the certificate itself can be stored in the person's   self-sovereign   identity.

ARCHITECTURE OF A BLOCKCHAIN-SECURED
SELF-SOVEREIGN IDENTITY

CCCA4D888C1A4
1897565E084644
76FDC00E6EDDC
C030827253A80
D2A099E5DD2

BEC9F9CA626E0E1
511F46C4EDDF3D4
04586034B99AC28
116160C36F2F4009
DEE

HASH OF IDENTITY
STORED ON BLOCKCHAIN

HASH OF CERTIFICATE
STORED ON BLOCKCHAIN

SELF-SOVEREIGN IDENTITY
15cCKswq9beXHvhV19wy4tZUfwLH9GZut

PERSONAL DATA

Name: John Smith
Date of birth: 24/05/92
Grade Point Average: 4.5
Parental Income: $55000 / year

ATTESTATIONS
Verifying institution attests that person
qualifies for scholarship

PERSON
15cCKswq9beXHvhV19wy4tZUfwLH9GZut

INPUTS THEIR DATA INTO

SENT TO AND CHECKED BY

VERIFYING
INSTITUTION

ISSUES

CERTIFICATE

The verifying institution attest
that data presented by
15cCKswq9beXHvhV19wy4tZ
UfwLH9GZut is true, and
qualifies them for a
scolarship.

CERTIFICATE BECOMES PART OF THE SELF SOVEREIGN IDENTITY

Source: Camilleri, Anthony; Grech, Alex (2017): Architecture of a Verified Blockchain-Secured Self-Sovereign Identity. See: https://doi.org/10.6084/m9.figshare.5371516.v1

50

7   Implementations of Blockchain Technology in Education

Blockchain is a technology that clearly has applications in the world of learning at the individual, institutional, group, national and international levels. It is relevant in all sorts of contexts: schools, colleges, universities, MOOCs, CPD, corporates, apprenticeships, and knowledge bases. Rather than the old hierarchical structures, the technology becomes the focus, with trust migrating towards the technology, not the institutions. It really is a disintermediation technology.

Donald Clark

Digital documents can be just as ephemeral as paper; often issued in proprietary formats by vendors to customers, institutions without the correct software may not be able to read or verify them. Even with access to the correct software, in many instances, the verification process can be tedious and uncertain. The same goes for digital signatures: even in places where legislation has mandated their acceptance, digital signatures come in a wide variety of formats with varying levels of security, not all of which are accepted as legal proof.

Another challenge with digital documents is that one of the primary ways people share information digitally - email - is usually not secure, so proprietary transmission infrastructures need to be built to send sensitive documents, such as health records. This greatly improves on the security of postal mail, but raises interoperability headaches.

Finally, like paper documents, digital documents can also be spoofed by sophisticated users in ways that are difficult to detect.

7.1 Issuing Certificates

When blockchain technology is used in the issue of certificates, there is an opportunity to not just verify credentials without an intermediary, but to enrich and add value to the already existent digital certification ecosystem: BADGR and Mozilla Open Badge are already being used to provide digital certifications to students in some prestigious academic institutions. The objective of notarising certificates on a blockchain is therefore to transform a digital certificate that a student usually receives privately into an automatically verifiable piece of information that can be consulted by third parties through an immutable proof system, on a public Blockchain.

In current practice, access to a public platform almost inevitably requires a student to share or divulge 'sensible' metadata, which tends to include private information. By using a blockchain as 'proof of knowledge' (Aglietti 2017a) such private information does not necessarily have to be divulged during a public consultation of metadata related to certifications. In the short term, it is likely that students will be able to approach academic institutes and employers while maintaining a discreet level of confidentiality: in principle, only the information that the students would mark as public during the proof generation process would be accessible to third parties.

Aglietti (2017b) sees opportunities for software organisations that can facilitate and simplify the process of accessing the Blockchain for students and badge issuers (institutes, companies, schools etc.). Ideally applications would be built over an open-source architecture that can guarantee data continuity of lifelong & life-wide learning achievements and no lock-in with one particular solution. Academic institutes and companies will not be the only ones to take advantage of the accountability and consistency of the information available on the platform and the Blockchain. Students could in turn use the public metadata to seek similar profiles and, in doing so, foster the creation of new models of social inclusion and entrepreneurship: all of this without requiring a centralized authority to vouch for the validity of the information.

7.1.1 Blockcerts: An open Standard for Blockchain educational certificates

The cornerstone of the Blockcerts open standard is the belief that people should be able to possess and prove ownership of their important digital records. These records form the basis for proving aspects of oneself, consistent with the principles of self-sovereign identity (see Allen 2016, Jagers 2017b, Lewis 2017). Within this context, the Blockchain is considered to be a technology that allows individuals to own their official records and share them with any third-party for instant verification, all the while precluding any attempt to tamper with or edit the records.

The MIT Media Lab and Learning Machine, an enterprise software vendor, have developed the Blockcerts open standard for issuing and verifying credentials on the Bitcoin blockchain (MIT Media Lab 2015; Schmidt 2016). Blockcerts is currently the *only* open standard for issuing and verifying records on the blockchain, and it is the goal of the Blockcerts community to promote its adoption as the main global standard (in terms of social adoption) for issuing records on the blockchain.

The standard allows any user, including education institutions and governments to use the base code and develop their own software for issuing and verification. Blockcerts is free and available for anyone to use without credit or royalties to its core developers; from a scan of the Blockcerts Community forum, it is clear that a number of organisations, start-ups and individuals around the world are using it to develop applications. Blockcerts is also free for recipients with the Blockcerts mobile app and wallet available for free download for both iOS and Android; its code is also completely open -source.

The purpose of making Blockcerts open source was to avoid a standards war and vendor lock-in, perceived by the developers to be two major impediments to the easy interoperability and wide adoption that are prerequisites for true recipient ownership of official records. Data trapped in silos is the status quo and is perceived by the Blockcerts community as a significant challenge which the Blockchain gives us the opportunity to move beyond.

Jagers (2017) claims that Blockcerts sets the precedent for a mobile wallet that meets the most important umbrella criteria of **digital self-sovereignty**: recipient ownership and vendor independence. Within this context:

— **recipient ownership** means that individuals control the private keys that allow them to demonstrate ownership of money or their digital records.

— **vendor independence** means that access, display, and verification do not rely on any particular vendor. When based on open-source standards, records can therefore be migrated, shared, and verified independent of any vendor.

The combination of these two conditions is cited as the only way to guarantee that individuals independently own their personal data.

Figure 15 below is a high-level view of this process:

Figure 15: Simple process diagram for issuing and verifying a certificate on the Blockchain
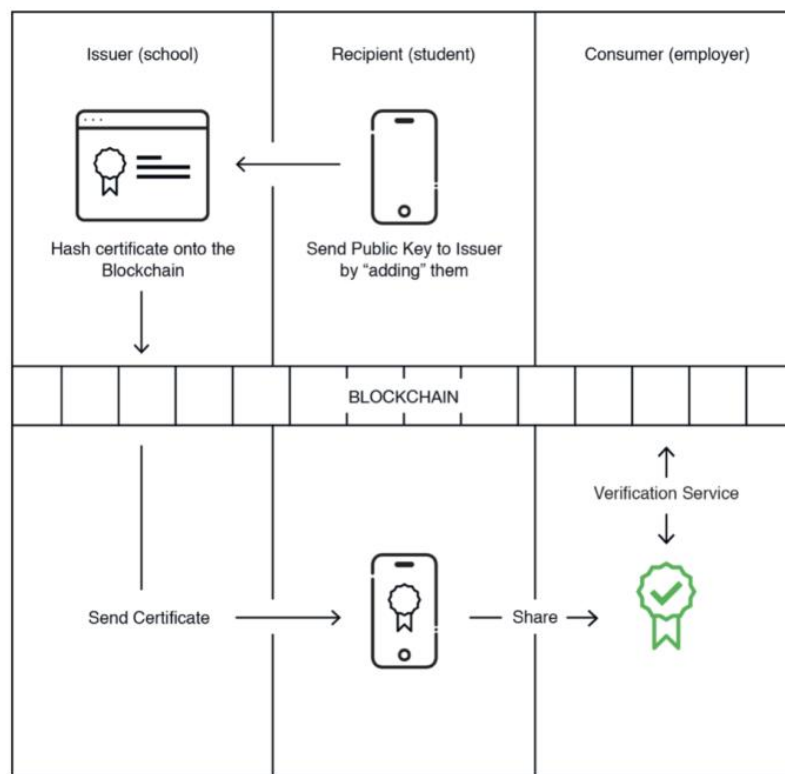
Source: Blockcerts (2016)

Blockcerts has been built to provide a common set of patterns so that credentials can be issued and verified across any blockchain, and across different market domains. According to key developers involved in the project[25], when research started in 2015, the Bitcoin blockchain was the logical choice for the underlying blockchain to which to anchor lifelong digital records. In 2016, there was some discussion about expanding resources to Ethereum, but Ethereum's hard fork at the time made it seem unreliable for credentials that need to last a lifetime. The decision made at the time was to make documentation for Bitcoin as useful as possible, while keeping it open to cover other Blockchains in the future. In 2017, Ethereum has gained significant momentum with developers, and many are asking for Blockcerts to expand documentation (and reference implementations) to include Ethereum. Since Blockcerts is an open-source community, several developers are currently contributing to make this expansion happen[26].

The Blockcerts community is aligned with (and contributing to) the following standardisation communities: IMS Open Badges[27]; W3C Verifiable Claims[28]; W3C Linked Data Signatures[29] and W3C / Rebooting Web of Trust Decentralised Identifiers[30].

---

[25]   See discussions on the community site, including http://community.blockcerts.org/t/why-the-bitcoin-blockchain/153

[26]   Blockcerts was designed to write and verify to any blockchain, so a chain split wouldn't affect this set of libraries. According to the Blockcerts community, while the foundation for this work is complete, more chains necessitate small extensions and more specific documentation for each, as is already planned for Ethereum.

[27]   See http://www.imsglobal.org/tags/open-badges

[28]   See https://w3c.github.io/vc-data-mode l

[29]   See https://w3c-dvcg.github.io/ld-signatures

MIT, the University of Nicosia and researchers at the University of Birmingham[31] are developing their own systems using the Blockcerts open specification.

Figure 16: Example of a Learning Machine Analytics Dashboard
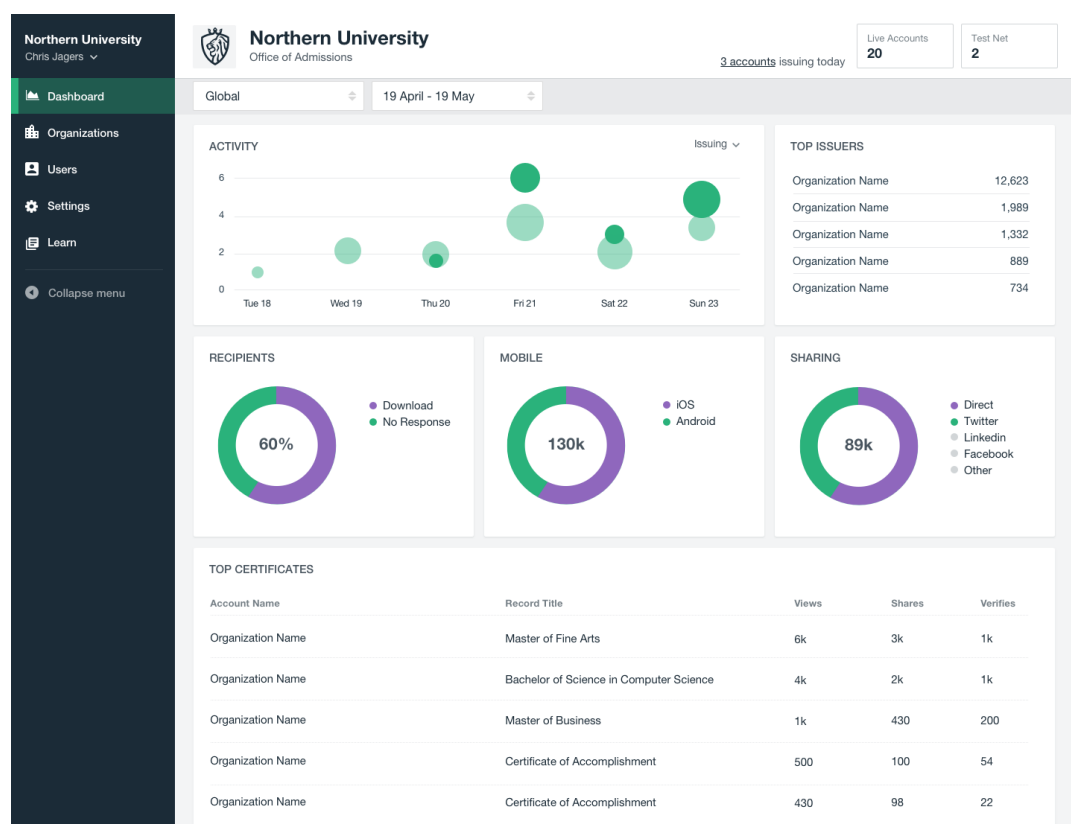
Source: Learning Machine

7.2 Snapshot of Vendors in the Certificate and Identity Workspace

The vendor offering for Blockchain-related products in the certificate workspace is increasing exponentially. At the time of writing, there are over 20 companies building customers' platforms on the blockchain (Mesropyan 2017). They generally have a similar set of features.

Jagers (2017) has proposed a model which helps differentiate these offerings on the basis of four distinct criteria. These are reproduced here as a point of departure in differentiating between the offerings of a sample of vendors:

---

(30) See https://github.com/WebOfTrustInfo/rebooting-the-web-of-trust-fall2016/blob/master/draft-documents/DID-Spec-Implementers-Draft-01.pdf

(31) See Li (2017) and Blockcerts.ehcoo.com

Proof of Existence solutions use the blockchain as a time-stamping notary to guarantee that a particular document hasn't changed since a particular point in time. These vendors typically use standard open-source approaches so that the blockchain is used for verification, without any ongoing vendor dependence. However, vendors in this quadrant aren't encoding recipient's public keys into documents, nor transmitting them to recipients—they are simply providing data verification. This means that document recipients cannot prove the unaltered document was issued to them. None of these vendors should be confused with identity claims for individuals.

Vendor as Notary solutions also provide proof of existence for data and position themselves as products to issue identity documents, like academic credentials. However, they do so in a format that is always dependent upon the vendor for access, hosting, and verification—they do not provide any sort of ownership for individual recipients. In effect, they are using the blockchain to support their vendor-centric approach to verification and stewardship of records.

Know Your Customer solutions typically do provide a mobile app that allows recipients demonstrate ownership of their verified data. While this creates efficiencies within a robust network of participating companies who want more efficient ways to validate customer data, this data is only useful to recipients within the perimeter of a vendor-controlled network. So, while recipient ownership is established, reliance on the vendor is absolute. KYC solutions are promising for many use cases, but shouldn't be confused with solutions that provide verifiable claims that are useful everywhere.

Digital Self-Sovereignty solutions enable individuals to receive official records that are fully owned by the recipients, with no ongoing dependency upon a vendor for viewing, sharing, or verifying these records. This independence is achieved by three things working in combination:

- issuing records in a format based on open standards

- issuing records that include the public key of recipients

- holding records with an open-source container (i.e. a mobile app) that gives recipients control of their own private keys and continues to operate and survive beyond any particular vendor.

Figure 17: Current Positioning of Vendor Independence vs Recipient Ownership

Source: Adapted from Jagers (2017)

7.2.1 Certification Solution Vendors

The following organisations are currently representative of a set of vendors[32] whose emerging suite of certification products and services may be applicable to the education sector.

---

[32] Certification Vendors are starting to emerge on a regular basis. Recent entrants include GrowBit (www.growingabit.io) and INTEGRAL+, the later being a new initiative coordinated by Kiron Open Higher Education and funded by the German Federal Ministry of Education and Research (BMBF), Kiron and Lübeck University of Applied Sciences. INTEGRAL+ is studying opportunities to provide more automated, verified and scalable issuer-hosted digital certificates to students in the digital learning environments of Kiron and FH Lübeck. The project levers on existing initiatives, including the UNIC Blockchain initiative and the Blockcerts standard from the Open Initiative for Blockchain Certificates. The planned pilots will test several implementation possibilities for German universities and Kiron Open Higher Education looking at two major scenarios: achievements/learning outcomes reached with only one online course or MOOC and achievements/learning outcomes reached as a combination of several digital learning opportunities. The partners are also exploring opportunities to merge blockchains with open badges in this context.

7.2.1.1 Learning Machine Certificates deployed over Blockcerts

Blockcerts can be used by vendors to build commercial solutions which are configured for specific target market requirements. Learning Machine has developed a set of tools for organisations to issue, track, and verify Blockchain-based records – essentially a commercial ecosystem composed of a Registrar CRM and a set of APIs over the open source Blockcerts platform. In terms of the business model, the issuing institution is Learning Machine's paying client; the recipients secure access the service for free, including the mobile app and wallet, and verifiers secure access to instant and free verification of records through web browsers and the mobile app.

The tamper-proof format allows recipients to prove ownership and allows third parties to instantly verify, without any dependence upon a centralised authority. The target customers for issuing digital records include governments, companies, education providers, accreditation bodies, and others. The technology is being marketed as a solution that does not require the client to have any inhouse blockchain technology skills and capability, regardless of the content type. Notarising official records on the Blockchain is particularly appropriate when organisations provide recipients with records that third parties may later want to verify – education institutions are clearly a primary target market[33].

Learning Machine claims that the Blockcerts standards-based solution is tamper-proof in that the records are digital files that have been cryptographically signed by an issuer and registered on the Blockchain. Each record contains a recipient's public key and thus can demonstrate ownership of the record without any dependence upon a certificate authority. With Blockcerts, a:

— presentation layer can be styled to mimic the look of traditional records;

— content layer is code that contains all of the data and images;

— receipt layer contains proof of the transaction, which includes a signed hash of the content.

---

[33] The University of Melbourne became the first university in the Asia-Pacific region to issue recipient-based credentials on the Blockchain, using the Learning Machine issuing system. See: https://www.newswire.com/news/university-of-melbourne-first-in-asia-pacific-to-issue-recipient-owned-19980513

Figure 18: Multiple layers in production of a certificate notarised on the Blockchain
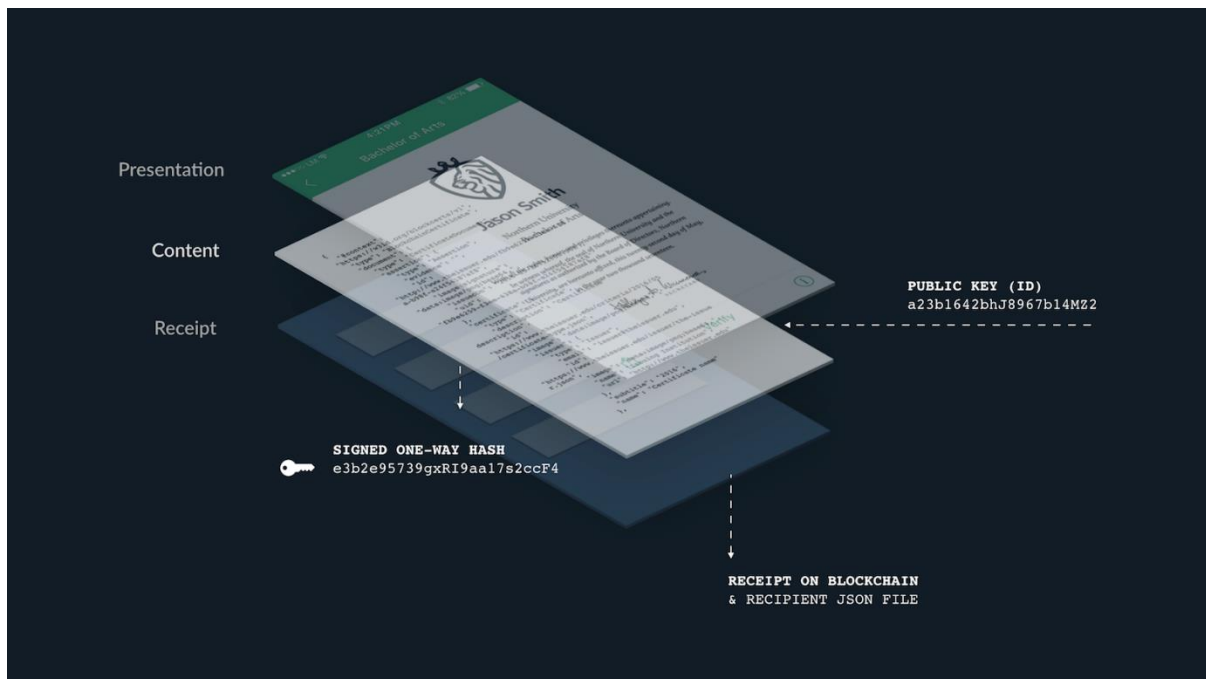
Workspaces are used by organisations to complete the entire process of designing certificates, connecting with recipients, and issuing these official records. These workspaces allow users to:

— import/manage recipient lists;

— easily collect recipient public keys;

— design templates for digital records (content, layout, metadata);

— issue records to entire cohorts;

— track aggregate analytics of how records are being used online;

— view profiles that show all records issued to an individual.

Figure 19: Example of the Certificate Editor in an Issuing Works Spaces
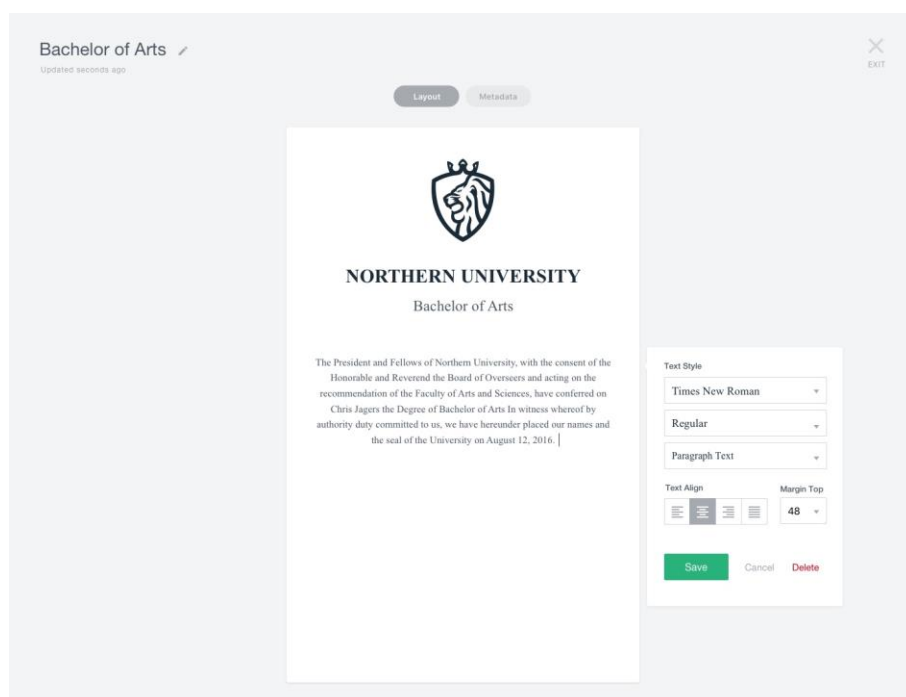
Source: Learning Machine

7.2.1.2 Sony Global Education

Since 2016, **Sony** has been making announcements that it has developed in-house certificate-issuing system that uses blockchain technologies (Sony 2016, Russell 2017). On 10 August 2017, Sony Corporation and Sony Global Education (SGE) announced[34] the development of a system that will specifically applies blockchain technology to the education sector. The press release states that by using "technology that makes mutual use of educational achievements and activity records in an open and safe way," this reliable system centralizes the management of data from multiple educational institutions and makes it possible to record and reference educational data and digital transcripts". The system is built on IBM Blockchain, which is delivered via the IBM Cloud and powered by Hyperledger Fabric 1.0, a blockchain framework and one of the Hyperledger projects hosted by The Linux Foundation. It brings together 1) a function that authenticates and controls usage rights to educational data, and 2) an application programming interface for handling these rights aimed at educational institutions. In 2018, Sony will start to deploy its own service offerings, starting with its Global Math Challenge which brings together 150,000 participants from around the world.

7.2.1.3 Attores Solutions

Attores has launched a product called **Open Certificates**[35], which will be able to issue educational certificates on the Ethereum blockchain as smart contracts. The product is currently being tested; there have been announcements about partnerships with educational organisations in Singapore.

---

[34]   https://www.sonyged.com/2017/08/10/news/press-blockchain/

[35]   https://www.opencertificates.co

7.2.1.4 Additional companies

The number of companies offering certificates on the blockchain is likely to increase in the near future. **Gradbase[36]** and **Stampery**[37] are developing proprietary solutions that aspire to become new global standards for issuing and instantly verifying qualifications.

7.2.2 Identity Solution Vendors

The following organisations are currently representative of a set of vendors whose emerging suite of identity solution products and services may be applicable to the education sector.

7.2.2.1 Civic

Civic[38] describes itself as a secure identity platform stored on the blockchain. The company has just raised $33 million in funding to develop and launch its products. Using the Civic solution, a user uploads pieces of personally identifiable information to an app on their phone, the hash of which is stored on the blockchain. When any organisation (such as a university admissions office) needs the users' personal information, the user can choose which pieces of information to share. The Civic Platform also supports attestation, whereby an organisation can issue a certificate to the user (also linked to a blockchain) attesting that they have verified the data provided. Using the hash of their personally identifiable data together with the attestation, and a biometric identifier on their phone, a user can then identify themselves to other parties who need the information and trust the assessor. Within our example of the university, this would mean that they would be able to identify themselves to the library, to the canteen, to individual lecturers and to student associations, without the need for these bodies to store or even view the user's personal identifiable information. Furthermore, since the data is stored and encrypted only on the user's personal device, and not in a central database, it makes large scale data thefts of thousands of users' data impossible.

7.2.2.2 Uport

Uport[39] is a secure, easy-to-use system for self-sovereign identity developed by ConsenSys and built on Ethereum. The uPort technology consists of three main components: smart contracts, developer libraries, and a mobile app / web-based wallet. The mobile app holds the user's keys. Ethereum smart contracts form the core of the identity and contain logic that lets the user recover their identity if their mobile device is lost. Finally, the developer libraries are how third-party app developers would integrate support for uPort into their apps. uPort identities can take many forms: individuals, devices, entities, or institutions. Uport identities are self-sovereign, meaning they are fully owned and controlled by the creator, and don't rely on centralized third-parties for creation or validation. A core function of a uPort identity is that it can digitally sign and verify a claim, action, or transaction - which covers a wide range of use cases. An identity can be cryptographically linked to off-chain data stores. Each identity is capable of storing the hash of an attributed data blob, whether on IPFS, Azure, AWS, Dropbox, etc., which is where all data associated with that identity is securely stored. Identities are capable of updating this file themselves, such as adding a profile photo or a friend, or they can also grant others temporary permission to read or write specific files. Since they can interact with blockchains, uPort identities can also control digital bearer assets such as cryptocurrencies or other tokenized assets.

---

[36]   See https://gradba.se/en/

[37]   See https://stampery.com

[38]   See: https://www.civic.com

[39]   See https://www.uport.me and Lundkvist et al. (2017)

7.3 Storing a Verified e-Portfolio

The following organisation are currently representative of a set of vendors whose emerging suite of e-portfolio products and services may be applicable to the education sector.

7.3.1 Indorse

Indorse[40] is using blockchain-technology to launch a verified e-portfolio. Using the system, anyone will be able to upload any **claim** together with a link of how to verify that claim. Other users of the platform will then be asked to verify that claim - thus creating a trusted digital portfolio.

The system architecture from the user perspective is best illustrated through an example:

— Alice joins the Indorse network. Upon registration, she is issued a minimum Indorse Score (an SCR token) that will enable her to post a single claim to her profile.

— She starts by creating her unique profile identity, and then adds a claim. She claims that she graduated from the University of Malta. She provides a link to the university's verification page for her certificate information. She submits the claim and her Indorse Score is locked. The Indorse platform randomly chooses a number of other members who can indorse the claim, and the claim enters the gestation period.

— Bob is an Indorse member who is chosen to indorse the claim. He receives a notification and sees that Alice has placed a link to the verification page for her certificate. He verifies that the claim is valid and indorses the claim, locking up his Indorse Score.

— The gestation period ends with a consensus of indorsements. Alice's Indorse Score is increased by 1, for making a valid claim – if her claim is unable to verified, her Indorse Score will decrease by 1, and the claim will remain unverified. She is also rewarded with Indorse Rewards. Bob also has his Indorse Score increased by 1 and receives an Indorse Reward.

— Both user's Indorse Rewards are given a cash value based on the advertising taken in by the platform during that period

7.4 Managing Intellectual Property

The following organisations are currently representative of a set of vendors whose emerging suite of products and services focused on managing intellectual property on the Blockchain may be applicable to the education sector.

7.4.1 Binded

Binded (formerly known as BlockAI)[41] is a copyright registration service for images on the blockchain. When an image is created, its author can upload the image to the service, and a hash of that image, together with the timestamp of when it was uploaded and the identity of the author is registered on a blockchain. This creates an indelible, immutable proof of time of first publication, which later can be used to enforce copyright claims on the image.

In the future, Binded will also monitor the web for copyright infringements, and register the copyright of images secured through the service with copyright offices.

---

(40) https://www.indorse.io

(41) https://binded.com

7.4.2 Ledger Journal

Ledger[42] is a peer-reviewed scholarly journal that publishes full-length original research articles on the subjects of cryptocurrency and blockchain technology, as well as any relevant intersections with mathematics, computer science, engineering, law, and economics. It is published online by the University Library System, University of Pittsburgh.

Aside from publishing research about the blockchain, the journal asks users to digitally sign their documents using their bitcoin private keys, and also timestamps published manuscripts in the blockchain. Additionally, the journal has created open source plugins for Open Journal Systems[43], which allow anyone running the software to also sign and timestamp journal articles on the blockchain.

7.4.3 Bernstein Technologies

Similar to the two cases already described, **Bernstein Technologies** registers the hash of documents on the blockchain, thus providing proof of existence, integrity and ownership. However, Bernstein specialises in making intellectual property claims, which can then be used to secure copyright or patents. As such, it provides a platform by which patent claims can be uploaded to their platform, notarised and time-stamped on the blockchain. Traditional copyright and patent practices provide protection for an invention, but also require the disclosure of such invention. By storing the hash of the document on the blockchain, the invention can be verifiably published, without needing to reveal its contents.

Outside of copyright and patents, the system can also be used to secure trade secrets, lab notes and other internal intellectual property.

Figure 20: Managing Intellectual Property in the Blockchain with Bernstein

Source: Bernstein (2017)

---

(42)   http://ledgerjournal.org

(43)   Open Journal systems (https://pkp.sfu.ca/ojs) is the leading open source package for managing and publishing academic journals. Over 3 million academic articles have been published globally using the software (Source: https://pkp.sfu.ca/ojs/ojs-usage).

Simply time-stamping records on the blockchain or creating a vendor-owned environment in which recipients can store their records does not necessarily empower individuals: they must be able to take their records with them anywhere, store them *independently* from any vendor or issuing institution, and prove that they own them.

The argument for the merits of digital self-sovereignty in particular underpin the rationale for the development of the Blockcerts standard – or some other as yet unidentified standard - as an *open* standard.

At the time of writing this report, it is too early to determine the value that education institutions, governments or even learners (the target users) will attribute to the basic tenets of 'openness', 'vendor independence' and 'learner empowerment' - particularly those related to the value learners will attribute to owning their own digital certificates as opposed to being perpetually locked in with (albeit trusted) institutions or vendors. Although in principle these are powerful arguments, it is too early to determine whether these arguments are more compelling for target users than, say, proprietary solutions being developed by global brands such as Microsoft, IBM and Sony or some as yet undisclosed hybrid solutions.

8 Use Case Studies for Blockchain Technology in Education

Self-sovereignty means that once the certificate is notarised on a blockchain, and the user's credentials are notarised on a blockchain, and the user has a private key, they automatically become custodians of their own identities and credentials. The user can now take the document that was issued by a third-party and turn it into something else beyond the albeit limited tools for accreditation and moves it into the broader values of identity. Consider what Uport and others are doing in building data stores that can reside on the cloud but can also be used as proof to leading identifiers, including future employers and accreditation bodies, that these credentials are first and foremost controlled by the individuals themselves. The signed ledger and signed transcript become a broader sense of identity.

(Casey, M.J. 2017, Interview)

This section highlights four use case studies where the Blockchain is being deployed with an education context.

8.1 Open University UK

Interview with Professor John Domingue, Director Knowledge Media Institute (KMI)

The KMI within Open University (OU) is engaged in a number of research initiatives on the Blockchain. This research interest is primarily driven by an interest in next generation web, media, augmented reality, smart cities and analytics: OU is the leader in Learning Analytics in the UK.

Within the context of blockchain research and accreditation, KMI is particularly interested in enhancing standards for badging, certification and reputation on the Web with the use of the blockchain as a trusted ledger. According to Professor Domingue, it was a natural progression to embed open badges within the blockchain project and conduct research on micro-accreditation[44] and e-Portfolios. KMI is levering on the potential of Ethereum for accreditation to turn badges into smart contracts and has developed a prototype for assembling and issuing micro-credentials on a blockchain. The OU, with over 170,000 students, its own MOOC platform (FutureLearn) and its core Open Learn platform (with over 5M visitors a year and 8K hours of course work), has provided KMI with the opportunity to badge all OU courses and notarise these on the blockchain.

KMI's blockchain strategy is holistic, with researchers encouraged to explore the full potential of technology, as opposed to one particular aspect (such as cryptography). Professor Domingue equates this to the early days of cinema: "It took ages for moving pictures to become cinema because people were just interested in filming plays!"

Collaboration networks

Professor Domingue describes internal KMI activities on blockchain as 'experiments with data' while external activities are driven primarily by partners' interests. KMI is working with JISC[45], the educational digital services organisation, to create a blockchain which can be used for all UK higher and further education qualifications. The objective is to facilitate a network that can spearhead blockchain projects in higher education. For instance, KMI, Jisc and the University of Southampton are in turn collaborating as a node in an international version of a blockchain that includes the University of Texas, the

---

[44] Also see Learningisearning2026.org

[45] See Jisc.co.uk

University of Ghent and BT. Other current KMI initiatives include: collaborations with startups Gradbase[46] and APPII[47] on projects that link blockchain accreditation to CVs; working with The University of Texas at Austin on a global network of accreditation badges for micro-courses; and collaborating with BT on providing badging for their new Tommy Flowers research institute; and working with industry on in-company training.

Professor Domingue explains: "Although we continue to develop on the Ethereum standard, we also have third-party organisations' software on our blockchain – for instance BT, who are deploying applications behind firewalls. KMI has the remit to explore partnerships that can have an impact on the present and future of higher education. Within this context, OU is an experimental test bed for new approaches to higher education. Procurement is an ongoing area of applied research for OU within the context of Blockchain research: the supply pipeline and the service that a higher education needs to render may be vastly improved through the intelligent, strategic use of blockchain."

Research and Teaching

According to Professor Domingue, KMI is not necessarily looking to produce or develop blockchain products that generate incremental revenue streams for the OU: KMI remains a research hub, not a product supply-chain for the OU[48]. For research conducted by the OU, the external impact is vital: in the case of the blockchain projects managed by KMI, the non-academic impact is also measured.

According to Professor Domingue, research on the blockchain is not necessarily focused on the end user; nor is it available to be re-purposed by students or third parties. The state of play with blockchain research is comparable to IBM where the focus is on large enterprise systems, with IBM are developing an intermediary layer. Similarly, rather than employing teams of crypto researchers, KMI is more interested in the application layer. Although in principle, people can control their own data and their wallet of private keys, at this juncture, applications tend to be too complex for the average user to adopt without the existence of a technical intermediary[49].

OU is looking at re-engineering student boards (and the way students secure credits) as well as university procurement. Having access to researchers with a background in semantics and web-scale data means that the OU can semantically index the blockchain; it also makes a site more easily discoverable on the worldwide web. User training goes hand in hand with the blockchain becoming part of the web interface. Within this context, the Blockhain can be considered as yet another online development in web interface – similar to developments in mobile interface. Users will secure more control over their data – say through education wallets. User training would therefore be developed at both the conceptual level, at server level, within middle management etc. OU is planning to run online and distance learning courses in April on Teaching Cryptography and the Blockchain.

There are no plans to develop a closed, proprietary blockchain. The approach to the blockchain is synonymous with the Web, with its own protocol and tools. There is a fundamental, ideological principle at stake: as you make it easier for users by introducing

---

[46] See https://gradba.se/en

[47] See http://www.appii.io

[48] OU itself relies on funding from various academic channels, such as US$ 20M for the OU from the Institute of Coding and from various EU projects.

[49] This is similar to the Blockcerts scenario, where Learning Machine is operating as an intermediary in organising the interface for both the issuer and the receiver.

intermediaries (or, say, having closed versions of the blockchain) you find that you are violating the basic, founding decentralised principles of the blockchain.

Blockchain as a disruptor of education models

In his interviews (Domingue, 2017), including with the writers of this report, Professor Domingue is enthusiastic about the promise of blockchain technology as applied to education, positioning the technology primarily as a source of learner empowerment as an opportunity for the re-engineering of the traditional education institution. Specifically, the Blockchain will give learners ownership of their qualifications and associated coursework and feedback, rather than control being vested in educational institutions or employers.

"We are interested in any technology that can contribute, particularly within a UK context, to making higher education better value for money. The centralized model of present-day learning is no longer sustainable – indeed, blockchain technology allows for a total disintermediation and disaggregation of higher education. Today, learning happens increasingly outside the brick-and-mortar lecture hall universities: it happens on online platforms, within communities of like-minded individuals, or by contributing to projects and initiatives in the real world. Blockchain technology may hold the answer to securely and verifiably collating the outcomes of this new distributed learning reality." Students gain control and ownership of all their education data, their accreditation and portfolios of work, in a secure place that is accessible to anyone who needs to verify them – and for their entire lifetime. Within a context where students, teachers and course authors are in a direct relationship with one another, new transactional models will emerge. For example, when a student views a learning video, a small micropayment can automatically be made to the video authors.

Professor Domingue believes that in the medium term, blockchains will present significant challenges and opportunities to the business models of educational institutions. The strategic application of blockchains may dramatically lower administration costs, increase transparency and reduce fraud - in the case of the latter, this is interesting in scenarios where the stakeholders in a transaction mistrust each other. Prima facie, the advantages of blockchain technology are more likely to be readily embraced by higher education institutions with significant brand equity to protect. Within the UK context, where most universities and technical colleges are rolling out fee-paying courses, institutions are also looking at the blockchain as a means of lowering the costs of the hiring process – for instance through the intelligent search of CVs.

Conversely, OU is investigating the 'university of one'[50], whereby the business of teaching in higher education is disrupted and re-imagined through the deployment of new tools, smart contracts and distributed, autonomous, networked organisations. Research interest focuses on alternative approaches that can improve student access to higher education and improving the transparency of qualifications. In the near future, students will not want to embark on a three- to four- year university programme, for a variety of reasons – from financial to opportunity costs. A degree will be deconstructed as an 'a la carte' set of courses. Students will also wish to use plug and play models within an EU context – studying components in different locations and different contexts, and with some modules being undertaken through face to face tuition and others through blended or totally online means.

Within this emerging model, micro-accreditation will take place through a blockchain. Transferability of skills could also be facilitated through the accreditation of MOOCs – again, the future seems to indicate mix and match teaching and learning via different media and different locations for face to face learning. There are also significant opportunities in those areas which are increasingly positioned as alternatives (or in

---

[50] Also referred to as 'the Uber university' in the interview

opposition to) mainstream academic approaches, such as VET, corporate training and the qualifications awarded by professional bodies, such as those in finance.

Blockchains can facilitate and allow for statements for non-formal and informal learning throughout the lifelong learning journey of citizens. This will work particularly well for qualifications such as advanced and higher apprenticeships, where components of the programmes are delivered by a number of different organisations. The content on online education fora, for instance, would be stored on a Blockchain, and facilitate the answering of questions. The information that may be stored about an individual student, for instance, could also be made available to an external examiner of the student's work, enabling a better understanding of research.

Professor Domingue believes that administrative and student-facing processes within universities are ripe for radical change because of the fundamental need for the disintermediation of roles that currently sit within the institution and add little value to the end user – the student. Some components of these process (such as certification) need to be placed within the custodianship of students and not just the institution.

Data Protection

To date, KMI reports that it has not encountered any issues with data protection and blockchains. In the case of research projects where it is a lead partner, only public data is being used, which is in turn placed on the Ethereum blockchain. When working with start-ups, the scenario is somewhat different since some of these solutions are closed': in this case, none of the data or analysis is rendered public. KMI protects privacy through end to end encryption although EU legislation on the right to be forgotten remains challenging. OU is currently only using student data sets to attempt to improve value for money for its paying students.

Professor Domingue identifies two tangible risks at the moment in relation to public perception of data protection issues: a) the unforeseeable release of private data onto a public blockchain; and b) negative publicity triggered by, say, a cohort of students who for some reason or other object to (albeit standard) data being used in conjunction with the affordances of blockchain technology to produce new analytics. In the near future, universities will have to update and develop their ethics policies as they start to understand the opportunities and limitations of blockchains.

Blockchain Analytics and the EU

Professor Domingue believes that learning analytics will become one of the significant affordances of blockchain for education, with a positive impact on both the institution and students:

"Imagine a scenario where every learning activity is registered on the Blockchain, including informal learning – together with informal feedback. All assignment test scores will be mapped on learning environments across Europe. Europe-wide analytics could then be developed from the ground up. The best lecturers in Europe by subject could be easily identified. Learning would become that much more interactive – and reputations built on more tangible matrices".

Professor Domingue suggests that the EU should consider supporting the development of an EU-wide blockchain for experiments in education. Funding would be provided for the more innovative projects on the same blockchain – starting with pilots managed by consortia of universities and other researchers. It should organise an education programme and a set of information meetings for different stakeholders. For instance, colleges should using blockchains to connect with other colleges in different parts of the country, and in different EU countries – fostering collaboration. At the same time, colleges, VET and higher education institutions should also be looking at the registrar function, and how this could be vastly upscaled through the strategic use of a European blockchain. The success of pilots on a European blockchain could then be levered to encourage knowledge-transfer across EU Member States.

8.2 University of Nicosia

Interview with Professor Soulla Louca and Professor George Giaglis

The University of Nicosia (UNIC) has claimed a number of 'world firsts' in its commitment to maximising the potential of the blockchain in education[51]. UNIC claims it is the first university to:

— accept Bitcoin for tuition for any degree program at the university (October 2013);

— teach a university-level course on cryptocurrency, delivered as a MOOC called 'Introduction to Digital Currencies' (January 2014);

— offer an accredited academic degree program – a Master of Science in Digital Currency – taught online in English (March 2014 with first students graduated in june 2016);

— issue academic certificates onto the Bitcoin blockchain, using its own in-house software platform (September 2014).

Discussions with Antonis Polemitis, CEO of UNIC at the ASU GSV Summit, 2017 and a subsequent interview with Blockchain Initiative coordinators Professor Soulla Louca and Professor George Giaglis indicate that UNIC considers Blockchain technology as a cornerstone of its strategy[52], and a point of differentiation from other higher education institutions. Although UNIC's introductory free MOOC on Digital Currencies is not unique[53], it is positioned as the first course of the MSc in Digital Currency. Components of the MSc are in turn repackaged into blockchain professional certification programs which translate into CPD and ECTSs.

In September 2017, the eighth version of the MOOC will be launched. To date, the MOOC has attracted students from 80 different countries and has shown good completion rates. Course content is hosted by UNIC, and continues to evolve because of the university's networks in the global teaching community. The Blockchain Research Centre is positioned as a world class centre on emerging technologies, which will integrate, expand the scope and strengthen the inter-disciplinary research already carried out in this evolving field.

Bitcoin to facilitate payment of tuition fees, admissions and access

When UNIC introduced the Masters in digital currency, one of the first things it did was to allow students to pay in Bitcoin. Both Professors Louca and Giaglis identify this early decision as having significant advantages for the university and students:

— It was perfectly logical to allow students joining a digital currency program that is taught online to pay for their studies with a digital currency. This immediately demonstrated UNIC's commitment to embrace the new technology and its affordances.

— It enabled the Masters course to attract a truly multinational cohort of motivated students, many of whom are from developing countries. Foreign students are normally associated with a legacy of pseudo-remittance cases. UNIC's 'pay as you go' system for tuition fees mean that for instance African students are paying for

---

[51]   See DigitalCurrency.unic.ac.cy

[52]   UNIC's role as a Blockchain innovator in academia has also been recognised by Blockchain industry publications, such as CoinDesk (2016) and the Merkle (2017). See https://www.coindesk.com/the-global-universities-embracing-cryptocurrency

[53]   See https://www.coursera.org/learn/cryptocurrency

their fees on a monthly basis, and avoiding remittance charges associated with traditional bank clearing which may amount to up to 20% of the tuition fees[54].

— Rebuilding the system for issuing certificates and verifying credentials is not necessarily going to solve day-to-day problems for students such as cashflows or administration costs. Being able to pioneer a payment system without an intermediary payment provider adds value to both parties in the transaction. UNIC incentivizes its target students to pay in Bitcoin over Bitpay, its own payment gateway, by offering a 5% discount over net fees.

— Helping someone pay and going the extra mile from a registrar point of view also increases access to higher education: a refugee was given a scholarship for the programme and this in turn led to him securing residency status.

Issuing and authenticating Certificates using a Blockchain

Blockchain certification is one way of bridging the gap between traditional university research practices and the need for pragmatic solutions for the market. UNIC has commissioned its own development team to issue and authenticate certificates using the Blockchain, using the Blockcerts open source standard – its relationship with MIT Media Lab dates back to 2015.

The challenge many universities face is not just admissions offices wary of the fraud associated with taking payments from 'international students', but also long-standing problems of higher education institutions tampering with the numbers of student cohorts. In certain countries people are prepared to pay a bribe for a semi-authentic seal of authenticity from some central authority. There is also no current registrar SaaS that can readily verify identity.

UNIC describes the process for issuing and authenticating certificates using a blockchain in a web link[55]. All the MOOC certificates are being issued using a public blockchain; in June 2017 testing commenced on a system to publish all diplomas using a blockchain by October 2017 and provide software tools so people can confirm the authenticity of certificate through the use of language and other applications. UNIC remains part of the Blockcerts consortium and committed to open standards, but is now using a variety of tools to improve the user-facing interface layers.

Figure 25 below is an illustration of an index of certificates:

---

[54] Transaction payment charges to Cyprus are also high because of the modularity of payments.

[55] See https://digitalcurrency.unic.ac.cy/free-introductory-mooc/self-verifiable-certificates-on-the-bitcoin-blockchain/academic-certificates-on-the-blockchain/

UNIVERSITY OF NICOSIA

INDEX OF CERTIFICATES AWARDED TO THE STUDENTS WHO SUCCESSFULLY COMPLETED THE 6th DFIN-511, INTRODUCTION TO DIGITAL CURRENCIES COURSE OF THE UNIVERSITY OF NICOSIA's MSc IN DIGITAL CURRENCY, AUTUMN 2016

A SHA-256 hash of this index document has been stored in the Bitcoin blockchain on January 19, 2017, in a transaction that will originate from address 1A94iDxxJijPvo8CjCWe4GLUfT6BGTWuUq and will also be announced through the University of Nicosia's website and Twitter account @MScDigital.

On the following pages are the SHA-256 hashes of the certificates awarded to the students who successfully participated in the 6th DFIN- 511 Introduction to Digital Currencies MOOC, offered by the University of Nicosia.

To verify the authenticity of a presented certificate, please follow these steps:

(1) Confirm the authenticity of the index document:
(a) Ensure that you are using a valid index document supplied by the University of Nicosia
(b) The index document PDF can be found at : http://digitalcurrency.unic.ac.cy/free-introductory-mooc/academic-certificates-on-the-blockchain/ and at other online locations distributed by the University of Nicosia
(c) The validity of the index document can be confirmed by reviewing the OP_RETURN field in a blockchain transaction confirmed on January 19, 2017.
The SHA-256 hash of the valid index document, prepended by "UNicDC " (554e6963444320 in hex encoding) will be found in one transaction during that day

(2) Confirm the authenticity of the certificate:

(a) Produce a SHA-256 hash of the PDF certificate to be authenticated using any method or any online tool
(b) Search for the certificate's SHA-256 hash within the authenticated index document.

If the hash is found, then the certificate is authentic

CERTIFICATES OF ACCOMPLISHMENT

Certificates of Accomplishment were awarded to the students who attempted and completed at least 75% of all quizzes and achieved a grade of 60% or above on the final exam of the DFIN-511 Introduction to Digital Currencies MOOC

SHA 256 hashes of certificates awarded:

43392791dd7c5247733f9be8f91e419a3d8bed21c445e353e49d64925b027699
296dd861832844e44b36e7b163e0a2c67a648f031454d418109f05fcae803ebf
df8ed817a150e14ad70b6f200c55e9bbd1bae5199a2af9b82a7bdb1363bb2ed9
9b9d8ca500d8d0fe64f58dca9ba7fe936921c26587e638ce583d7e04264f2b66
f88d748dab2a9e87c26b213867e80d747b0c128ac25e7b6ee155346a37db9513
955c113a44a9c4cb35d6412dac8f249038c49384e6e605027d9a3d00155ffcf9
dbc6fc13ff568e9445a7a5682d5e033472b57e1773595a1fbce50ffa970f4edf
bfb19bef770a05c9706106103d8bf492df1f862b18ef75421e524ec63fcf2539
3be215f0bd5682e6f53e301b6620bb8708184c5484e19533d71f535d85b300fd
2fac30937af41fefc066981ddf68937c359c2f83900df9de638d6994eddebd3a
bc996119794f652347ea35bb287600ef1932bf30654354b2bd81fe9d63d6ec29
15da1de9b16c39280649130356e4b1e452957590e8d131d96565c8ae51046bc7

The need for a standard for certification: scalability and portability

The challenge with issuing of credentials using a blockchain is not the technology – that may well be the most manageable part of the equation. If we want to look at increased widespread applications of the technology – for instance, integrating certificate verification into HR software or using the technology to facilitate the seamless recognition and transfer of credits between universities – the problem that has yet to be solved is the transfer of metadata.

Professor Giaglis notes: "There are difficulties if you want to optimise what you do on the Blockchain and do it at scale. It is one thing to develop technology that publishes PDF certificates; it is altogether more complicated to do have technology that supports full degree transcripts and diploma supplements. Nevertheless, this is doable, and doable now. The real challenge is to scale this technology across higher education institutions so

it gets integrated with internal systems – this is now not dependent on technology, but on the propensity of universities to exchange information; and for employers and other interested parties to validate the authenticity of a certificate without having to contact the university itself in the first place. A student from Bangladesh University should be able to demonstrate that a certificate is authentic and verifiable without having to contact the country that issued the certificate in the first place."

Mr Polemitis notes: "It would be hugely valuable if high schools around the world had some common standard for accreditation and recognition. We cannot have 40 standards on a blockchain. How does this become useful to higher education - which is being fed by secondary education? How can we get everyone to subscribe to the same standard? If any one institution like ours is doing it - it is limited; if a nation state or all higher education institutions and schools in a country come on board – that would be very useful".

Professor Giaglis opines that there is currently not enough traction on Blockcerts to make it the de facto 'standard' for blockchain in education – although UNIC continued to support it, and develop applications on the open standard. "It may well be that MIT has different priorities at this juncture as the early momentum in the community site appears to have slowed down. It is not in UNIC's interest to develop closed applications, independent of the open spirit of Blockcerts. But we do need to move at pace. Sooner or later our paths will hopefully converge and there will be shared experiences which will enable UNIC to tunnel back into Blockcerts as the de facto open standard for the blockchain in education".

Having the CEO as a champion of blockchain means that UNIC is inevitably an advocate for the affordances of the technology. UNIC believes that its commitment to the strategic use of the Blockchain may soon be mirrored in other institutions, and in sectors beyond education, with a network effect that will impact industry – the "real market": there are some doubts that higher education alone can lead the charge to make blockchain technology sustainable in the very short term.

The corollary is that if people in complementary industries can interoperate, there will be inevitable benefits to education. UNIC pointed to the need for a standard, for instance, that could authenticate comments on the Blockchain. Such agreement would lead to network dynamics. The hope is that a de facto open standard will emerge – despite the efforts of enterprise to primary go for closed, proprietary solutions. When people see real life benefits in the implementation of a technology, it is inevitable that a set of commonly agreed metadata will be exchanged.

8.3 MIT

Interview with Mary Callahan, Registrar and Senior Associate Dean, Registrar's Office and Brian Canavan, Senior Associate Registrar at MIT

In 2015, the MIT Media Lab started using Blockcerts for issuing digital certificates to groups of people in its broader community, such as Director's Fellows (Schmidt, 2015; MIT Media Lab, 2016). In the process, MIT has become an advocate for recipients having more control over the certificates they earn, and without having to rely on third-party intermediaries such as universities and employers to store, verify and validate credentials – often at an additional cost. Blockchain technology and strong cryptography have been used in conjunction to develop the Blockcerts open platform for digital certificates and reputation. In June 2017, MIT used Learning Machine (LM) Certificates, a commercial solution developed over Blockcerts, to issue diplomas for two cohorts of students at the MIT Media Lab (Media Arts and Sciences) and the Sloan School of Business. This is the first issuance of such certificates, using LM technology and the first example of recipient-owned diplomas.

Ms Callahan and Mr Canavan identified the following objectives for the two pilots:

- provide alternatives to the current options for official MIT transcripts, which already include eTranscripts[56];

- learn first-hand from students' experience as recipients of digital certificates that have been notarised on a public blockchain;

- gather information that may optimise the development of an administration console;

- secure information that may determine the format for future-proof certificates that are time-stamped, durable, transparent and notarised on the public blockchain;

- gather information from recipients over the summer before expanding their implementation across campus;

- develop confidence and knowledge for a larger pilot in Quarter 4 2017, and much wider deployment at MIT in 2018.

Registrars empowering Students

The selection of the two pilots has much to do with the fact that the majority of the student cohort is international, highly mobile and therefore interested in certification and transcripts as a means of empowerment in different geographical contexts. MIT is particularly sensitive to the needs of these students, and the feedback it receives when issuing paper-based certificates, diplomas and transcripts. MIT is committed to empowering students to own their credentials but does not see its experiments with blockchain technology as being prescriptive: students will continue to receive their paper diploma for the foreseeable future.

The pilots will be invaluable in observing how students interact with the new technology – the student is the critical path in the pilots. Once they download and use the app, students are guided to a console where they are encouraged to provide feedback about their user experience. MIT are using LM data analytics for this purpose, monitoring how students are interacting with the technology interfaces and measuring success against pre-determined parameters for the pilots. The registrars believe that much will be learnt from what learners want from the digital space now – and in the future. Both quantitative and qualitative data will be collected, including data on what students do with the certificate once it has been downloaded.

MIT is approaching the pilots purely from a service perspective. The goal is to provide students with control over some of their own records and let them be their own stewards, raising awareness of the importance of ownership of credentials in a global context, and beyond academia.

Ms Callahan observes: "Starting with their own diplomas, students will realise that they can operate without the university as an intermediary. Without an intermediary means that as Registrar, I am not involved in the transaction. There needs to be trust that the diploma is bona fide and issued by MIT, but now also residing on a blockchain. Right now, that gives me great confidence that the credentials are protected and there will not a risk of spoofing. Students get control of their record – it is certainly a different dynamic to making paper copies. We have such a global group of students and this diploma will be forever deliverable for higher education. It is a composite of things that come together in this pilot – it can become a truly transformative approach for higher education. Whatever happens we will learn a lot – we will determine if our contribution is really fulfilling a need in higher education".

Mr Canavan reiterates that the litmus test is the learner. "As registrars, we are getting our hands dirty. We will get data which will loop back into improving administration. It is

---

(56)   http://web.mit.edu/registrar/records/transcripts/official.html

certainly not a way of saving costs for MIT. Our objective is to empower the learner, to translate our efforts for the student's benefit."

Other considerations for the present and the future

MIT's decision to use Learning Machine certificates to issue digital diplomas as opposed to building in-house applications in line with Blockcerts, was based on the state of readiness of LM's technology for the pilots and their speed to market. LM are also considered to be arms-length MIT trusted partners because of their collaboration on Blockcerts. As an advocate for open source, issuing diplomas using the LM certificates retains MIT's capability to take over future development since the certificates are built on Blockcerts, which means that the code is fully accessible. Each diploma has a badge that links back to blockcerts.org, so anyone can inspect what is happening, how it works, what is on the blockchain, etc. – there is no 'black box'.

Ms Callahan says that at this juncture, there has not been much thought on more complex issues such as standards for certificates or credit transfers of institutions; whether the pilots will lead to research and academic publications; how blockchain records could interface with HR systems; or how collaboration networks with other universities could evolve – into say a private blockchain between reputable universities.

"We don't want to be coy, but we don't know as yet (about these issues). There is significant interest from MIT faculty to certify some level of knowledge, and particularly to look at academic programmes and research that have not yet resulted in a degree or a credential. Perhaps blockchain technology can help us find a way of credentialing some of this learning. We could also be looking at standardising our contributions to blockchain. But we are not there yet".

The pilots have been developed in such a manner that they can be rapidly scaled up for other faculties within MIT, and accommodate much higher volumes of transactions. Lessons learnt from the experience by the registrars are likely to serve colleagues in higher education, including those who have already expressed an interest to develop their own applications. There is an awareness that a pilot in a high-profile environment such a MIT's will inevitably have an impact beyond systems and procedures that are native to MIT. The next issuance of diplomas is scheduled for September 2017, after which date plans will be made for a larger, more robust pilot. At this stage, the registrars will also consider the advice of members of faculty who may well wish to have a more federated approach, from their learning perspective. To date, the registrars are guided by the technical expertise within MIT that has identified the blockchain as a technology of the utmost security that meets the requirements of a top university with a brand with significant brand equity: the risks of scooping are minimal.

Mr Canavan confirms that the MIT Registrar's office has been working with Learning Machine to refine the product's rough edges, since MIT is the first to use it. Many good ideas have been exchanged for future enhancements. "At the moment, when we issue a diploma certificate on the Bitcoin blockchain, it may take up to 30 minutes for the data to be processed - but that is reasonable considering the time savings for MIT and learners in the future who require transcripts. Lessons are also being learnt by Learning Machine, so we expect improvements in the user interface in the near future. A small example is when we have a recipient list and we used to host those lists. Our expectation is that this data will eventually be exchanged digitally with little human information - right now there is still a significant need for human intervention. This is particularly important if we want to start to address the full cohorts of students".

MIT uses third-party transcript vendors to publish transcripts. It is highly likely that such vendors will also be monitoring developments linked to blockchain: it would not be surprising to see vertical partnerships in the industry in the future. The MIT Registrar's

office is open to sharing its future blockchain experiences with others considering doing pilots which may benefit the end user[57].

8.4 Maltese Educational Institutions

While many governments have expressed an interest in implementing blockchain technologies as part of their eGovernment efforts, few have committed to actual technology rollouts[58].

The Republic of Malta has been considering a nation-state pilot on the Blockchain in education since 2016. Malta's aspirations to be proactive in the blockchain space are not restricted to education, but to become a 'blockchain island', in a similar vein to other small or island states, such as Mauritius (see Stanley, 2017): Malta has a track record of pioneering technology, including telecoms and online gaming, earning a reputation for being an 'island lab' (ASU GSV Summit, 2017) in the EU for the testing and rapid deployment of new technologies. There is no one unique factor that differentiates Malta from other jurisdictions seeking a similar positioning other than a composite of factors: strategic location, size, topography, social diversification, language and proactive role within the EU – and perhaps most importantly, access to policy-makers and the political class.

In January 2017, the Ministry for Education and Employment (MEDE) signed a Memorandum of Understanding with Learning Machine Group (LM). The MOU coincided with the conclusion of a conference held between 19th and 20th January 2017 as part of Malta's Presidency of the Council of the European Union[59]. The MOU signalled the intention of both parties to develop and implement a Malta pilot of LM's nation-state technology platform, which is based on the Blockcerts open standard developed by LMG and the MIT Media Lab.

MEDE believes that the strategic deployment of Blockchain technology signals Government's commitment to provide learners and workers with maximum ownership and portability of their own official records of learning achievement. The stated objective of the pilot is self-sovereignty - to lever on the affordances of the Blockchain to empower Maltese citizens to own their credentials, as fully contributing, skilled members of the 21st century workforce which is increasingly mobile, international, and self-developing (as lifelong learners). The secondary objective is to continue with ongoing initiatives to internationalise and cross-reference credentials secured from Maltese institutions with EU frameworks[60].

---

[57]   MIT describe their experience with the Blockchain pilots: see http://news.mit.edu/2017/mit-debuts-secure-digital-diploma-using-bitcoin-blockchain-technology-1017

[58]   The Republic of Georgia is an exception to this trend. In February of 2017, they signed an MOU with the Blockchain company Bitfury to log real estate transactions on the Blockchain. Georgia uses a combination of private and public Blockchains as part of its digital real estate initiative. It logs details of the transaction on the private government Blockchain while also encrypting those details into a "hash" that is stored on the public, Bitcoin Blockchain. That way, any individual can verify the authenticity of real estate ownership certificates without seeing the details of the real estate transaction itself. In the real estate purchase use case being implemented by Georgia, keeping the details of the transaction private makes sense.

[59]   See: links for "The State of Digital Education: Engaging with Connected, Blended and Open Learning" at https://education.gov.mt/en/digitaleducation/Documents/conference_magazine.pdf and a subsequent manifesto on digital education at: https://education.gov.mt/en/digitaleducation/Documents/Malta%20EU%20Presidency%20Digital%20Education%20Manifesto.pdf

[60]   Malta is a full member of the Bologna process / higher education area since 1999. The Malta Qualifications Framework (MQF) assists in making the Maltese qualifications system easier to understand and review, and more transparent at a national and international level. The MQF is also a referencing tool that helps to describe and compare both national and foreign qualifications to promote quality, transparency and mobility of qualifications in all types of education: it is primarily referenced to the European Qualifications Framework (EQF) as well as to other non-European qualifications frameworks.

MEDE selected the LM solution specifically because it is built on Blockcerts, an open-source initiative that is OBI-compliant and sets out a common path for learner and worker-owned official records. The LM technology to be deployed in the nation-state pilot provides policy-makers to advanced analytics. Having been built specifically for academic credentialing and professional certifications, the solution supports the creation, issuing, viewing, and verification of blockchain-based certificates. The digital certificates for participating institutions will be registered on a public blockchain and cryptographically signed, and, as such, are tamper-proof and immediately useful when applying for employment, university or immigration. The Malta pilot will commence with a public chain for educational records, with the caveat that this is both scalable and flexible, with the option that citizens who receive blockchain credentials will benefit from both public and private blockchains in the future.

Although certificates are being issued using a blockchain (a distributed p2p data store that does not reside in any one geography by design), the certificates themselves can be hosted anywhere if countries and recipients want to use the web to display and validate them. Anything that is hosted on the web (from the data entered into the issuing platform to the certificates stored after being issued) is held in an encrypted, private EU data environment that is fully compliant with all EU data protection laws[61]. The data and analytics interface will only be accessible to authorized users given access by the Maltese government.

Education perspective: Parallel pilots at three institutions

On 22nd September 2017, MEDE signed a contract with LM to implement four separate pilots at the Malta College for Arts Science and Technology (MCAST), the Institute for Tourism Studies (ITS) and the National Commission for Further and Higher Education (NCFHE), commencing Q4 2017[62]. The University of Malta is also in discussions on a strategic partnership with LM on a blockchain credentialing pilot and academic research.

MCAST Diplomas

LM will provide MCAST an issuing workspace to design diploma templates, approve recipient lists, and issue digital diplomas to graduates through an opt-in process. Recipients who choose to receive their diploma in this format can share them online or directly with others (schools, employers, etc.) in a format that can be independently verified as authentic. MCAST benefits from fraud protection and a new form of marketing & analytics that arise from the sharing of these digital diplomas.

ITS (Training Certificates)

Similar to MCAST, LM will provide an issuing workspace to the Institute for Tourism studies (ITS) for conferring digital certificates of completion/achievement to students. These official digital certificates can be provably owned by graduates and contribute to their lifelong record of learning. ITS benefits upgrading digital infrastructure with latest technology that ensure fraud protection and public presence that raises the profile of ITS.

NCFHE (Equivalency Statements)

LM will provide an issuing workspace for the NCFHE to create templates and issue statements of educational equivalency to learners upon request, to replace the PDF-based process currently used. The benefits of these blockchain-based records are fraud protection for the NCFHE and instant verification for any entity that wishes to check the authenticity of the statement. These equivalency statements are owned by the NCFHE, not recipients, so the implementation process is relatively simple. An ongoing application of equivalency statements is for the certification of credentials of people who claim

---

[61]   Also see Smolenski (2017b)

[62]   See http://connectedlearning.edu.mt/malta-first-nation-state-to-deploy-blockchain-in-education/

refugee status, arrive in Malta as irregular migrants or who for some reason cannot readily secure access to their academic credentials.

NCFHE (Accreditation and Licensure)

LM will provide a second issuing workspace for NCHFE to issue certificates of accreditation to the 100+ institutions they regulate. The benefits of these records are fraud protection for the NCFHE and more convenient verification of institutional accreditation for providers that operate outside of Malta's borders. Estimated launch date is June 2017, but may be vary based on NCFHE's timing preference.

The Malta pilots will involve registrars, technologists, researchers and policy-makers. The objective is that strategic decisions on scalability and private vs public blockchains will also be made in the process. There are benefits associated with writing certificate data to both public and private chains. When certificate data is logged on a public chain, that enables learners to completely own their entire record of achievement: this means they can present their certificate to any employer, any admissions committee, or anyone else, and that third-party can instantly see the entirety of the credential's content and verify its legitimacy.

Beyond Education: The Nation-State perspective

The MEDE pilot is being positioned as a live case study for the National Blockchain Strategy for Malta (Diacono 2017a, b). In July 2017, Malta appointed a Parliamentary Secretary within the Office of the Prime Minister (OPM) to drive national initiatives related to the digital economy. The pilots on education certification are therefore being deployed within this wider framework, as the first examples of praxis. There are clearly many potential e-government projects[63] that would also benefit which involve the issue of certificates on the Blockchain. The following is an ongoing list identified by OPM: Health Care; Land Registry; Notarial Acts; Life Events (Births, Marriages, Death Certificates); Address Points; Police Conduct; Court Case outcomes; Driving Licenses and E-Democracy Events.

The education pilots will also be monitored while planning for pilots in more challenging areas, such as finance.

---

[63] Malta has a reputation for excellence in the delivery of eGovernment services. In a 2016 study commissioned by the European Commission, Malta led rankings in all top key indicators measuring the delivery and performance of eGovernment services. See European Commission, eGovernment Benchmark (2016), available at: https://ec.europa.eu/digital-single-market/en/news/eu-egovernment-report-2016-shows-online-public-services-improved-unevenly

9 Government and Blockchain Technology

Governments and regulatory bodies world-wide are closely monitoring technology advances in blockchain technology. The benefits of this are likely to be profound for government – delivering productivity, security and efficiency gains. Blockchains can be used as a common reference point to bring together different levels of government (local, state and federal) to host government registries of open data. This may mean more reliable integration across government services, improved mobility and business consistency across states and better regulatory oversight when blockchains record operational information in regulated industries[64].

9.1 Considerations for Policy Makers

The social value proposition of blockchains discussed in section 4.2 is of fundamental importance to government. For policy-makers, assessing the current and future impact of a disruptive technology such as blockchain - and determining the policy choices to be made and strategies to be developed as a result - is a particularly complex exercise. This is not just due to the newness of the technology, and the uncertainties over how it will be adopted by various stakeholders in the near and medium-term future. The complexity has much to do with the *relative importance that stakeholders may attribute to the value proposition of blockchains*. There are potentially conflicting interests at play in disparate groups of stakeholders, where such groups may be numerous and sometimes not readily identifiable. What may be a value proposition to one stakeholder group may well constitute a risk that needs to be mitigated by another user group. Government has the additional onus of having to mitigate risks and identify policies and strategies that may be implemented for the 'public good'.

If we had to quickly assess the relative importance of the five principles making up the social value proposition of blockchain to Government and compare this with the likely assessment of the three other primary stakeholders in the education landscape, differences in evaluation are revealed.

Table 1 is a snapshot of key stakeholders' assessment of the social value proposition, indicating potentially conflicting positions and agendas:

---

[64] Two recent publications by the Government of Australia conducted by Data61, the innovation arm of the Commonwealth Scientific and Industrial Research Organisation (CSIRO) provide fascinating insights on the emerging technology and its impact on both private and public-sector organisations. One focuses on four possible scenarios for blockchain adoption in Australia, while the other centers around the opportunities and risks for the technology in several application areas, including government registries and agricultural supply chains. These publications are essential reading for policy-makers interested in the opportunities and risks for Government planning for a mass take-up of blockchain technologies. See Hanson et al. (2017) and Staples et al. (2017) for a deeper analysis on some of the ideas discussed in this section.

		Government	Industry / Stakeholder Bodies / Self-Regulatory Bodies	Education Institutions	Learners
1	Self-Sovereignty and Identity	High	Uncertain	Medium	High
2	Trust	High	High	High	Uncertain
3	Transparency and Provenance	Uncertain	High	High	High
4	Immutability	High	Medium	Medium	Medium
5	Disintermediation	High	Low	High	Uncertain

The rate of change and the speed of introduction of new, disruptive technologies add to the complexity of assessing the social value proposition – particularly since scale, speed and complexity must be *considered together*. It becomes increasingly difficult for governments to understand this mesh, and to plan, implement and realise benefits using their traditional non-collaborative organisational structures.

There are several 'unknowns' at play that impact the social value proposition for Government, at the core of which lies a communication dilemma:

— The 'market' for blockchain's social value proposition has still to be developed: for instance, although blockchain technology is forecast to impact many areas (see Annex 1) to date, it is currently synonymous with fintech, not education, the subject of this study.

— Attempts at communicating the value of blockchains to society at large are currently within the domain of specialist researchers, academics and industry insiders. There is a need to communicate the very complicated concepts in a clear and comprehensible manner that can resonate with target audiences within the various stakeholders if we are to make rapid progress. This process has yet to start.

> *"It is often assumed that if blockchain technology has significant benefits, then it will inevitably be adopted. However, there are many challenges to the adoption of blockchain. First, the many risks and limitations of blockchain must be weighed against their possible benefits. Second, the path to adoption of a technology is not always clear, especially where many of the benefits are significant only with large-scale adoption because of network effects, and where it is not clear whether the parties who benefit also bear the costs of deployment and operation. Third, the potential disruption and disintermediation enabled by blockchain may be a threat to powerful incumbent organisations who may act to limit the acceptance of blockchain technologies"*
>
> *(Staples et. al. 2017)*

When considering how to engage with the fundamental social value propositions of blockchain technology, policy-makers therefore need to strike a balance between the excitement that is rightly associated with a technology that has significant potential for public services and the public good; and the uncertainties on the very fundamentals of the technology, which therefore call for policies and strategies that are as much rooted in caution and forethought as they are driven by the opportunities to secure a competitive advantage over other nation states.

Table 2 tabulates some of the primary considerations for policy-makers in Government when engaging with the fundamental social value propositions of the Blockchain[65]. In reality, these principles are inter-linked, so issues raised are likely to be cross-cutting across a number of areas, also reflecting the very nature of Government and public service.

---

[65] These considerations are based on interviews with industry experts and on recent research commissioned by the Australian Government. See Hanson et al. (2017) and Staples et al. (2017)

Table 2: Considerations for Policy-makers on the Social Value Proposition of the Blockchain

SOCIAL VALUE PROPOSITION	CONSIDERATIONS FOR POLICY-MAKERS
Self-Sovereignty and Identity	— At face value, democratic governments in the EU would be expected to be supportive of new technologies that empower citizens' self-sovereignty. From a pedagogical perspective, the principles of self-sovereignty are at the core of the European project.
	— Governments are taking different approaches in determining how to engage with blockchain technologies. Self-sovereignty inevitably opens up a Pandora's box on data ownership, data protection, verified online identities, user privacy, eID systems, user identity verification in a decentralised verification environment – to name a few. What represents a self-sovereign right for citizens and learners in particular, may well be a threat to the traditional way governments have organised their proprietary information and e-identity systems. *Digital identity management* therefore presents the benefits of bolstering trust and certainty for economic activity, but continues to pose challenges to Government in terms of privacy and security.
	— If we were to use a technology metaphor, on a blockchain a citizen's digital identity is represented by an anonymous public/private key combination. From a government perspective, there is the need to tie digital identity to a real human being: this may mean tying it to a social security number or, in the future, biometric data or some hash of biometric data. In the near future, our fingerprints may become our default private key[66][67].
	— It is reasonable to assume that organisations working on eGovernment solutions in Member States will already be researching and considering the development of solutions that enable notarisaton on a blockchain. These organisations may range from in-house technology teams to niche startups. For instance, Procivis[68], a Swiss technology firm, develops 'government trusted electronic ID solutions built around the safeguarding and self-sovereignty of personal data'. Its *Procivis eID+* product levers on biometrics, cryptography and the blockchain to provide both Government and the end user with a tamperproof digital

---

[66] At a recent Ethereum summit, Melanie Shapiro, CEO of Case, announced that her company is developing applications that use biometrics for deployment via the Case Wallet. At a recent Ethereum summit she said that Case are working with biometrics. See www.choosecase.com.

[67] A blockchain wallet could be used as a hard wallet and secured with a biometric key and keep a thumbprint record which is in turn *kept securely in pieces so there is no centralised record*. You can then give some security to the thumbprint as well. It is likely that there will be industry announcements on this aspect of the Blockchain in the near future.

[68] See www.procivis.ch

	identity. Procivis are working through issues related to real person / Government vs Blockchain attestation of identity to create one to one shops for eGovernment applications. This dual accreditation challenge is likely to resonate with any member state that has invested significantly in e-identity systems and now needs to understand how the self-sovereignty at the core of the Blockchain proposition impact the affordances of existing e-identity systems.
	— As the operator of national eID systems, Government has a duty of trust in identifying users online and linking their digital to their 'real life' identity, since such identification is critical to establishing trust in transactions, and for accessing essential services. Digital identification services currently verify claims about the attributes of an identity, usually by assessing the provenance of a supplied document. In our globalised world, every commodity consumed corresponds to the movement of people, and/or materials across locations. The underlying supply chains, however, are often opaque to the end consumer. Creating transparency and provenance for consumer goods, by identifying and cross-referencing their relationships with locations and people, enhances trust and confidence in these transactions. Proof of identity is, however, one of the most fundamental, often challenging, and resource-intensive transactions involved in the digitised world.
	— There is awareness within Government that all the sources of verifiable data are not necessarily 'talking to each other'. Blockchains could give a student the permission to have rights to his or her data, and in turn assign the rights to share this data – creating a chain. This would be tantamount to empowering an individual to be able to give permission to institutions to talk to each other as opposed to assuming that the institutions will do this on his or her behalf. Power is pushed through a master key that is kept by the individual who then decides what to do with variants of his or her identities. Smart contracts, if programmed properly, could choose the entire sets of authorisations and certifications and then you provide the learner (or a third-party like a potential employer) with the requisite assurances that everything is in order.
Trust	— Blockchain technology is of significant importance for its potential to generate trust on the internet, where trust is difficult to establish.
	— Despite claims that the blockchain heralds the arrival of a 'trustless society[69]', using a blockchain does not remove the need for the basic principles of trust to continue to be applied. Users are still inevitably exposed to an element of risk in their use of blockchain technology. In a blockchain, what is trusted (relied upon) is the blockchain software, the incentive or contractual mechanisms driving the behaviour of processing nodes

[69] Blockchain technology integrates networks with databases resulting in a peer-to-peer based distributed database spread across multiple entities, with no single owner or single point of failure. Blockchain technology removes the need for trust because immediate synchronisation ("near real time") across entities means no single trusted third-party is needed to guarantee that the transaction occurs - hence the claim for the 'trustless society'.

	that operate the blockchain system, and the trusted third parties that act as 'oracles' which record information about the external world on the blockchain. Although a blockchain does not remove trust, it can remove the need to trust a single specific third-party to maintain a ledger, and so is sometimes called a 'distributed trust' mechanism. In a blockchain-based system, the trust boundaries are wider. For example, if users access a blockchain through an intermediary, such as a digital currency exchange, they trust that intermediary: if the intermediary's system fails, their users may lose control of assets on the blockchain.
	— At this early stage in its development, policy-makers have to consider what the blockchain can be trusted to do, and for how long. The experience to date with Bitcoin is that the digital currency can be trusted to retain its integrity because it cannot be counterfeited. The ongoing discussion, however, is whether the blockchain can perform for use cases beyond digital currency – such as the education sector. The challenge with software is that is essentially a black box – and particularly for policy-makers with a tradition of minimising risk and maximising control over enterprise software. Trust is subjective, conditional and contextual – and is typically dependent on trusting something or someone to perform a particular action. New distributed ledger technologies (DLT) primed to go beyond digital currencies need time and experiments to build their reputations and awareness for what they can be trusted to do. Governments will be sensitive to the fact that reputations are built over time, and tightly coupled with performance. Poor performance quickly erodes trust, and people's trust in machines erodes much faster than in people.
	— Understanding technological capabilities is therefore paramount for regulators so they may ensure they are able to set appropriate regimes with respect to information disclosure, fair commercial practices, such as quality of service, and dispute resolution and redress. The core benefit is the underpinning capability of distributed ledgers to establish a fact at a given point in time, which can then be trusted. The distributed ledger is able to act as an *oracle* – where an oracle is any source of information that is deemed to provide credible and reliable (trusted) information – and that in turn can be used as a reference that contributes to the integrity of other transactions. A distributed ledger could be an oracle for identity, content and/or transactions.
Transparency and Provenance	— In principle, blockchain technology should contribute towards governments increasingly obliged to operate in a transparent manner, and demonstrate provenance when required.
	— Distributed ledgers can store digitised representations of real-world transactions that may be trusted to prove the history of an asset or object. By tracing the transactions, the identity of the asset or object (or the current owner) can also be demonstrated. Whilst this may be easier for an easily identifiable asset (such as an academic certificate), a commodity like grain or milk generally requires a proxy for each asset unit such as an RFID tag – increasing the assurance being provided but not providing absolute provenance. Blockchain technological would significantly contribute towards guaranteeing provenance, with significant positive impact on related Government activities and markets.

	— Blockchains can also contribute to better governance, since the permanent and persistent storage of assertions, or transactions, allows for them to be trusted for evidentiary purposes. Through the transparency and immutability of the ledger, blockchains present opportunities for regulators to access high integrity records of transactions in real or near-real time. Programmable transactions and automated contract tools would enable regulators to enact granular and risk-based market controls aligned with this surveillance.
	— Blockchain software can embed other information - making a blockchain register much more reliable than the orthodox register of property transfers and paper records and officials who could be bribed!
	— The corollary to this is that openness does not necessarily mean open software, or vendor independence: indeed, some of the more innovative blockchain applications deployed by Government are currently dependent on partnerships with a small number of trusted, external, specialist partners and processes that are neither transparent or necessarily incorruptible (being dependent on private blockchains, for instance).
Immutability	— Individual self-sovereignty has much to do with the affordances of a blockchain as a tamper-proof environment: by which we mean that a permanent record is guaranteed since no data is ever deleted, and only appended to the blockchain.
	— From a Government perspective, immutability is associated with security as much as it is associated with standards and interoperability. The dilemma governments face with the blockchain is that a fundamental reason for their very existence is predicated on long-standing notions of trust in their ability to function as representatives for the common good, as trusted intermediaries. Immutability, therefore, has much to do with the ability of a government to develop and administer immutable (and hence secure) systems, levering on state of the art technology which is administered solely by government or its trusted intermediaries. At present, it is challenging for policy-makers to delegate that responsibility to, say, the public blockchain – despite the claims made that in practice it is likely to be more secure and tamper-proof that any system that relies on the administration by central government (introducing multiple points of risk and failure etc.).
	— Standards enable complex ecosystems to form and evolve. However, in order to be relevant and drive innovation (see section 10.1 for more on standards), they require a relatively stable and defined system.
	— Interoperability is more than seeking agreements on technical configurations. There needs to be trust in the market that the standard will be adhered to. Interoperability involves three key factors:
	a) Data interoperability. We need to understand each other in order to work together, so our data has to have the same syntactic and semantic foundations.
	b) Policy interoperability. Our policies need to be aligned or based on agreed common policy, so that I can be confident that you will treat my information in the way that I expect (and vice versa)
	c) The effective, collaborative implementation and use of international standards. The participation of

	numerous countries in the current international standards development exercise, however, makes the global adoption and uptake of relevant standards more likely. — Interoperability also occurs at the legal layer. Whilst software is global, the law is not. Complex legal questions may occur when executing 'smart contracts' across multiple jurisdictions. In particular, the question of which jurisdiction the 'smart contract' is operating in is a fundamental determination. The distributed ledger could also potentially be required to be compliant with an unwieldy number of legal and regulatory frameworks for many, if not all the jurisdictions it is operating in. Customary law and trade practices are often benchmarks that support dispute resolution in multi-jurisdictional scenarios. The disruptive potential of distributed ledgers includes potentially new business models, and new value chain participants, however, this means accepted industry norms are yet to be formed and tested. Distributed ledgers need to be tested for failure in both an operational and a legal sense. — Casey (2017) suggests that at this juncture it is prudent for policy-makers to be" deliberately agnostic" about the various debates on public versus private or hybrid blockchains. The situation on the future of the technology is at best fluid so interoperability is the only sensible option to support.
Disintermediation	— For Government, disintermediation through the removal of third-party control of ledgers (specifically asset and transaction data management) may be interpreted as decentralisation: for a number of socio-cultural, economic and political reasons, governments tend to be suspicious of disintermediation. It will be vital that policy-makers also consider the fact that: a) a centralised authority always represents a potential single point of failure; and b) a blockchain that is not Government-owned may provide a much more robust infrastructure to protect against the loss of records[70]. — Governments will worry about scalability. Blockchain systems such as Bitcoin and Ethereum cannot currently match the maximum throughput of conventional transaction processing systems such as the Visa payments network. This is a known and current limitation, but is being addressed by the development of new mechanisms. While blockchains are currently not highly scalable, this is not necessarily an inherent limitation, and may be overcome in the medium-term future.

([70]) Also see Annex 2 for more information on Decentralized networks.

9.2 Snapshot of ongoing initiatives in EU Member States

The majority of EU Member States are likely to be experimenting with blockchain technologies. Some are working on national strategies, while others are conducting trials of specific applications.

The corollary to the considerations in section 9.1 is that blockchain technology may represent an opportunity for those nation states who are more agile, such as small and / or developing nations, and who perceive the Blockchain as a means of making significant advances that can lead to transcending borders and provide international benefits. The following data is primarily compiled from desk research, and is included here to contextualise the issues identified above through specific country perspectives. Section 8.4 also includes a use case study for Malta.

9.2.1 Estonia

As a nation-state, Estonia has long been associated with the concept of the digital society[71] and more recently with blockchain technology. After the nation-wide cyberattacks of 2007, the government decided to secure its digital infrastructure through radical new technology. In 2007, supported by Government and the private sector, a team of Estonian cryptographers, network architects, software developers and security specialists started to design the digital signature system that would eventually lead to a technology called **Keyless Signature Infrastructure** (KSI) to safeguard all public-sector data. Today, almost all public services in Estonia are digitalised and accessed through secure digital identities that are provided to every citizen and resident.

Experiments with blockchain technology commenced around 2008. The Estonian government is not operating a full-blown blockchain eco-system, but levering on its significant expertise in digital identity management to develop private blockchains in conjunction with trusted partners. Estonia's position is that crypto-currency protocols are excellent for what they were designed for, but not for large scale enterprise data supply chains.

A blockchain is at the core of the Estonian national identity management system: almost all public services are digitalised and accessed through secure digital identities that are provided to every citizen and resident. Citizen interactions with the state are facilitated through a raft of e-services and programs, including i-Voting, e-Tax Board, e-Business, e-Banking, e-School and most notably e-Residency[72], a program that offers electronic residency to people from outside the country. Since 2012, blockchain technology has been in operational use in Estonia's registries, such as national health, judicial, legislative, security and commercial code systems, with plans to extend its use to other spheres such as personal medicine, cyber security and data embassies. Estonia relies on a centralized validation authority to confirm the validity of certificates, using a one-way hash system to cryptographically seal identity documents, which they also publish in newspapers to prevent date spoofing. Since 2013, Estonian government registers — including those hosting all citizen and business-related information — have used Guardtime's KSI to authenticate the data in its databases.

Estonia's national public key infrastructure (PKI) enables secure digital authentication and signing. The infrastructure also allows forwarding data by using an encrypting key pair: a public encryption key and a private decryption key. The technology is used in relation with electronic identity (ID card, mobile ID, digital ID). The public key infrastructure used in Estonia is the national PKI, which means that the state undertakes to assure the existence and functioning of a public key infrastructure.

(⁷¹) See https://e-estonia.com and https://www.eesti.ee/en .

(⁷²) See https://e-resident.gov.ee

Many of the services related to the PKI are purchased from the private sector, such as the certification, the infrastructure for making enquiries about the validity of the certificate, the infrastructure for distributing the public key (LDAP service), the key creation environment (e.g. ID card chip). Digital authentication is critical to government, business and public services alike, from drafting policy and legislation, to declaring finances and registering property and inheritance rights[73]. The custodianship and accuracy of public records are vital to Estonia: PKI renders them tamper-proof from the inside, or by a cyberattack. Ultimately, the KSI block chain means that while the Estonian ID Card may never be immune to a breach (although there have been none so far), the government is assured that rogue alterations to public data will be 100% detectable.

Keyless Signature Infrastructure (KSI)

KSI is used for independent verification of all government processes in Estonia, protecting e-governance services offered to the public. KSI pairs cryptographic 'hash functions' with a distributed ledger, allowing the Estonian government to guarantee a record of the state of any component within the network and data stores.

Using a blockchain provides exabyte-scale real-time authentication since because every alteration of a piece of data is recorded. By providing proof of time, identity and authenticity, KSI signatures offer data integrity, backdating protection and verifiable guarantees that data has not been tampered with. It is transparent and works to the user's benefit too: citizens can see who reviewed their data, why, and when; and any alterations to their personal data must be authorised. Moreover, through using hash functions, as opposed to asymmetric cryptography used in most PKI, KSI cannot be broken by quantum algorithms. It is also so scalable that it can sign an exabyte of data per second using negligible computational and network overhead. It removes the need for a trusted authority, its signed data can be verified across geographies, and it never compromises privacy because it does not ingest customer data. It is clear that the system marks a major advancement in PKI.

It creates hash values, which uniquely represent large amounts of data as much smaller numeric values. The hash values can be used to identify records but cannot be used to reconstruct the information in the file itself. The hash values are stored in a blockchain and distributed across a private network of government computers. Whenever an underlying file changes, a new hash value is appended to the chain, and this information can no longer be changed. The history of each record is fully transparent, and unauthorized tampering from within or without the system can be detected and prevented. KSI allows government officials to monitor changes within various databases—who changes a record, what changes are implemented, and when they are made. The electronic health records of all Estonian citizens are managed using KSI technology, and the country is planning to make KSI available to all government agencies and private-sector companies in the country.

Estonia is levering on its significant experience and reputation with verified online identities and eGovernment to develop a smart policy framework for blockchains. This

---

(^{73}) By using their ID card, citizens can order prescriptions, vote, bank online, review their children's school records, apply for state benefits, file their tax return, submit planning applications, upload their will, apply to serve in the armed forces, and fulfil around 3000 other functions. Businesses can use the ID card to file annual reports, issue shareholder documents, apply for licenses, and so on. Government officials use the ID card to encrypt documents for secure communication, review and approve permits, contracts and applications, and submit information requests to law enforcement agencies. Ministers even use their ID cards to prepare for and conduct cabinet meetings, allowing them to review agendas, submit positions and objections, and review minutes.

framework will eventually extend to education, with the collation of all academic certifications issued by higher education institutions. It is uncertain at this juncture if:

— the system will be positioned as the national education database, and whether and how the data would lever with the shared e-identity base and used for applications beyond education (for instance, labour market purposes);

— the Estonian national database for qualifications / credentials will interact with the Blockchain applications;

— all universities in Estonia will be participating in the framework.

9.2.1.1 Key Players in Estonia e-identity initiatives

Guardtime[74]

This is the world's largest blockchain company by revenue, headcount and actual customer deployments. It has a team of over 130 cryptographers, developers and security architects, with decades of experience defending networks from nation-state attack. It underpins the operations of government and its customers include the largest global defence and telecom vendors.

Guardtime's mission is to validate online information and make it universally reliable. Within this context, states that the most valuable application of blockchain is for software, physical and information supply chains that are within and across organisations. The company claims it helps clients understand those supply chains and build solutions to harden them, eliminating inefficiencies and providing mathematical certainty for their integrity - track and trace at the digital and physical item level.

The Guardtime stack is the Unix philosophy applied to blockchain - abstraction and encapsulation into layers, each of which does one function well. This approach provides scalability, interoperability, reliability and works with legacy systems.

Services reflect a very wide set of focus areas. These are listed as: Critical Infrastructure Protection; Enterprise security; Big Data Archiving; Data Breach Management; Insider Threat Mitigation; Object Storage; DevOPs; Cloud Radio Area Networks; Advertising Attribution; Cloud Assurance; eGovernment; Internet of Things (IoT); Connected Vehicle; GDPR Compliances

Clients are in telecoms, defence and aerospace, Fintech, Insurance, eGovernment and digital advertising.

Information System Authority (RIA)[75]

The Information System Authority (RIA) is a governmental organisation established in 2011 and currently reporting into the Ministry of Economic Affairs and Communications. coordinates the development and administration of the state's information systems, and coordinates all activities related to information security. RIA advises the providers of public services on how to manage their information systems as per requirements and monitors them. In addition, RIA is an implementing entity of the structural assistance of the European Union.

SK ID Solutions (SK)[76]

---

[74] See https://guardtime.com

[75] See https://www.ria.ee/en

Founded in 2001 by Swedbank, SEB Bank and Telia Eesti, SK specializes in international e-identity solutions.

SK is the official, state-accredited provider of certification and timestamp services and validity confirmation services that processes client data. As the partner of the Estonian state, SK is responsible for issuing certificates for national identity documents (ID-card, Mobile-ID, Digi-ID, residence permit card and e-resident's Digi-ID).

SK's software for using ID-card includes the DigiDoc software, which enables digital signatures, checks the validity of signatures and encrypts data. Currently SK enables the citizens of different countries to log in to e-services and give digital signatures. It supports more than 600 organisations, which include financial, healthcare, and various other private and public-sector e-services. SK's services in Estonia have more than 700 000 end users.

Key Initiatives:

- certification and time-stamping service;

- development of technology and applications for digital signatures

- validation services.

- certification service within electronic tachograph project in Denmark.

9.2.2 Netherlands

The Dutch Government is partnering up with industry and knowledge institutions to identify a set of national and international pilots[77] that can be launched in the short to medium term. The Dutch Blockchain Coalition agenda is a joint initiative of over 20 organisations active in the logistics, energy and financial sectors, as well as government and research institutes. The coalition considers blockchains to be a potential source of trust, well-being, welfare and security for citizens, society and companies. The aim of the coalition is to create the conditions for reliable and socially acceptable blockchain applications, with the Netherlands aiming to become an international leader in the application of blockchain technology.

Several pilot initiatives are approaching the prototype phase and are expected to be operational within several years[78]. A first set of pilots was concluded in November 2016 and an action plan presented in April 2017[79]. In September 2017, international pilots will be launched. At the time of writing this study, the coalition is moving from research mode to actually building small pilots.

Although the Dutch government favours a vision for a 'blockchain-based government' as promoted by Estonia, the UK and Dubai, its action plan indicates that public blockchains and open standards may be more in line with the emerging national blockchain strategy than the Estonian model that promotes private blockchains and reliance on or close collaboration with private organisations. Specifically, the Dutch Coalition identifies the need to establish rules and standards for blockchain code that is created with government funding and recommends that this code should be completely open source.

---

(76) See https://sk.ee

(77) See www.blockchainpilots.nl/home-eng and www.dutchdigitaldelta.nl/en/Blockchain

(78) See https://docs.wixstatic.com/ugd/df1122_3de6de424d3b4f618af9e768e12d0ca0.pdf

(79) See http://www.the-blockchain.com/2017/04/14/dutch-national-blockchain-coalition-presents-action-agenda/

There is a clear direction that vendor lock-ins are to be avoided in any form: this extends to service contracts and apps built on top of open source code. This also requires for the public service to make open, transparent and honest arrangements with all suppliers. Again, the Coalition favours partnerships of the public sector with 'innovative companies' that are not necessarily 'large IT companies and consultancy firms'. TNO, a research institute in the Netherlands, is one of the key partners influencing national strategy on Blockchain[80]. Delft University[81], with its IMS, has a research lab on blockchain, primarily working on blockchain research areas that engage with human capital, fintech and cryptocurrencies. The Coalition is planning to set up a Blockchain Lab in collaboration with the ICTU (an IT Foundation that works for the Dutch government). Such a lab would enable the blockchain team and governmental organisations to quickly transform use cases into working prototypes in a secure and trusted environment. There is a clear preference for starting small: invest in knowledge and small experiments as a means of creating the first building blocks of sustainable blockchain projects.

Government is obliged to decide on the future of blockchain regulation within the context of a) Proof of Concept and b) Proof of Technology. The issue of standardisation needs to be addressed, particularly within the framework of ISO/TC 307 Blockchain and distributed ledger technologies[82], where the Netherlands is part of 20 participating members.

Like the majority of EU Member States, the Netherlands is likely to welcome a clear EU policy on open standards for blockchain in education. Dutch universities are currently working on stand-alone research projects that explore standardisation processes over the public blockchain: the estimate at the time of writing this report is that in the Netherlands there are some 100 projects involving 180 people from various organisations working on research projects and dissertations: these are likely to be primarily focused on human capital projects but there are also credentialing, diploma and regulation research projects in the pipeline.

---

[80] https://www.tno.nl/en

[81] See http://www.blockchain-lab.org/

[82] See https://www.iso.org/committee/6266604.html

10 Challenges to uptake of Blockchain in education

There are several challenges to the uptake of the blockchain in the education sector, in addition to the issues already identified in this study and necessarily associated with an early-stage technology.

10.1 Standardisation

Defining standards too early in the evolution of a technology lifecycle could be detrimental, as competition for innovation and commoditisation could produce counterproductive practices and alliances that fragment the market. When competing, the better standard may not win. If organisations move too early, potentially better alternatives could be stifled, and if they move too late the costs of switching to the standard will be higher for existing users.

(Hanson et al., 2017)

"The most important work that lies ahead is not technical. Much has to do with institutions and governance. It will require a concerted effort to ensure that the standards for digital credentialing systems are open and that they take into account the needs of all involved — learners, educational institutions, employers, and governments — and don't prioritise the interests of some organisations over others. This is the time to experiment, to collaborate, and to share experiences to realise the full potential of building a new ecosystem of digital credentials".

(Schmidt, 2017)

10.1.1 What is a Standard?

A standard, is an agreed way to do something.

While any person may claim to create a standard, **not all standards are created equal**, since they require the development of consensus and of clear instructions.

Within the standardisation community, the most respected forms of standards are those developed by organisations such as ISO, CEN and the IEEC, in accordance with the principles outlined by the World Trade Organisation's Technical Barriers to Trade Committee (WTO/TBT) (ISO, 2010):

— transparency;

— openness;

— impartiality and consensus;

— effectiveness and relevance;

— coherence;

— addressing the concerns of developing countries.

Other international standards, are generally referred to as private international standards, and may be developed by NGOs, networks and/or companies.

10.1.2 Decentralised Standardisation through Blockchain Technology

As explained in section 6.2.1, a blockchain network is constituted by a set of nodes all running the same blockchain software. Encoded within this software are the rules of the network – who can write to the blockchain, how consensus is formed, the structure of the data, and any other rules the network sees fit. Thus, by running the software the network effectively creates a standard for trading the assets for which that particular blockchain was designed – consensus and standardisation within the network is assured, since any changes to the software need to be approved by the whole network, otherwise it splits in two (known in technical circles as a 'fork'.

This method of standardisation is so effective, that it has led many people to propose a concept of Decentralised Autonomous Organisations, whereby formal governance rules contained in corporate bylaws or imposed by law are programmed into a blockchain network, to ensure consensus occurs only according to those rules (Jentzsch, 2016).

10.1.3 Current initiatives for blockchain standardisation

While blockchain technology effectively enforces a set of technical standards on the users of a specific blockchain through its consensus mechanism, it does not mean that blockchain technology is standardised.

Thus, for example, most vendors using blockhchaints to issue certificates only store the hash of the certificate on the blockchain. Thus, the issue, sharing and verification processes all occur off-chain using vendor-developed software – none of which is currently standardised. Thus, it is possible to have a situation where tens of companies and organisations are issuing certificates on the same blockchain, but where each certificate would require different software and vendor agreements to be able to utilise.

Secondly, different groups may create different blockchains to trade the same asset amongst themselves, without ensuring interoperability between the different chains.

The W3C Consortium, which have been responsible for creating most of the (private) standards that underpin the Internet, have set up a verified claims working group to tackle standardisation issues around the issue of educational certificates and self-sovereign identities, and also a blockchain community group which discusses issues around creating a message format for blockchains.

ISO has also launched Technical Committee 307 to deal with Blockchains and Distributed Ledgers. Currently it has formed 5 working groups to deal with the following issues:

* reference architecture, taxonomy and ontology;
* use cases;
* security and privacy;
* identity;
* smart contracts.

10.1.4 Standardisation of Educational Records

In Europe, within the educational sphere, there is little standardisation of student records. Currently, education which is received at tertiary level has been tokenized and is represented by credits of learning using one of two credit standards, namely ECTS or ECVET. However, metadata standards do not exist for either credit standard.

All degrees issued within the European Higher Education Area are accompanied by a diploma supplement that describe the degree in standard terms. However, again there are no standards for computer-readable data for diploma supplements. The EU has only just published a feasibility study on the digitalisation of the diploma supplement at European level (Pocius, D., et al 2017) which makes no reference whatsoever to the opportunities afforded by blockchain.

For all other levels of education not covered by ECTS or ECVET, there is no standardisation of systems, documentation or system information. While blockchain's ability to integrate disparate data sources offers significant opportunities for development in this area, **the lack of standardisation will limit the impact of any implementations unless addressed**.

10.2 Resource Usage and Ensuing Complexity

Most blockchains have extremely high storage costs, since the entire blockchain needs to be stored on each node in the network, and also extremely high energy usage, due to the computational power required to process the cryptography. To give an example 1TB of storage on the Ethereum blockchain currently costs around €6000.00[83] compared to approximately €60.00 for a hard-drive of the same size. In terms of energy costs, it is estimated that a single bitcoin transaction currently uses 160 kwH of electricity, which is approximately enough to power a US household for 6 days. In fact, the Bitcoin network is currently estimated to use around 0.1% of the world's electricity to process 4 transactions per second. If this were to be scaled linearly to thousands of transactions per second, it would clearly result in a massive increase in global electricity consumption, and likely an environmental disaster.

Due to this, any transfer of assets on a blockchain increasingly includes both on-chain and off-chain data. As explained in previous chapters, rather than storing assets or records directly on a blockchain, only the hash of those records is stored to save space. However, even this is not sufficient to meet blockchain technology's energy and storage constraints. More nodes in a blockchain means higher energy and storage costs, but also higher security. Thus, many applications for the blockchain now only store the hash of the entirety of their transaction data on a blockchain. A common technique for doing this kind of storage is by using a cryptographic technique called a Merkle tree, which simply put is a hash of other hashes:

Figure 22: Typical Data Structure for Blockchain storage using Merkle Trees
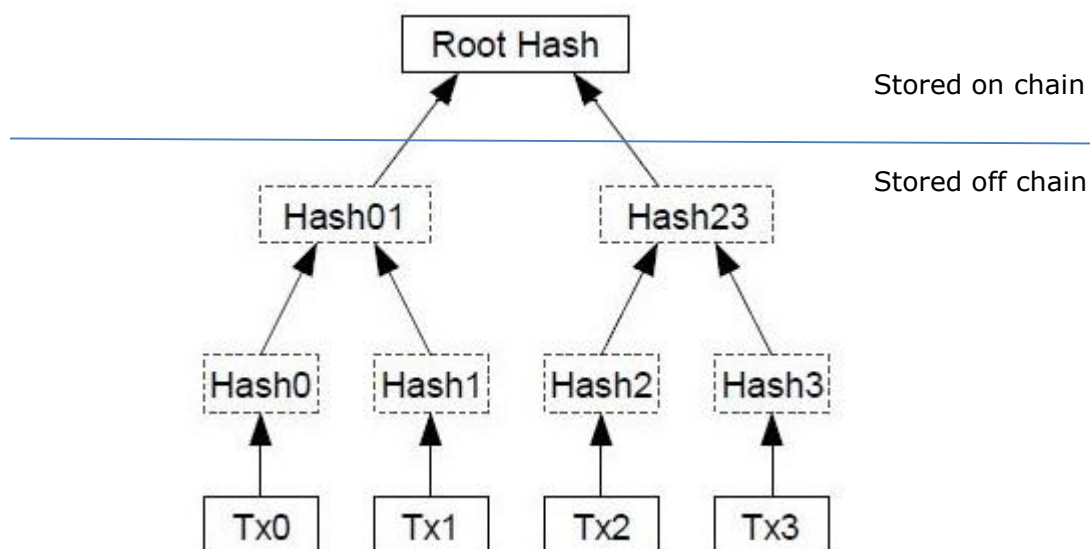
Under such systems, the actual data represented by the hashes, be it certificates, signatures, personal data, contracts, etc. still needs to be stored somewhere off-chain.

---

[83] Assuming a gas price of 20 gwei and an Ethereum price of €300.

Numerous different implementations of how to store this data are in operation, including systems for storage on:

— users' personal devices (linked to a self-sovereign identity);

— centralised servers operated by third parties;

— other (smaller and more specialised) blockchains known as side chains;

— distributed peer to peer networks[84].

10.3 New Dependencies on Third-Parties

While blockchain technology eliminates the ability of any one party to control a ledger, and while public blockchains theoretically allow any person to join the network and participate directly in creating and verifying entries on the chain, in reality there are significant technical, knowledge and resource barriers to entry, which means that in practice people only interact with blockchains through companies which specialize in blockchain technology.

Types of services, which already number in the hundreds (and possibly thousands), which have been built on top blockchain technology include:

— digital wallets, which allow you to hold assets and/or records which have been issued on the blockchain;

— trading platforms which facilitate the exchange of assets on a blockchain;

— issuance platforms which allow for the creation of assets and records on a blockchain;

— entirely new blockchains;

— token creators, which create ways to trade new asset classes on top of already existing blockchain platforms;

— tool providers which build interfaces for interacting with the blockchain;

— storage solution providers which provide ways to deal with off-chain data.

Due to the limitations explained in 10.2, usually all these services only store a fraction of their code and data on the blockchain itself, thus effectively inserting themselves as intermediaries between the user and the data, and re-introducing all the disadvantages of dependence upon a central authority discussed in this report.

Should the organisations in question adopt best open-source and open-data practices, then it is still possible for them to operate only as a facilitator and not as a gatekeeper to accessing blockchain based services. However, the complexity of the architectures and the multiplicity of parties involved means that it is unrealistic for a user to be able to make informed decisions about which operators are truly open.

In the case of traditional centralised ledgers such as those run by banks, regulatory and standardisation bodies such as financial regulators create technology standards and only allow the organisations to operate if they meet stringent criteria.

There is currently no standard, government body or third-party organisation which could assess these services to make determinations on whether their claims are true, how they actually handle data on the technical solidity of their blockchain implementations.

This situation of near-unlimited opportunities for developing applications, coupled with the infancy of regulation and opportunities for abuse often lead the blockchain ecosystem to be described as the *Wild West.*

---

[84] An example of such a network is IPFS (Interplanetary File System). More information is available here: (https://ipfs.io)

11 Usage Scenarios for the use of the Blockchain in Education

11.1 When to use a Blockchain

Given the costs of using blockchain technology discussed in section 10.2, it is clear that, despite the hype surrounding the technology, from a technical standpoint it can only be applied to specific use cases. Therefore, an application should only use blockchain technology if it meets a specific set of criteria (Greenspan, 2015), namely the need for:

— **a database formatted as a ledger**, i.e. a list of timestamped transactions listing what was transacted, from whom and to who;

— **multiple writers**, i.e. different persons (usually in different physical locations) need to write to the database;

— **transacting in the absence of trust,** i.e. each of the writers to the database would not be willing to allow anyone else to edit their entries;

— **disintermediation,** i.e. the various writers do not wish to grant control over the database to a centralised authority, so that it could manage it;

— **transaction interaction,** i.e. there is some interdependency between the transactions. Thus, e.g. in the case of cryptocurrency if person A transfers 1 unit to person C, and person B also transfers 1 unit to person C, determining C's balance requires checking both transactions;

— **a clear set of rules,** i.e. transactions are only allowed if they meet precise conditions, which can be independently and automatically verified;

— **a store of value,** i.e. entries on a blockchain should represent assets or records which have real-world value.

11.2 What kind of blockchain to use

Broadly speaking, there are three different types of blockchain solutions which may be applied, each of which has significant differences in architecture and governance:

— **Public** blockchains are open for anyone to download, run and transact on. Solutions built using this rely on public consensus to reach decisions, and typically may run on up to millions of machines. Thus, public blockchains produce maximum immutability, decentralisation and transparency – however, this is at the cost of high inefficiency in the form of high storage costs, high electricity usage, as well as low transaction speed and volume.

— **Private** blockchains are by invitation only, and operate according to a set of rules put in place by those inviting. Such a blockchain may be used by a small number of parties to trade exclusively amongst themselves, or it may be open to anyone to transact upon, but only allow a select group of users to change the rules and/or to validate transactions. Effectively, a private blockchain reduces the immutability, and transparency of the chain, and is highly centralised (while still offering these advantages more than a traditional database) – however, the reduced number of parties involved means that the chain itself tends to be much smaller and specialised – leading to high efficiency, high transaction volume and speed, and consequently lower costs and resources usage

— **Consortium** blockchains are effectively a hybrid of the two models. A consortium blockchain is a private blockchain, i.e. by invitation only, but all persons invited have equitable voting rights, with decisions taken by consensus. Thus, from a governance perspective it keeps the decentralised nature of a public blockchain. In terms of immutability, transparency and resource usage it provides a midway between the features of private and public chains.

11.3 Usage scenarios for Blockchain in Education

This section tabulates eight scenarios for the application of the Blockchain in an education context, based on the current state of technology development.

Scenario 1: Using Blockchains to permanently secure certificates

Prospect: Short-Term / Present

Current State: Educational organisations currently issue certificates either in paper format or electronic format using public key infrastructures. These certificates are time-intensive and expensive to issue, maintain and verify. Public key infrastructures require using a certification authority as an intermediary to issue the certificates, creating a dependency which may be abused. Current verification records are also liable to be destroyed in the case of natural disasters or wars.

Description: In this scenario, educational organisations that issue digital certifications will use a public Blockchain to store the digital signatures associated with those digital certifications. Unique signed digital certifications are given directly to the users. Thus, verification[85] of the authenticity of a certificate only requires comparison with the digital signature/hash stored on the blockchain.

Advantages over Current state: The proofs of the certificates will be stored completely, securely and permanently on a blockchain. Thus, even if the institutions that issued the certificates were to close down, or if the entire system of education collapses (as, for instance, happened in Syria), those certificates are still verifiable against the records stored in a blockchain. Furthermore, once institutions issue a certificate, they do not need to spend any further resources to confirm the validity of that certificate to third parties, since these will be able to verify the certificates directly themselves on a blockchain.

Pre-requisites: The only pre-requisite necessary to enable this scenario is software that will allow the issuing of certificates with signatures posted to a blockchain, as well as verification software to confirm those certificates. Blockcerts is an already-existing open source solution that enables this.

Furthermore, since the certificates themselves are not stored on the Blockchain, both the institutions and users would need a secure and fail-safe system for storing these certificates for the long-term.

Scenario 2 : Using blockchains to verify multi-step accreditation

Prospect: Short-Term

Current State: Currently, there are literally hundreds of accreditation pathways in Europe. In terms of public accreditation, each country has a different system for accrediting organisations (and the agencies that accredit them), and often different systems for different kinds of organisations. In addition, multiple important accreditations are run by non-governmental organisations and by the private sector.

Employers and educational organisations recognising credentials often need to verify not only the issuer of the credential, but also the quality of the institution issuing the credential. In such case, certifications issued by government or private certifying bodies hold significant weight in determining the quality of the qualification.

To verify whether a certificate is issued by a legitimate institution, an individual will need to check:

---

[85] Note that the only thing that is verified is that an identifiable institution *has indeed issued a specific, identifiable certificate*. No claims whatsoever are made as to the quality of the education represented by such a certificate.

— with the institution to verify if it really issued the certificate;

— the quality of the accreditations that the institution claims to have;

— with the accrediting bodies if they really issued the certificate to the institution;

— by which authority the accrediting bodies issue the accreditation;

— with the authority if they really authorized the accrediting bodies to operate.

This is an extremely time-consuming and technical process which requires experts in accreditation to manage. The ENIC/NARIC network is an entire network of agencies with staff and offices in every EU member state aimed at facilitating this for higher education qualifications.

Description: Under this scenario, not only would educational organisations use digital certificates in the manner described under Scenario 1, but organisations which accredit them would also put their own digital signatures onto the Blockchain. This would allow for verification not only that Student X had indeed received a certificate from Institution Y, but also that Institution Y was certified by Accreditation Organisation Z.

Such a system could be used to ensure that the educational organisation issuing the certification was licenced by government, or to verify that the educational organisation had specific quality-certifications, e.g. that an MBA-provider was actually certified with the EQUIS accreditation.

Advantages: Using a blockchain, rather than researching these connections, institutions needing to check the 'pedigree' of a degree could easily do so with a single click. A fully-automated process would then be able to visualise the accreditation chain and verify that certificates had indeed been issued, and (critically) that they were still valid for each step of the chain.

Pre-requisites: There are a number of different ways in which such a scenario could be brought into being, all of which assume that the accrediting organisations publish their accrediting certificates (or the signatures of those certificates) on a blockchain, namely:

— the accrediting organisations could create and publish 'verifiers' on their own websites, which would allow anyone to upload their certificate and check whether it was genuinely issued by an accredited organisation;

— the accrediting organisations could publish the issued certificates themselves into a public registry. This would allow for any third-party to verify whether: (a) a certificate was issued by an HEI to a student; (b) whether that HEI has a certificate in in the public registry, and (c) whether all those certificates are genuine. This implementation requires that an independent trusted party would create the public registry;

— institutions could create self-sovereign identities to store identity-data – in this case the accreditations they had received. Thus, a third-party verifier would check the validity of the student-certificate against a blockchain, and check the pedigree of the institution based on the published elements of its federated identity.

Scenario 3: Using a blockchain for automatic recognition and transfer of credits

Prospect: Medium Term

Current State: Currently there is no meta-data standard to describe ECTS or EQAVET, no standard database for storing ECTS, and no standardised way to automatically store ECTS or EQAVET. The European Commission has commissioned a feasibility study on

digitizing the diploma supplement, while a few EU funded projects have looked at the feasibility of ICT-enabled transfer of credits[86].

Description: Under this scenario, educational organisations that use credits to award learning (such as Higher Education Institutions using ECTS, or vocational institutions using ECVET), would award and transfer credits on a custom-Blockchain built specifically for those credits.

Advantages: The primary advantage of this is that not only would the proofs of the validity of a certificate be stored on a blockchain, but the certificate itself would be stored on a blockchain – meaning that the certificate itself becomes permanent and immutable. Furthermore, it means that no third parties would be needed to create 'backpacks' and store the certificates – students/graduates would only need to give an HEI or employer access to their profile, and their entire educational history in terms of those credits would be instantly visible and verifiable.

Furthermore, credit systems are often used for transfer and accumulation. Transfer means that a credit received in one institution is recognised as contributing towards a qualification in a second institution, while accumulation means that on receiving a certain number of credits students can be awarded with a qualification such as a degree.

Currently, credit transfer depends on institutions to negotiate agreements to recognise each other's credits subject to certain conditions – but students often report that these agreements are not recognised. Using a blockchain, these agreements could be written as smart-contracts whereby upon fulfilment of the conditions of the contract, the credits would automatically be transferred. The same goes for accumulation – a smart-contract could be programmed to automatically issue a degree upon the achievement of certain credit-targets, according to the policy of the institution – ensuring that the transfer and accumulation rules are applied equitably across all cases.

Pre-Requisites: This scenario requires (a) that a standard for credits exists, describing specifically what a credit consists of and how it is awarded, (b) the creation of a custom-blockchain designed specifically to store this information together with software to interact with the blockchain and (c) a critical mass of institutions participating to ensure immutability of the transactions on the Blockchain.

For Higher and Vocational institutions in Europe a standard for credits already exists in terms of ECTS and ECVET respectively. This scenario could be deployed in different ways:

1. The 'credit Blockchain' could be deployed by any entity (such as a government or leading institution) with sufficient reputation to ensure its uptake, as a public, *permissionless* blockchain. This would allow any institution to offer credits on the blockchain. This could be then combined with systems of multi-accreditation as described in Scenario 2 to create additional levels of trust.

2. Institutions which already offer credits could launch a credit blockchain amongst themselves as a consortium blockchain. Additional institutions would only be given access to the blockchain if they met certain standards, thus ensuring that all credits issued on the blockchain were from institutions with a shared quality standard.

Finally, if smart-contracts were to be incorporated into the design of the system, software would need to be built to program these smart-contracts and upload them to the chain.

---

[86]   The Erasmus without paper project (http://erasmuswithoutpaper.eu) is attempting to influence the HEIs to exchange student information for mobility programmes fully in an electronic way by providing an evidence-based feasibility study with different use case scenarios and the practical solution to build connect all existing systems in one network.

Scenario 4: Using a blockchain as a lifelong learning passport

Prospect: Medium Term

Current State: Many different social networks, e-portfolio companies and 'backpack' providers already provide users with a way to record their achievements. However, except for Open Badges, none of these provide ways to verify the experience and credentials described and included within these systems – therefore these systems operate as a digital counterpart to a box full of paper certificates – deriving, little to no additional benefits or efficiencies from the process of digitisation.

Description: Under this scenario, learners would store their own evidence of learning received from any source – whether formal, non-formal or informal – and when shared, a blockchain would be used for instant verification of the authenticity of these documents.

Advantages: The advantage of this scenario is effectively that every student would have an automatically verifiable CV containing a record and evidence of all learning and employment they had received – significantly reducing CV fraud, as well as, depending on the form of implementation, significantly reducing workload for organisations and individuals that have an interest in verifying that CV.

Pre-Requisites: From a technical standpoint, the easiest way to implement this is through the creation of a verified digital federated identity. A blockchain can be created whereby people upload their claims, which are then verified by other nodes on the blockchain (through checking the facts of the claim). Once a certain number of users confirm the claim as true (and depending on the reputation of the users verifying the claim), the claim receives a trust score which is a score of its verifiability. There are already companies testing this kind of software and services, as described in section 7.3.

If a meta-data standard is used, to described different types of claims (e.g. NGO experience, employment, training courses), then this would be tied into recruitment software and systems to allow institution to automatically verify whether persons have the required skills for various positions.

Scenario 5: Blockchain for tracking intellectual property and rewarding use and re-use of that property

Prospect: Medium Term

Current State: Currently, tracking intellectual property is a costly endeavour run by specialized organisations, usually when there is a significant business case to do so. Thus, collecting agencies track intellectual property usage of music and video so as to collect royalties, while journal companies track citations of articles, since this data is valuable due to its use for academic promotion. Due to the complexity of tracking intellectual property, it is hard for people who are self-publishing to track and commoditise the reuse of their intellectual property. Thus, for example reuse of open educational resources is generally not tracked, or tracked with extremely simple metrics with limited use.

Description: Under this scenario, educators would use a blockchain to announce the publication of open educational resources, and record the references they used. This would allow for notarization of the date of publication for copyright reasons, as well as allow the level of re-use of any specific resource to be tracked.

In a closed intellectual property scenario, the same system could be used to track use and reuse of intellectual property created by an institution. This could also be coupled to a smart-contract that would distribute payment to the authors of the material based on the quantity of use of their intellectual property.

Advantages: From a structural standpoint, this scenario is very similar to the existing system which is used to track citations for journal articles. However, tracking citations of journal articles has up until now required intermediaries which have put limits on the use of those articles in return for those services, often in the form of high costs for access,

and restrictions on the sharing and use of the intellectual property within them. This has limited uptake of the model for open educational resources.

Using a blockchain, we eliminate the intermediary, thus allowing anyone to publish openly, and accurately keep track of re-use without putting limitations on the source material.

Were such a system introduced, it would allow for teachers to be rewarded based on the level of actual use and reuse of their teaching materials, similar to how they are rewarded based on citations to research papers. By serving as a proxy for quality materials, it would also allow students and institutions to make metrics based decisions on which teaching materials to use.

Pre-Requisites: Under this scenario, a blockchain would be used to (a) announce the publication of their resources and link to those resources, and (b) to announce which other resources they used in creating the material. Coins would be awarded to educators in line with the level of reuse of their respective resources.

In an open-scenario, coins would not be spendable – and would be used to determine the prominence of an author. In a closed-scenario, coins would have monetary value and would result in monetary compensation.

A more advanced implementation might automatically scan resources to identify what percentage of other resources were re-used and automatically award accordingly.

Scenario 6: Receiving payments from students via blockchains

Prospect: Short Term / present

Current State: At the moment, students pay for their studies using a specified currency. Especially for cross-border studies, and also in response to legislation, many organisations only accept payment made through electronic means.

Description: Under this scenario, students would provide payments for studies via blockchain-based cryptocurrencies.

Advantages: Students do not always have access to bank accounts or to credit cards, depending on the country they are from, their age, employment status etc. This can sometimes serve as an additional barrier to access education. Cryptocurrency based payments would allow this issue to be solved.

Pre-Requisites: The only pre-requisite for this scenario is for the students and the institution to have ways of sending and receiving cryptocurrencies, i.e. a wallet for the cryptocurrency.

Scenario 7: Providing student funding via blockchains, in terms of vouchers

Prospect: Long-Term

Current State: Many countries (as well as private sponsors) fund tuition by giving students 'vouchers' to be 'spent' at any educational organisation or at a list of pre-approved educational organisations. Such voucher systems are an increasingly popular method for funding education, since they provide free education to students, but still allow institutions to compete amongst themselves to provide the best possible offer to students Depending on the funding model, these vouchers may be subject to conditions such as requiring the student to graduate. Tracking compliance with these conditions requires a large administration. Also, changes in policies might mean that promised funding is not always allocated to students in line with the originally agreed rules.

Description: Under this scenario, government (or sponsor) funding for tuition would be given to students as 'vouchers' on a Blockchain. The vouchers could be programmed to release tranches of funding to either the student or the educational organisation, based on certain performance criteria such as grades.

Advantages: By using blockchain based smart contracts, funders can provide the entirety of the funding up-front (providing security for the students and institutions), but only release it when certain criteria are met. This process can also happening automatically without the need for any intermediaries, vastly decreasing the bureaucracy required to manage such a system.

Such a system could also be linked to student loans, with levels and periods of repayment being linked to grade-performance, wages or any other indicator.

Pre-Requisites: From the Blockchain perspective, the Ethereum Blockchain already supports such a capability. To use this system, one would only require (a) software to 'build' the smart contracts easily and upload them to the Blockchain, and (b) the data sources (such as a database of student grades) which would be required for the smart-contracts to know whether the conditions of the contract have been fulfilled.

Scenario 8: Using Verified Sovereign Identities for Student Identification within Educational Organisations

Prospect: Mid-Term

Current State: Within larger organisations, students need to regularly identify themselves with different parts of the organisation. In such cases, either each part of the organisation will collect the student data for itself, or the organisation will use single-sign-on, whereby one shared copy of the student data is used by all parties within the organisation. Under both these models, tens if not hundreds of people might have access to a student's personal information. Keeping that data safe requires managing access rights for all those people, and ensuring that their devices are also secure and hack-proof – a mammoth undertaking.

Description: Here, after students would share their personal data with the admissions office within an educational organisation, they would receive certification of their identity from the same office. Using biometric identification on a smartphone, coupled with this certificate, students would be able to identify themselves to any other part of the organisation that required identifying them, such as the library, gymnasium, canteen, student dormitories, student associations, etc. Each of these services would be able to identify the student without the need to ask for or store any personal data again.

Advantages: By using verified sovereign self-identities, only the persons responsible for verifying the student's identity in the first instance require access to the data. Other than that, the only person who holds the data is the student themselves. This means that the organisation no longer needs to manage the complex systems for access rights, and only needs to secure the device or network where the verifications initial verification is taking place. This would save significant resources spent in hardening the network against data-breaches, staff training on data-protection and in managing access rights.

Additionally, persons interacting with the student within the organisation do not need to take on the responsibility of keeping sensitive data private, since they will not need to know it in the first place.

Pre-Requisites: Several companies are currently launching sovereign self-identity solutions that could be applied to this use-case. Currently, these would require institutions to undertaken significant technical work to tie these systems into their current student-information systems. Widespread adoption is likely to occur when existing student information system vendors adopt sovereign self-identities into their architectures.

12 Conclusions and Recommendations

This section tabulates a set of Conclusions and Recommendations based on the desk research, interviews and use case studies at the core of this study.

12.1 Conclusions

This section tabulates 13 key conclusions from the empirical data reviewed during the course of this study.

CONCLUSIONS	
C1. Blockchain applications for education are still in their infancy	— Currently, the only implementations of blockchain technology for education are in pilot stages. As demonstrated by this report, several organisations are in the initial stages of pilot-testing award of certificates using a blockchain, while others are accepting blockchain-based cryptocurrency payments.
	— There continues to be a widening gap between the claims being made about potential distributed ledger technology applications and the actual roll-out of such applications. Anecdotal evidence suggests that a growing number of organisations are 'looking down the wrong end of the telescope' at blockchain technology: instead of bringing their problems to the table and assessing whether blockchain technology might provide solutions, they are bringing blockchain technology to the table and looking for problems to which the technology might be applied.
	— While the majority of attention is currently directed at Fintech as opposed to education, trust in blockchain technology will migrate from finance to education. Large players will eventually shift their attention to education. The implications and applications of trying to outsource trust to technology cannot be accurately forecast, and may well entail complications and side-effects that we can't currently envisage (Collins, 2017).
	— Industry insiders are talking in three- to five-year increments but blockchain technology implementation may well be a decades-long experiment. The indicators are that most industries and their business models will be touched by this technology, in the same way as they were impacted and disrupted by the Internet.
C2. The full benefits of blockchain technology are only achieved through open implementations	— 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.
	— Much will depend on the value that education institutions, governments or even learners (the target users) will attribute to the basic tenets of 'openness', 'vendor independence' and 'learner empowerment' - particularly

	those related to the value learners will attribute to owning their own digital certificates, as opposed to being perpetually locked in with (albeit trusted) institutions or vendors. — Although in principle these are very powerful arguments, it is too early to determine whether these are more compelling for target users than, say, proprietary solutions being developed by global brands.
C3. Blockchain may disrupt the market in student information systems	— Blockchain technology has significant use cases beyond crypto currencies, whose use cases are beginning to enter the mainstream. This could happen over the next 12 months. — Blockchain-based ledgers have the potential to disrupt the key technology that underpins an industry currently worth $2.7 billion[87], and as such will likely disrupt the market as a whole. We are likely to see tens to low-hundreds of established companies and start-ups seeking to secure early-mover advantage of this space. — Since significant network effects will be achieved through scale, it is likely that within the next few years a handful of powerful technology vendors will gain a foothold over the entire industry.
C4. Vested interests have an interest in locking down blockchain technology and creating standards based around partial implementations	— As outlined in section 4.2, implementation of the blockchain offers a significant social value proposition. These benefits result directly from the removal of key ledgers from the control of single authorities. — Organisations and companies that have built (or are planning to build) solutions and business models around controlling these ledgers, have a vested interest in resisting implementation. Since they cannot roll back the invention of blockchain technology, many of them are creating 'partial' and hybrid implementations which allow them to retain control of the ledgers, while still offering other advantages of the technology such as cost savings. — Therefore, despite the hype, the mention of blockchain technology does not automatically imply a universal trust protocol - it often implies exactly the opposite. To transact anything of value other than tokenisable assets via a blockchain requires additional layers of agents, third parties and auditors – things that just don't square with the trust-free architecture. — Within education, this is being in seen in the first instance by a flurry of companies offering to issue certificates linked to a blockchain, but only allowing access to the content of those certificates through proprietary, closed platforms – effectively using the promise of an open system as a foil to creating a closed system.

---

[87] According to Technavio (2017), the Student Information System market is likely to grow to $5.7 billion by 2021.

C5. Public private partnerships are necessary to fully exploit blockchain	— The interests of the market and the public are not always in alignment when it comes to deployment and application of blockchain technologies in education. Such a situation is usually a textbook case for market regulation. — On the other hand, due to the fact that blockchain technology is so new, and that the potential of the technology is just being discovered, governments should not at the moment 'pick winners' or lock down the technology with excessive regulation. — With this in mind, we conclude that the only possible model to achieve the full potential of the blockchain is through a balanced, strategic public private partnership.
C6. Blockchain technology has the potential to accelerate the end of a paper-based system for certificates	— Until now, 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.
C7. Blockchain technology removes the need for educational organisations to validate credentials	— 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 courses[88]. 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.
C8. Blockchain has the potential to release a wave of innovation around learners' data	— Learners' data is a critical component of many applications including human resource management systems, e-portfolios and professional social networks. Blockchain technology allows all these systems to automatically validate certificates from any issuer in any (metadata) format. — This ability to store verified claims rather than mere claims, should significantly enhance the usefulness of such systems to their various stakeholders. — We may well imagine applications that: automatically verify CVs and shortlist candidates with appropriate qualifications; and other applications that would automatically place employees into a higher-earnings bracket based on evidence of completed training and professional networks that would use verified professional

---

[88] Institutions would still have a role in re-issuing certificates if they were lost by the user, or revoking them, e.g. if they were late found to have been obtained by cheating.

	certificates as the requirement for subscription. Countless other ideas are likely to be imagined by start-ups and established companies working in the field.
C9.Self-Sovereign Identities have the potential to significantly reduce educational organisations' data management costs	— European law imposes significant obligations on organisations which are custodians of personal data – obliging them to control who has access to it within an organisation and to ensure its safe storage within the organisation. The more people have access to the data, the more complex the management, the higher the costs and the higher the risks of a data breach or abuse.
	— Self-sovereign identities effectively create a secure identity card which can be held by a student, and which can be biometrically linked to them – allowing the student to identify themselves without actually handing over any data, and without the need to cross data with a database held by the institution. The institution will be able to identify the student without actually holding and retaining their data.
	— This significantly reduces the administrative overhead, as well as reducing the potential 'footprint' for a data breach or abuse.
C10. Blockchain technology enables much more sophisticated systems for reliably tracking usage of intellectual property	— 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.
	— Blockchain technology also allows for detailed and incremental tracking of who has used intellectual property, where and how, and for these to be associated with credit – either in the form of payment or in the form of academic credit. Such systems for intellectual property could, for example, serve as the basis of future journals, or even as the basis for tracking the production and re-use of open educational resources. As such, they would be able to significantly incentivise the opening up of education and educational resources.
C11. Educational networks can automate and standardise many of their functions through decentralised autonomous	— A Decentralised Autonomous Organisation (DAO) is effectively a community, with its resources organised according to rules agreed in advance and set out in its code (Allen & Overy, 2016). As such, communities which exist for the purpose of creating and transferring those resources against set rules, are ideal candidates for being reimagined as DAOs.
	— Within the European education sector, there are several examples of such communities. Quality Assurance in

networks	Higher Education is run by a community of stakeholders, that work together to create standards for accreditation of institutions, and award accreditation to those institutions that meet the criteria. ECTS, having no centralised registration body, is effectively a network of institutions that agree to award credit based on set rules, and then to allow the transfer of credit between institutions.
	— The application of DAOs may: (a) automatically ensure that such awarding of credit or certification always happens according to the same set of criteria in every implementation; (b) ensure that transfer and/or use of these certificates always occurs in accordance with the rules; (c) create a single unified database of awarded certificates; (d) share control of the system between members of the network, with no party having centralised control.
C12. Regulation and Standardisation may determine the extent and speed of progress	— Widespread adoption of any records-based system requires standards, agreements and regulatory frameworks as well as systems for interoperability.
	— While various forms of student qualification data, particularly in tertiary education, have been somewhat harmonised and standardised across Europe over the years, there are reams of other data which still have no common format or standard. At lower levels of education, school leaving certificates have yet to be harmonised or standardised.
	— Furthermore, the tools that do exist, such as the diploma supplement, ECTS and Erasmus agreements, have not been designed with digital records in minds – none of these essential tools follows a digital data format or digital metadata standard.
	— With its ability to store different kinds of records, as well as its ability to automatically establish consensus between parties without a central authority, blockchain can simplify the creation of such standards, but cannot be deployed in a truly pan-European sense without them.
	— There are trade-offs between open and closed standards, but data portability operability is essential. If we want people to be able to take and verify their data anywhere in the world, by any system, open standards are a must.
C13. People are unaware on the social advantages and potential of blockchain technology	— 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.
	— However, educational organisations have little evidence available to prove that blockchain offers a significant value added, either to themselves or to their students. Understanding the potential of blockchain without

	examples of implementations to point to requires significant knowledge and specialisation.

12.2 Recommendations

This section tabulates 7 key recommendations on the basis of the empirical data reviewed during the course of this study. These recommendations are intended to serve as guidance for policy-makers seeking to improve educational processes and outcomes using blockchain, and are not high-level recommendations for the promotion of blockchain technology more generally.

	RECOMMENDATIONS
R1. Create and promote a label for 'open' educational records	— Should the EU wish to support the development of 'open' blockchain implementations, and enshrine the principles of a) Recipient Ownership; b) Vendor Independence; and c) Decentralised Verification, then these terms will need to be defined in terms of educational records. — We recommend that the EU bring together a group of experts in certification, blockchain technology as well as data protection to define criteria for an 'open records' label. — Once it is created, to promote the idea of open records, the EU, in conjunction with Member States could agree to only support and/or adopt technologies which are in compliance with such an open records label.
R2. Policy-makers should consider investigating and supporting the application of blockchain technology to specific educational use cases	— We recommend that the significant potential of the blockchain in areas such as the issuing of certificates, verification of accreditation pathways, lifelong learning passports, intellectual property management and data-management to mention a few be further investigated, and that the development of applications to address these use cases be supported and accelerated. — Since each of these use cases has different dependencies, and furthermore, since there are several technological pathways to addressing each use case - we strongly recommend that the EU fund and support competitive pilots for each use case, to allow optimum technological solutions to be readily-identified. — Such pilots should encourage the collaboration of private companies, startups, educational organisations and public authorities from several countries, using, for instance, an instrument such as Horizon 2020. The best ideas would then receive follow-up funding for mainstreaming, thus completing a full innovation pipeline. — These Scenarios are described in section 11.3
R3. Europe should urgently consider supporting the creation of digital meta-data standards for	— Meta-data standards support innovation in the use of data (Dawes, 2010). As such, any innovation based on educational records, including that of blockchain requires widely agreed standards for digital meta-data. — Standards need to be developed for identification of

	educational records	students, recording student accomplishment in formal and non-formal settings at different levels of education, for recording certification and accreditation of institutions and use and reuse of educational resources to mention such a few.
		— Digital meta-data standards should be developed through a multi-country multi-stakeholder approach to ensure that they address all (standards-related) technical barriers to trade.
		— The European Commission, together with Member States, should launch an urgent and major standardisation drive in this area, possibly in collaboration with CEN or ISO.
R4.	**Support stakeholder engagement with blockchain technology and decentralised autonomous organisations**	— Many of the most exciting potential implementations of blockchain technology revolve around its ability to allow for trusted transfers of certificates, credits, accreditations or other assets between parties in a network. Rather than 're-inventing the wheel', a key foundation of any blockchain strategy should involve initiatives to empower these networks to utilise blockchain technology to improve their transfers of such assets within the network using blockchain.
		— We recommend that the EU therefore creates a mechanism to support European University Federations (or federations of other educational organisations), that may enable them to investigate applications of blockchain to their activities, launch pilots and mainstream these activities within their networks. Such support might take the form of targeted operational funding for such networks.
		— We recommend that these activities be connected to those in R2.
R5.	**Support policy makers in understanding the implications of blockchain technology to various activities within education**	— Using blockchain to its fullest potential for education requires that policy-makers secure awareness that the emergence of the blockchain may have a significant impact on existing and planned activities and strategies. Specifically, policy-makers need to have access to the knowledge to define this aspect, so as to inform blockchain-first design thinking.
		— Doing this requires readily-accessible cross-domain knowledge.
		— We recommend that a consultative group be constituted, with the remit of providing regular advice to policymakers at EU and member-state levels as to the potential rewards of the technology for specific applications and help Member States balance the risks and manage expectations.
		— This will require the engagement and support of professionals and subject matter experts from the various disciplines, including specialist private sector organisations and industry insiders.

	—	Furthermore, we would suggest that such a group cover the spectrum of formal education, non-formal education as well as employment.
R6. Recognise self-sovereignty as a key digital competence	—	It is unrealistic to expect that data protection legislation that concentrates on putting the onus on data-handlers alone will be enough to prevent the abuse and mishandling of highly sensitive personal data.
	—	The concept of self-sovereignty, whereby users own their own data and share in the responsibility for its management, is a preferable model for data-management.
	—	For users to take advantage of self-sovereignty, they need to be made aware of the different options available for data management, and the advantages and trade-offs of each one. These principles should be integrated into education frameworks relating to digital competences for lifelong learning.
R7. Support further research in key areas likely to influence the readiness of the education sector to consider using blockchain technologies	—	Policy-makers and education institutions would benefit from further research in privacy implications, Intellectual Property (IP) management; and Digital identities.
	—	Guidelines, training, regulations and other mechanisms may be necessary, as part of a framework to ensure unacceptable privacy breaches from the misapplication of distributed ledgers are prevented. Conducting risk assessments on emerging use cases would provide an analysis of the current gaps needing to be filled.
	—	Research into effective platforms that manage the provenance and integrity of IP may unlock significant economic activity and new business models.
	—	Digital identity management presents the benefits of bolstering trust and certainty for economic activity, but poses challenges in terms of privacy and security. Research into policy and technology options as a result of new developments in blockchain technology would inform regulators and industry of ways to improve the related risks and rewards. **Significant digital infrastructure enabling digital identity management could be considered a European shared asset, and a competitive advantage for Europe.**

References

Abramovich, S., Schunn, C., & Higashi, R. M. (2013). Are badges useful in education? It depends upon the type of badge and expertise of learner. Educational Technology Research and Development, 61(2), 217-232.

Aglietti, A. (2017a). Proof-of-Knowledge: same Blockchain, different story. Available at: https://tail.agquadro.it/proof-of-knowledge-efc138f2a17c

Aglietti, A. (2017b). GROWBIT @ International Open Recognition Day. Available at: https://tail.agquadro.it/growbit-international-open-recognition-day-a39281072a6c

Allen & Overy (2016). Decentralised Autonomous Organisations. Available at: http://www.allenovery.com/SiteCollectionDocuments/Article%20Decentralised%20Autonomous%20Organisations.pdf

Allen, C. (2016). The Path to Self-Sovereign Identity. Available at: http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html

Au, S. Don't forget what self sovereign identity system uPort doesn't claim to do. Available at: https://decentralize.today/dont-forget-what-self-sovereign-identity-system-uport-doesn-t-claim-to-do-1f43ca228575

Batchu, Y. (2017). What did #Blockchain bring to the table? Available at: https://blog.unocoin.com/what-did-Blockchain-bring-to-the-table-ded18ef70432

Byrne, W.I. (2017). What is the Blockchain? Available at: https://medium.com/badge-chain/what-is-Blockchain-5e4498f05c20

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

Christensen, Clayton M. (2003). The innovator's solution: creating and sustaining successful growth. Harvard Business Press. ISBN 978-1-57851-852-4.

Clark Donald (2016). 10 ways blockchain could be used in education. OEB Insights. Available at: https://oeb-insights.com/10-ways-blockchain-could-be-used-in-education/

Coin Telegraph (2015). How Estonia Brought Blockchain Closer to Citizens: GovTech Case Studies. Available at: https://cointelegraph.com/news/how-estonia-brought-Blockchain-closer-to-citizens-govtech-case-studies

Collins, A. (2017). Four reasons to question the hype around Blockchain. Available at: https://www.weforum.org/agenda/2017/07/four-reasons-to-question-the-hype-around-Blockchain

Consensys (2015). uPort: The Wallet is the new browser. Available at: https://media.consensys.net/uport-the-wallet-is-the-new-browser-b133a83fe73

d'Artis, K., Ciaian, P. and Rajcaniova, M., (2016). The Digital Agenda of Virtual Currencies. Can Bitcoin Become a Global Currency? Available at: http://publications.jrc.ec.europa.eu/repository/bitstream/JRC97043/the%20digital%20agenda%20of%20virtual%20currencies_final.pdf

Dawes, Sharon S. "Stewardship and usefulness: Policy principles for information-based transparency." Government Information Quarterly 27.4 (2010): 377-383.

Deloitte UK (2016). Blockchain: Democratised Trust. Available at: http://www.mondaq.com/uk/x/506472/fin+tech/Blockchain+Democratised+Trust

Diacono, T., (2017a). Malta set for 'revolutionary' national Blockchain strategy. Available at:
http://www.maltatoday.com.mt/business/technology/76459/malta_set_for_revolutionary_national_Blockchain_strategy_#.WTfGvpB96Uk

Diacono, T., (2017b). Malta lays the ground for a blockchain revolution. Available at:

http://www.maltatoday.com.mt/business/business_news/79185/malta_lays_the_ground_for_a_blockchain_revolution#.WXiM2oiGOUk

Domingue, J., (2016). Blockchains and Higher Education. Available at: https://www.slideshare.net/johndomingue/the-potential-of-Blockchain-in-higher-education

Domingue, J. (2017). Education's new kid on the block. Available at: http://www.open.ac.uk/research/main/news/educations-new-kid-block

Ethereum Foundation (2017). Ethereum Homepage. Available at: https://www.ethereum.org/

European Commission (2016). eGovernment Benchmark 2016. A turning point for eGovernment development in Europe? Study carried out for the European Commission by Capgemini, IDC, Sogeti, and Politecnico di Milano.

Evans, J. (2017). Blockchains are the new Linux, not the new internet. Available at: https://techcrunch.com/2017/05/28/double-double-cryptocoin-bubble

Feldstein, M. (2017). A Flexible, Interoperable Digital Learning Platform: Are We There Yet? Available at: http://mfeldstein.com/flexible-interoperable-digital-learning-platform-yet

Findlay, C. (2015). Decentralised and inviolate: the blockchain and digital archives. Retrieved from https://rkroundtable.org/2015/01/23/decentralised-and-inviolate-the-blockchain-and-its-uses-for-digital-archives/

Forde, B. (2017), Using Blockchain to Keep Public Data Public, available at: https://hbr.org/2017/03/using-Blockchain-to-keep-public-data-public

Gibson, D., Ostashewski, N., Flintoff, K., Grant, S., & Knight, E. (2015). Digital badges in education. Education and Information Technologies, 20(2), 403-410.

Gideon, G. (2015). Avoiding the pointless Blockchain project. Available at: http://www.multichain.com/blog/2015/11/avoiding-pointless-Blockchain-project

Global Banking & Finance Review (2017). Blockchain Technology in Estonia: What happens at Governmental Level. Available at: https://www.globalbankingandfinance.com/Blockchain-technology-in-estonia-what-happens-at-governmental-level

Government of Canada (2011). Federating Identity Management in the Government of Canada: A Backgrounder. Available at: https://www.canada.ca/en/treasury-board-secretariat/services/accessinformation-privacy/security-identity-management/federating-identity-management-government-canadabackgrounder.html

Government Office for Science, UK (2016). Distributed Ledger Technology: beyond blockchain. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf

Greenspan, G. (2015). Avoiding the pointless blockchain project. Available at: https://www.multichain.com/blog/2015/11/avoiding-pointless-blockchain-project/

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

Hall, M. (2016). The Blockchain revolution: will universities use it, or abuse it? Available at: https://www.timeshighereducation.com/blog/Blockchain-revolution-will-universities-use-it-or-abuse-it

Hanson, R.T., Staples, M. (2017). *Distributed Ledgers, Scenarios for the Australian economy over the coming decades.* Canberra. Commonwealth Scientific and Industrial Research Organisation.

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

Inamorato dos Santos, A., Witthaus. G. & Punie, Y. (2016) OpenCred: exploring issues around the recognition of non-formal learning via MOOCs in Europe. Available at: http://emoocs2016.eu/wp-content/uploads/2016/02/proceedings-emoocs2016.pdf

International Standardisation Organisation (1999). Information technology -- Programming languages -- Ada: Conformity assessment of a language processor, 1999. ISO/IEC 18009:1999.

International Standardisation Organisation. (2010). International Standards and 'Private' Standards. Geneva, Switzerland: International Organisation for Standardisation.

Introduction to the Dutch Blockchain Coalition (2017). Available at: https://www.dutchdigitaldelta.nl/en/Blockchain/introduction-to-the-dutch-Blockchain-coalition

Jagers, C. (2017a). Blockchain-Based Records and Usability. Available at: https://medium.com/learning-machine-blog/Blockchain-based-records-and-usability-179a4eeaeb6e

Jagers, C. (2017b). Digital Identity and the Blockchain. Available at: https://medium.com/learning-machine-blog/digital-identity-and-the-Blockchain-10de0e7d7734

Jentzsch, C. (2016). Decentralised autonomous organisation to automate governance. Retrieved from https://download.slock.it/public/DAO/WhitePaper.pdf

Kirkland, R. (2017). What next for Blockchain? Available at: http://www.mckinsey.com/industries/high-tech/our-insights/what-next-for-Blockchain

Lewis, A. (2017). A gentle introduction to self-sovereign identity. Available at: https://bitsonblocks.net/2017/05/17/a-gentle-introduction-to-self-sovereign-identity

Li, R. (2017). Blockchain Based Multi-Signature Educational Certificates. University of Birmingham. Unpublished paper.

Lilic, J. (2015). uPort; A Glimpse into a Next Generation Self Sovereign Identity System. Available at: https://www.linkedin.com/pulse/uport-glimpse-next-generation-self-sovereign-identity-john-lilic

Lundkvist, C., Heck, R., Torstensson, J., Mitton, Z., Sena, M. (2017). UPort. A platform for self-sovereign identity. Available at: https://whitepaper.uport.me/uPort_whitepaper_DRAFT20170221.pdf

Mamoria, M. (2017). WTF is the Blockchain? The ultimate 3500-word guide in plain English to understand Blockchain. Available at: https://hackernoon.com/wtf-is-the-Blockchain-1da89ba19348

Marvin, R. (2017). Blockchain in 2017: The Year of Smart Contracts. Available at: http://www.pcmag.com/article/350088/Blockchain-in-2017-the-year-of-smart-contracts

McKinsey (2016). How Blockchains could change the world. Available at: http://www.mckinsey.com/industries/high-tech/our-insights/how-Blockchains-could-change-the-world

MIT Media Lab (2016). What we learned from designing an academic certificates system on the Blockchain. Available at: https://medium.com/mit-media-lab/what-we-learned-from-designing-an-academic-certificates-system-on-the-Blockchain-34ba5874f196

Ministry for Education and Employment, Malta (2017). Press release available at: https://www.gov.mt/en/Government/Press%20Releases/Pages/2017/January/24/PR1701 53.aspx

Morabito, V. (2017). Business Innovation Through Blockchain. The B3 Perspective. Springer.

Nakomoto, S. (2013). Bitcoin: A Peer-to-Peer Electronic Cash System. Available at: https://bitcoin.org/bitcoin.pdf

Newman, P. (2017). The Blockchain in the IoT Report. How distributed ledgers enhance the IoT through better visibility and create trust. BI Intelligence Report.

Peters, G.W., Panayi, E. and Chapelle, E., (2015), Trends in cryptocurrencies and Blockchain technologies: a monetary theory and regulation perspective. The Journal of Financial Perspectives: FinTech. Winter 2015, Volume 3 - Issue 3.

Peters, G. W., & Panayi, E. (2016). Understanding Modern Banking Ledgers Through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money. In P. Tasca, T. Aste, L. Pelizzon, & N. Perony (Eds.), Banking Beyond Banks and Money: A Guide to Banking Services in the Twenty-First Century (pp. 239– 278). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-42448-4_13

Piscini, E., Guastella, J., Rozman, A. and Nassim, T. (2016). Blockchain: Democratized trust. Distributed ledgers and the future of value. Deloitte University Press. Available at: https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/technology/deloitte-uk-tech-trends-2016-blockchain.pdf

Ryan, P. (2017). We need to figure out how to use the Blockchain properly. This is why. Available at: https://www.weforum.org/agenda/2017/06/Blockchain-is-stalling-but-whats-holding-it-up

Rzepecki, L. (2017). What is the difference between block chain, e-signature, and PKI/EIDAS? Available at: https://www.quora.com/What-is-the-difference-between-block-chain-e-signature-and-PKI-EIDAS

Pocius, D., Vaikutyte-Paskauske, J., Ravaioli, S., Dumcius, R., Saduikis, K., Buinauskas, D. (2017). Study to review the revision of the diploma supplement and analyse the feasibility of its digitalisation at European level. Available at: https://publications.europa.eu/en/publication-detail/-/publication/1ae19aac-6a9a-11e7-b2f2-01aa75ed71a1/language-en/format-PDF/source-32160429

Russell, J. (2017). Sony wants to digitize education records using the blockchain. Available at: https://techcrunch.com/2017/08/09/sony-education-blockchain

Schmidt, J.P. (2015). Certificates, Reputation, and the Blockchain. Available at: https://medium.com/mit-media-lab/certificates-reputation-and-the-blockchain-aee03622426f

Schmidt, J.P. (2017). Credentials, Reputation, and the Blockchain. Available at: http://er.educause.edu/articles/2017/4/credentials-reputation-and-the-Blockchain

Shrier, D., Wu, W., Pentland, A. (2016). MIT. Blockchain & Infrastructure (Identity, Data Security). Available at: https://cdn.www.getsmarter.com/career-advice/wp-content/uploads/2016/12/mit_Blockchain_and_infrastructure_report.pdf

Siebold, S. and Samman, G. Consensus. Immutable agreement for the Internet of Value (2016). KPMG. Available at: https://assets.kpmg.com/content/dam/kpmg/pdf/2016/06/kpmg-Blockchain-consensus-mechanism.pdf

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

Smolenski, N. (2016b). Identity and Digital Self-Sovereignty. A New Paradigm for Sovereignty on the High Seas. Available at: https://medium.com/learning-machine-blog/identity-and-digital-self-sovereignty-1f3faab7d9e3

Smolenski, N. (2017a). Blockchain Records for Refugees. Available at: https://medium.com/learning-machine-blog/Blockchain-records-for-refugees-bd27ad6e6da1

Smolenski, N. (2017b). The EU General Data Protection Regulation and the Blockchain. Available at: https://medium.com/learning-machine-blog/the-eu-general-data-protection-regulation-and-the-blockchain-1f1d20d24951

Sony (2016). Global Education Develops Technology Using Blockchain for Open Sharing of Academic Proficiency and Progress Records. Available at: https://www.sony.net/SonyInfo/News/Press/201602/16-0222E/index.html

Stanley, A. (2017). Consensys, Nation of Mauritius in Talks to Create 'Ethereum Island' Available at: http://www.coindesk.com/consensys-nation-mauritius-talks-create-ethereum-island

Staples, M., Chen, S. Falamanski, S., Ponomarev, A., Rimba, P., Tran, A.P., Weber, I., Xu, X., Zhu, J. (2017). *Risks and Opportunities for Systems using Blockchain and Smart Contracts.* Canberra. Commonwealth Scientific and Industrial Research Organisation.

Stockton, N. (2017). A Curious Plan to Save the Environment with the Blockchain. Available at: https://www.wired.com/2017/05/curious-plan-save-environment-Blockchain

Tapscott, D. and Tapscott, A. (2017a). The Blockchain Revolution and Higher Education. Available at: http://er.educause.edu/articles/2017/3/the-Blockchain-revolution-and-higher-education

Tapscott, D. and Tapscott, A. (2017b). Realizing the Potential of Blockchain. A Multistakeholder Approach to the Stewardship of Blockchain and Cryptocurrencies. Available at: http://www3.weforum.org/docs/WEF_Realizing_Potential_Blockchain.pdf

Torverkar, G. and Moskowtiz D. (2017) Indorse White Paper. V 1.0. Available at: https://indorse.io/static/media/Indorse-Whitepaper-v1.0.869d6b72.pdf

The Economist (2017). Governments may be big backers of the Blockchain. Available at: http://www.economist.com/news/business/21722869-anti-establishment-technology-faces-ironic-turn-fortune-governments-may-be-big-backers

The Economist Babbage Science & Technology Podcast: Digital Self Sovereignty. Available at: https://soundcloud.com/theeconomist/babbage-send-in-the-microbots?utm_source=soundcloud

Technavio (2017). Global Student Information System Market 2017-2021.

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

University of Nicosia (2017). Self-Verifiable Certificates on the Bitcoin Blockchain https://digitalcurrency.unic.ac.cy/free-introductory-mooc/self-verifiable-certificates-on-the-bitcoin-Blockchain

Vian, K. (2016). Own Your Achievements: Three Ways Blockchain Tech is Disrupting Education. Available at: https://Blockchainfutureslab.wordpress.com/2016/03/16/own-your-achievements-three-ways-Blockchain-tech-is-disrupting-education

Vigna, J. and Casey, M.J. (2016). The Age of Cryptocurrency: How Bitcoin and the Blockchain Are Challenging the Global Economic Order. Picador.

Watterson, A. (2016). The Blockchain for Education: An Introduction. Available at: http://hackeducation.com/2016/04/07/Blockchain-education-guide

Wikimedia Commons contributors (2017, "File:Hash function.svg," *Wikimedia Commons, the free media repository. Available at:* https://commons.wikimedia.org/w/index.php?title=File:Hash_function.svg&oldid=172142077

Wilson, S. (2016). Blockchain really only does one thing well. Available at: https://theconversation.com/Blockchain-really-only-does-one-thing-well-62668

Winjum, J. O. (1971). "Accounting and the rise of capitalism: an accountant's view." Journal of Accounting Research: 333-350.

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.

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/microsoft-msft-thinks-Blockchain-tech-could-solve-one-of-the-internets-toughest-problems-digital-identities

World Economic Forum (2015). Deep Shift Technology Tipping Points and Societal Impact. Available at: http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf#page=24

Yamey, B. S. (1949). Scientific Bookkeeping and the Rise of Capitalism. The Economic History Review, 1(2–3), 99–113. https://doi.org/10.1111/j.1468-0289.1949.tb00108.x

Online Resources

12.3 Websites

Blockcerts.org

Blockcerts.ehcoo.com

Blockchain.open.ac.uk

Blockchain.mit.edu

Blockchain-lab.org

Blockchainpilots.nl/home-eng

Certificates.media.mit.edu

Community.blockcerts.org

Consensys.net/resources/guides

Dci.mit.edu

Developer.ibm.com/Blockchain

Dutchdigitaldelta.nl/en/Blockchain

Ethereum.org

Hyperledger.org

ibm.com/Blockchain

openbadges.org

Tierion.com

Wiki.P2Pfoundation.net/Blockchain

12.4 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

Gupta, V. (2017). European Parliament Blockchain Presentation. Available at: https://www.youtube.com/watch?v=fCYT9KWoIdI

IBM Developer Videos (2017). Available at: https://www.youtube.com/channel/UCpEJ53BOa9YWTTXerZtKNhg/videos

IBM Think Academy (2017). Blockchain, how it works. Available at: https://www.youtube.com/watch?v=lD9KAnkZUjU

Inamorato dos Santos, A. (2017) Blockchain in Education – European Commission's JRC report preview, *Blockchain in Education Conference,* Groningen . Available at http://bit.ly/2lsyvDb

Mesropyan, E. (2017). 21 Companies Leveraging Blockchain for Identity Management and Authentication. Available at: https://letstalkpayments.com/22-companies-leveraging-blockchain-for-identity-management-and-authentication

Perry, R.E. (2017). Blockchain technology: From Hype to Reality. Available at: https://www.youtube.com/watch?v=v--lqndp0V4

Rosic, A. (2017). What is Ethereum? A Simple Explanation Anyone Can Understand. Available at: https://www.youtube.com/watch?v=ptLfwp6JYqk

Rosic, A. (2017). What is a Smart Contract? A Beginner's Guide. Available at: https://www.youtube.com/watch?v=qdoUpGg_DpQ

Stagars, M. (2017) The Blockchain and Us. Available at: https://www.youtube.com/watch?v=2iF73cybTBs

Tapscott, A. (2016) Blockchain Revolution. Talks at Google. Available at: https://www.youtube.com/watch?v=3PdO7zVqOwc

List of Acronyms

AWS	Amazon Web Services
CEN	European Committee for Standardisation
CPD	Continuing Professional Development
DAO	Distributed Autonomous Organisation
DLT	Distributed Ledger Technologies
IPFS	InterPlanetary File System
ISO	International Standardisation Organisation
FINTECH	Fusion of Finance and Technology
KMI	Knowledge Media Institute at the Open University, UK
LM	Learning Machine
MCAST	Malta College of Arts Science and Technology
MIT	Massachusetts Institute of Technology
MOOC	Massively Open Online Course
NGO	Non-Governmental Organization
P2P	Peer to Peer
PKI	Public Key Infrastructure
TSA	Trusted Authority
SaaS	Software as a Service
UNIC	University of Nicosia

List of Definitions

For the purposes of this study, we use the following definitions:

Authentication means the process of proving the counterparty identities and the existence of assets via private / public keys.

Badge means a symbol or indicator of an accomplishment, competency, skill or quality. It is similar to the paper certificates one receives upon school graduation, participation in an event or successful completion of a course. A digital badge is an image file, and can be easily shared. Moreover, a digital badge contains within its code hidden, encrypted data with information on its owner, its origin, the criteria required to earn it and a link to the documentation that confirms it was successfully earned. Thus, the performance task, criteria and evidence all become accessible to educators, employers and others who may want to understand more about a student, candidate employee or volunteer.

BADGR is a free and open source achievement recognition and tracking system used to issue, organize, and share Open Badges.

Bitcoin means a cryptocurrency and a digital payment system invented by an unknown programmer, or a group of programmers, under the name Satoshi Nakamoto. It was released as open-source software in 2009. The system is peer-to-peer, and transactions take place between users directly, without an intermediary. These transactions are verified by network nodes and recorded in a public distributed ledger called a blockchain. Since the system works without a central repository or single administrator, bitcoin is called the first decentralised digital currency. Besides being created as a reward for mining, bitcoin can be exchanged for other currencies, products, and services in legal or black markets. The invention of the Blockchain for bitcoin made it the first digital currency to solve the double spending problem, without the use of a trusted authority or central server.

Blockchain means a distributed ledger or database that maintains a continuously growing list of transaction records with various protections against tampering and revision. It is collectively built and maintained by every party that uses it. It is made up of a number of entries, called blocks, which are composed of the data being stored. These blocks are transmitted to the partners in the distributed ledger so they can be verified by unaffiliated parties. Each block contains a hash code that identifies the block that immediately preceded it, making the blocks sequential and chaining them together - hence the term 'Blockchain'. In terms of size, Bitcoin is the biggest Blockchain and in terms of the popular vernacular is automatically associated as being 'the Blockchain'. In practice, there are other Blockchains, such as the Ethereum Blockchain, as well as public and private Blockchains. All Blockchains have a digital currency of some kind associated with them.

Consensus mechanism means a method of authenticating and validating a value or transaction on a blockchain or a distributed ledger without the need to trust or rely on a central authority. Consensus mechanisms are central to the functioning of any Blockchain or distributed ledger.

Cryptocurrency means a medium of exchange, created and stored electronically in the blockchain, using encryption techniques to control the creation of monetary units and to verify the transfer of funds. Bitcoin and Ether are the best-known examples.

Cryptography means the process of enforcing the authentication and cryptographic validation of transaction integrity via quorum structures and confirmation via code without the need to trust or rely on a centralized authority.

Cryptographic signature means a method to mathematically validate the owner of a piece of data beyond any doubt if the user has kept the private key to sign the transaction safe.

Decentralised Autonomous Organisation (DAO) is a computer program, running on a peer-to-peer network, incorporating governance and decision-making rules. DAOs can be programmed to operate autonomously, without human involvement, or the code can provide for direct, real-time control of the DAO and funds controlled by it. The earliest DAOs.

Delegated proof-of-stake means stakeholders who elect "witnesses," responsible for ordering and committing transactions, and "delegates," responsible for coordinating software updates and parameter changes.

Digital Signature means binary code that, like a handwritten signature, authenticates and executes a document and identifies the signatory. A digital signature is practically impossible to forge and cannot be sent by itself but only as a part of an electronic document or message. It is similar to an electronic "fingerprint". In the form of a coded message, the digital signature securely associates a signer with a document in a recorded transaction. Digital signatures use a standard, accepted format, called Public Key Infrastructure (PKI), to provide the highest levels of security and universal acceptance. They are a specific signature technology implementation of electronic signature (eSignature).

Distributed ledger means a digital record of ownership that differs from traditional database technology, since there is no central administrator or central data storage; instead, the ledger is replicated among many different nodes in a peer-to-peer network virtual private network, and each transaction is uniquely signed with a private key.

Ethereum means a decentralised platform that runs smart contracts. Developed as a custom-built blockchain with shared global infrastructure, that can move value around and represent the ownership of property. Every node (computer) in the network runs an operating system called Ethereum Virtual Machine (EVM). EVM understands and executes the software written in Ethereum specific programming language. The software/apps executed by Ethereum Virtual Machine are called 'smart contracts.

Ethereum Wallet means a gateway to decentralised applications on the Ethereum blockchain. It enables a user to hold and secure ether and other crypto-assets built on Ethereum, as well as write, deploy and use smart contracts.

Europass means an EU initiative which aims to help people make their skills and qualifications clearly and easily understood in Europe, thus facilitating the mobility of both learners and workers. The Europass documents have been designed in such a way as to help people chronicle their skills and competences in a coherent manner, whether they are planning to enrol in an education or training programme, looking for a job, or getting experience abroad. Europass consists of a portfolio of five documents as follows: Two documents which individuals can complete independently - Europass Curriculum Vitae (CV) and Europass Language Passport; Three documents which are completed by the competent organisation on behalf of the individual - Europass Mobility, Europass Certificate Supplement and Europass Diploma Supplement.

Fault Tolerance means the property that enables a system to continue operating properly even if some of its components fail.

Federated consensus means a way to achieve Byzantine agreement (consensus), in which nodes can share another node and reach consensus without directly knowing all other nodes.

Genesis Block means the very first block in a blockchain.

Governance means the establishment of a decentralised control: there is no central authority command whose approval is required for reaching consensus. Some types of consensus mechanism use an elected leader who leads the validation and maintains the data which is been shared among the nodes. The governance aspect also includes the onboarding and offboarding of nodes within a permissioned network.

Halving means that Bitcoins have a finite supply, which makes them a scarce digital commodity. The total amount of bitcoins that will ever be issued is 21 million. The number of bitcoins generated per block is decreased 50% every four years. This is called "halving." The final halving will take place in the year 2140.

Hash Functions mean an application programming interface creates, through a process called hashing, a unique key or digital fingerprint for each file. Cryptographic hashes, such as the SHA256 computational algorithm, ensure that any alteration to transaction input — even the most minuscule change — results in a different hash value being computed, which indicates potentially compromised transaction input.

Hashrate means the number of hashes that can be performed by a bitcoin miner in a given period of time (usually a second).

Hierarchical deterministic keys mean a system of deriving keys from a single starting point known as a seed. The seed allows a user to easily backup and restore a wallet without needing any other information and can, in some cases, allow the creation of public addresses without the knowledge of the private key.

Immutability means unchangeability. An **immutable** object (unchangeable object) is an object whose state cannot be modified after it is created. Blockchain data cannot in practice be easily changed because it is continually replicated across many different locations and organisations. Blockchains are tamper-evident. Attempts to change it in one location will be interpreted as fraudulent and an attack on integrity by other participants, and will be rejected.

Interledger protocol means a protocol that connects legacy ledgers of the past with the distributed ledgers of the future.

Interplanetary File System is a protocol designed to create a permanent and decentralised method of storing and sharing files. IPFS takes advantage of the Bitcoin blockchain protocol and network infrastructure in order to store unalterable data, remove duplicated files across the network, and obtain address information for accessing storage nodes to search for files in the network.

Leader-based consensus means a type of consensus in which a leader is elected and stays in control until a vote decides on a new leader. In this model, it is the leader who validates transactions and sends data to the other nodes.

Ledger means an append-only record store, where records are immutable and may hold more general information than financial records.

Liveness means the transmission of data that is happening now and not a replay of a recording of data sent previously. Liveness is introduced into secure transmissions by mixing in a number that cannot be duplicated again. A node enjoys liveness if it can externalize new values without the participation of any failed nodes. Some nodes may fail, and as long as a majority of nodes are available, the network is still able to operate, can overall consensus response times), and impact on the network bandwidth of ever-larger ledgers being distributed also has to be considered.

Merkle tree means multi-signature; an authentication function that allows a group of users to sign a single document with more than one private key.

Mining means a record-keeping service. Miners keep the Blockchain consistent, complete, and unalterable by repeatedly verifying and collecting newly broadcast transactions into a new group of transactions called a block. Each block contains a cryptographic hash of the previous block, using the SHA-256 hashing algorithm, which links it to the previous block, thus giving the Blockchain its name. In order to be accepted by the rest of the network, a new block must contain a so-called proof-of-work. The proof-of-work requires miners to find a number called a nonce, such that when the block content is hashed along with the nonce, the result is numerically smaller than the network's difficulty target. This proof is easy for any node in the network to verify, but extremely time-consuming to generate, as for a secure cryptographic hash, miners must

try many different nonce values (usually the sequence of tested values is 0, 1, 2, 3, ... before meeting the difficulty target. Every 2016 blocks (approximately 14 days), the difficulty target is adjusted based on the network's recent performance, with the aim of keeping the average time between new blocks at ten minutes. In this way, the system automatically adapts to the total amount of mining power on the network. The proof-of-work system, alongside the chaining of blocks, makes modifications of the Blockchain extremely hard, as an attacker must modify all subsequent blocks in order for the modifications of one block to be accepted. As new blocks are mined all the time, the difficulty of modifying a block increases as time passes and the number of subsequent blocks (also called confirmations of the given block) increases.

Network Protocols mean the formal standards and policies comprised of rules, procedures and formats that define communication between two or more devices over a network. Network protocols govern the end-to-end processes of timely, secure and managed data or network communication.

Node means members or systems of a consensus network; a server that holds a replicated copy of the ledger; can have varying roles: to issue, verify, receive, inform, etc. For all intents and purposes, a node can be a VM instance.

Node-to-Node (N2N) means a mechanism in which only two nodes involved in a transaction take part; in effect, it eschews traditional consensus mechanism.

Open Standard means a non-proprietary protocol or specification governed by an organisation open to all who wish to join, such as the ISO standard.

Participant means an actor who can access the ledger: read records or add records to.

Peer means an actor that shares responsibility for maintaining the identity and integrity of the ledger.

Peer to peer (P2) network means an architecture of computers or networks that shares tasks, work, or files between peers. Peers are partners in the network with equal privileges and powers in the environment. In a P2P network, each computer or user is called a "node" and collectively they comprise a P2P network of nodes. The P2P network in the Blockchain consists of a series of computers and servers that each act as a node in the network. A blockchain network can be either permissioned or permissionless.

Permissioned means a private network in which users set rules about access, the consensus mechanism, governance, participation etc. Permissioned networks are limited to participants within a given business network. On permissioned Blockchains, participants are allowed to view only the transactions relevant to them.

Permissionless means a network that is open to any participant, and where transactions are verified against the pre-existing rules of the network. Any participant can view transactions on the ledger, even if participants are anonymous. Bitcoin is the most familiar example of a permissionless network.

Permissioned Ledger means a ledger where actors must have permission to access the ledger. Permissioned ledgers may have one or many owners. When a new record is added, the ledger's integrity is checked by a limited consensus process. This is carried out by trusted actors — government departments or banks, for example — which makes maintaining a shared record much simpler that the consensus process used by unpermissioned ledgers. Permissioned block chains provide highly-verifiable data sets because the consensus process creates a digital signature, which can be seen by all parties. A permissioned ledger is usually faster than a permissionless ledger.

Privacy means ensuring that only the receiver intended can read the message. The field of computing cryptography addresses many security and privacy issues of distributed consensus through the use of mathematical formulas for specific secure communication requirements within the context of any application-to-application communications.

Private Blockchain means a blockchain with constrained read/write access alongside a consensus algorithm which allows only a preselected group of people to contribute and maintain the integrity of the blockchain. A private blockchain may also refer to a blockchain operated by a private entity or consortium, with no or limited access by other parties, and typically with a small number (tens or hundreds) of processing nodes operating the blockchain. In this context, compared to public blockchains, technical optimisations may be used to improve the latency and throughput of the blockchain, and BFT consensus mechanisms may be used to provide stronger guarantees about the completion of transactions.

Private Currency means a currency issued by a private individual or firm, typically secured against uninsured assets.

Private Key means a private key is a string of data that shows you have access to bitcoins in a specific wallet. Private keys can be thought of as a password; private keys must never be revealed to anyone but you, as they allow you to spend the bitcoins from your bitcoin wallet through a cryptographic signature.

Private Key means an encryption key uniquely linked to the owner and known only to the parties exchanged in a transaction; it is secretly held in a digital wallet.

Proprietary consensus mechanism means a consensus model that is unique in nature and may or may not be based off of any existing consensus algorithms. The styles and stages used by nodes in a network to exchange messages asserting statements (can technically be differentiated by factors such as (nodes) leader election, types of leaders, the method of validating transactions, fault tolerance levels, utilization of tokens, strictness of algorithm, liveness guarantees, and permissions management)

Public Blockchain means a network in which anyone can participate by reading data, submitting transactions, and participating in the validation process. A public blockchain is operated as a public peer-to-peer system. Parties are usually identified by pseudonymous public/private keys, and a form of Nakamoto consensus is typically used to allow a large number (thousands) of processing nodes to operate the blockchain.

Public Key means the public address where other wallets send transaction values.

Public Key Infrastructure (PKI) means a secure data transmission and authentication system that uses public key cryptography (PKC).

Remote procedure call means a protocol that one program can use to request a service from a program located in another computer in a network without having to understand network details, also sometimes known as a function call or a subroutine call

Round-robin means a consensus mechanism in which nodes take turns at being the leader.

Scalability means the capability to cope and perform an increasing throughput and maintain or even increase its level of performance or efficiency when tested by larger operational demands. Latency is the delay in transaction processing

Security or Distributed ledger security means the process for protecting and safeguarding business and personal data, as well as transaction information. The validation of the results should be correct under non-Byzantine failures; also includes integrity (an assurance to the receiving node that a message received has not been altered in any way) and nonrepudiation (a mechanism to prove that the sending node really sent this message). Security can include digital signatures as a feature

Sidechain means the transfer of assets from one mechanism to a separate "pegged" mechanism; special-purpose ledger.

Smart Contracts mean applications that run on a custom-built blockchain, exactly as programmed and without any possibility of downtime, censorship, fraud or third-party interference.

Throughput means a measure of how many transactions can be processed in a given amount of time

Tokenisation means the process of replacing sensitive data with unique identification symbols that retain all essential information about the data without compromising its security

Wallet means the store for the information necessary to transact bitcoins. While wallets are often described as a place to hold or store bitcoins, due to the nature of the system, bitcoins are inseparable from the Blockchain transaction ledger. A better way to describe a wallet is something that "stores the digital credentials for your bitcoin holdings" and allows one to access (and spend) them. Bitcoin uses public-key cryptography, in which two cryptographic keys, one public and one private, are generated. At its most basic, a wallet is a collection of these keys. There are several types of wallets. Software wallets connect to the network and allow spending bitcoins in addition to holding the credentials that prove ownership. Software wallets can be split further in two categories: full clients and lightweight clients. The Ethereum Blockchain uses a different proof-of-work hash function (Ethhash), and supports Turing complete script execution. Any script willing to pay for execution can run on top of Ethereum. This is in contrast to Bitcoin, which uses the SHA-256 hash function for proof-of-work and supports a very limited set of script instructions

Annex 1: Potential Blockchain Applications beyond Education

Blockchain technologies represent a fundamentally new way to transact business. They usher in a robust and smart next generation of applications for the registry and exchange of physical, virtual, tangible, and intangible assets. Thanks to the key concepts of cryptographic security, decentralised consensus, and a shared public ledger (with its properly controlled and permissioned visibility), blockchain technologies can profoundly change the way we organize our economic, social, political, and scientific activities.

Table 3 highlights some use cases that can benefit from blockchain technology:

Table 3: Potential Blockchain Applications in Specific Domains beyond education and eGovernment

Domains impacted by Blockchain	Potential Blockchain Applications
Internet of Things	Device management (payments, directories, operations etc.); Grid monitoring; Smart home an office management; Cross-company maintenance markets.
Healthcare	Electronic medical records; Virus banks; Seed vault backup; Doctor-vendor RFP services and assurance contracts; Blockchain health research commons; Blockchain health notaries
Financial services	Letters of credit; Corporate debts and bonds; Trading platforms; Deal origination; POs for securities; Equities; Fixed income; Derivatives trading; Return swaps; Collateral management; Payment remittance; Repurchase agreements; Foreign exchange; Transfer of Value; Know your Client; Anti-Money laundering; Client and Product Reference data; Crowd-funding; Peer-to-peer lending; Compliance reporting; Trade Finance; Risk visualizing; Betting; Prediction markets; Capital Asset management.
Payments	Micropayments; Business-to-business international remittance; Tax filing and collection; Wallets and personal banking.
Insurance	Claims processing; P2P insurance; Ownership titles; Sales and underwriting; Property payments; Fraud prediction and prevention.
Government	eGovernment (various) including Government tender processes; Voting; Taxes etc.
Industrial	Manufacturing processes
Retail	Loyalty points
Media	Digital rights management; game monetization; Purchase and usage monitoring; Ticket purchasing; Fan tracking; Ad click fraud prevention; Real time auction; Ad placement.
Identity management	Personal; Objects; Families of Objects; Digital Assets; Multifactor authentication; Refugee tracking; Purchase and review tracking; Employer and employee reviews
Computer Science	Modernization of work; Disbursement of work; Direct payments; API for payments; Notarization and certification; Peer-to-peer storage and computational sharing; Domain name serving.

Asset Titles	Various
Consumer	Digital rewards; Sharing Economy; Peer-to-peer selling; Cross Company brand and loyalty tracking.
Supply Chain	Trade finance; Commodities pricing; Real time auction for supply delivery; Pharmaceutical tracking and purity; Agricultural food provenance tracking; Shipping and logistics management; Shipping and logistics management; Fraud prevention.
Resources	Energy, waste and water management; Resource extraction and framing; Environmental monitoring; Industrial operations.

Source: Adapted from IBM (2017) and proprietary sources

Annex 2: Decentralised Networks

From a technological standpoint, the blockchain is a network oriented software implementation. It shifts the risk and responsibility of code execution and data storage from centralized machines to decentralised networks. The following table, adapted from Batchu (2017), summarises the three components of blockchain technology that have enabled decentralised networks.

Contribution to Decentralisation	How the Blockchain contributes to Decentralisation
Trustless Consensus of participating nodes *Fundamental problem of distributed computing is to achieve system reliability and integrity in the presence of faulty players*	Blockchain provides a solution for a decentralised network consensus using cryptographic hash functions. It has developed different flavours of consensus algorithms suitable for different set of problems with varied control level, latency, security and transparency: — Proof-of-Work, reliability on intense processing power preferred majorly for highly secure networks. — Proof-of-Stake, reliability on loyal stakeholders of the network which helps to avoid energy wastage. — Designated Signatories, considered for performant networks with strict access controls. — Permissioned, suitable for enterprise solutions and standardisation of sectoral accounting. — Permissionless, robust public projects aiding in interaction and transaction models.
Maintaining a shared truth *Truth is the foundational element of a business or public organisation, including Government*	Blockchain has introduced an innovative mechanism to preserve the provenance of digitally shared truth with a system of chronologically chained blocks holding transactional information which always refers to the previous block. The blockchain introduces an innovative mechanism that preserves the provenance of a 'digitally shared truth'. The major three innovative implementations that bring a secured shared truth to life are: a) Transaction based ledgers—makes it easy to validate the ledger data with a single point of source (agreed genesis block) and provides an additional ability to cross-verify the mutation records of the token ownership.

	b) Block level incentives—enables modular, open & competitive participation to keep the system secure and running.
	c) Immutability and block confirmations—back referencing the previous blocks keeps adding security layers with each block confirmed by the network and makes it practically impossible to reverse engineer or alter the metadata inside these blocks.
	With the combination of these technologies, the blockchain achieves a secure, transparent, immutable, repository of truth, designed to be highly resistant to outages, manipulation, and unnecessary complexity.
Decentralised execution of programs *Decentralisation orchestration of code execution is the key to efficiency and performance of an application*	Apart from ledger keeping, blockchain also introduced a new way to orchestrate open and decentralised execution of computer programs. The key technology behind this could be: — Scripting Capabilities—standardised assembly code language with mutual agreement of nodes on the scope of logics which help to design complex acceptable transactions. — Smart Contracts—autonomous software code that can help in building large scale business logics running with independence. Independence in software execution enables complete autonomy in data and decision making. With the help of oracle networks (autonomous hardware collecting data points on incentive model) we are about to witness completely autonomous industrial scale systems.

Annex 3: Overview of Key Blockchain Technologies

Different blockchains may be used to store different types of records. Blockchains may also vary in the permissions for users to access them, in the data structure used and in the mechanisms used for consensus. This section gives a broad overview of the main blockchains currently in use.

Bitcoin

Bitcoin is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third-party (Nakamoto, 2013). Invented by the pseudonymous Satoshi Nakomoto, it is the first implementation of Blockchain technology, and today the Bitcoin network still forms the largest public Blockchain in existence.

Bitcoin is an online equivalent of cash. Cash is authenticated by its physical appearance and characteristics, and in the case of banknotes by serial numbers and other security devices. However, in the case of cash there is no ledger that records transactions and there is a problem with forgeries of both coins and notes. In the case of Bitcoins, the ledger of transactions ensures their authenticity. Both coins and Bitcoins need to be stored securely in real or virtual wallets respectively — and if these are not looked after properly, both coins and Bitcoins can be stolen (UK Government, 2016).

Due to a feature that allows it to store strings of up to 80 characters with every transaction, the Bitcoin blockchain is also being used as a public register to store hashes of documents. This in turn enables tamper-proof digital signatures, as explained in section 6.3.

Bitcoin is a fully open source project, and as such is governed by the community of Bitcoin users. Updates to the Bitcoin software, protocol and blockchain are accepted when more than half of the computers on the network choose to switch to a new version of the software.

There are some limitations of the Bitcoin blockchain:

- It can only store the sender, receiver, amount of cash transferred and a hash.

- It can only process fewer than 10 transactions per second (compared to tens of thousands for a typical credit card network), a limit which has already been reached.

- Its size is growing exponentially, leading to a situation where only users with massive amounts of computing power can keep a copy of the entire Blockchain, reducing the number of computers in the network, and decreasing security overall.

Ethereum

Ethereum is a decentralised platform that runs smart contracts - applications that run exactly as programmed without any possibility of downtime, censorship, fraud or third-party interference. These applications are stored and run on a custom-built blockchain.

Ethereum enables developers to create markets, store registries of debts or promises, move funds in accordance with instructions given long in the past (like a will or a futures contract) and many other things that have not been invented yet - all without a middle man or counterparty risk (Ethereum Foundation, 2017)[89].

Ethereum allows users to launch their own cryptocurrencies, where each 'token' in the cryptocurrency can represent anything including assets, units of learning, shares,

---

[89]   For a quick overview see https://hackernoon.com/wtf-is-ethereum-c65e0d67ac09

certificates, memberships, references, etc. Thus, Ethereum vastly increases the number of applications for which a blockchain can be used.

Furthermore, Ethereum can process more transactions per second, and is more flexible in the amount and kinds of data which can be stored on it.

While Ethereum is also an open source project, it is backed by the Ethereum Enterprise Alliance, which brings together more than 40 major corporations including Accenture, Microsoft, Samsung, Deloitte as well as several of the world's largest banks. The Alliance continually updates a roadmap for Ethereum and contributes code to the project.

Other Blockchains

While the Bitcoin and Ethereum blockchains are the two main blockchains, according to Smith & Crown, a specialised blockchain research consultancy, at the time of writing there are around 30 other public blockchains available, and around 100 more blockchains which are in the process of launching. Many of these blockchains contain data structures, or verification mechanisms which are suited to specific uses, including registering intellectual property, trading specific kinds of assets, gaming, storing identities and much more.

Most of these blockchains are funded through Initial Coin Offerings, whereby the tokens which will be traded on the blockchain are sold to the public, as a way of raising start-up capital.

In addition, many companies or groups of companies may choose to run private blockchains to trade specific classes of assets amongst themselves.

Technology Providers

Technology giants IBM and Microsoft are currently investing heavily in blockchain solutions[90]. Both companies have deployed similar three-prong strategies:

- Offering clients, the ability to launch their own private blockchains using IBM or Microsoft Cloud Computing products;

- Building applications on top of public blockchains, in particular offering storage or data services to smart contracts to allow them to determine whether their conditions have been met;

- Contributing to the code of public blockchains, in particular the Ethereum blockchain, to help move the technology forward.

Microsoft

In March 2017, Microsoft announced the expansion of its blockchain support on Azure to be the first public cloud that enables multi-member consortium blockchain networks addressing scenarios that require a deployment of a private network. In a post[91], Microsoft stated that it sees scenarios divided into the three 'common topologies':

1. Single organisation, multiple subscriptions: This is a common topology when divisions in an organisation do not trust each other, for example when one division is auditing another division.

2. Multiple organisations, private: This is the true consortium scenario where each organisation will have its own footprint but the services deployed must not be publicly accessible on the internet, even though communication will occur across organisations.

---

[90]   See https://www.coindesk.com/ibm-vs-microsoft-two-tech-giants-two-blockchain-visions/

[91]   See https://azure.microsoft.com/en-us/blog/multi-member-consortium-blockchain-networks-on-azure/

3. Multiple organisations, public-facing: Similar to the above topology, but in industries, enterprises, or scenarios where IT requirements allow or require the services deployed to be accessible to the public, over the internet.

Microsoft's Project Bletchley[92] outlines the organisation's vision for an open, modular blockchain fabric powered by Azure, and highlights new elements we believe are key in enterprise blockchain architecture. On 13 August, 2017, Microsoft unveiled a new a new blockchain-based framework, dubbed Coco, designed to make it easier for organisations to build and scale blockchain-based enterprise networks[93].

IBM

IBM has also developed its own set of blockchain technologies known as Hyperledger[94]. Hyperledger is an open-source collaborative effort created to advance cross-industry blockchain technologies. It is a global collaboration, hosted by The Linux Foundation, including leaders in finance, banking, Internet of Things, supply chain, manufacturing and technology. These 130+ members and 8 ongoing projects, including Hyperledger Fabric and Hyperledger Composer, work in concert to create an open, standardized and enterprise-grade distributed ledger framework and code base.

> *If we think of Blockchain as just a distributed technology - can it deal with revocation, change in ownership, and changes to what is currently considered as 'the truth'? The actual resolution of the truth may reside in a stack. A stack is some central thing you need to attest to - a certificate, a stock - which is digitally signed. Then you go up to a different level of attestation - you go through a trust chain. You validate each level of the stack in different ways. If you have a self-sovereignty level of attestation which is attested to my identity - if I can then get my bank to attest to my identity - we have something interesting. The vector is individuals, their identities, and their transactions. (Grey, 2017)*

> *"Perhaps the Bitcoin blockchain is being held back by a perceived lack of flexibility and performance. Ethereum has other weaknesses - such as the solidity of multi-faceted languages. There are various projects*

---

(92) *See* https://github.com/Azure/azure-blockchain-projects/tree/master/bletchley

(93) According to Microsoft, Coco was built to accelerate transaction speeds and streamline governance on companies' blockchain networks, and will be integrated with multiple open-source blockchains and distributed ledgers, including Ethereum, R3's Corda, Hyperledger Sawtooth, and JPMorgan Chase's proprietary Ethereum-based Quorum blockchain. Microsoft claims that Coco could enable a blockchain to process up to 1,700 transactions per second on a *private* version of the Ethereum blockchain, as compared with about 13 per second without the integration. Coco also includes a built-in governance tool that enables a blockchain's participants to vote on all terms and conditions of their network, such as when members can be added or removed. Microsoft says this simplifies governance procedures, and thereby speeds up transactions. A JP Morgan spokesperson confirmed the bank will be integrating Coco into Quorum when it launches next year, to enhance the blockchain's speed and security.

See announcement at: https://www.coindesk.com/coco-revealed-microsoft-jpmorgan-demo-new-blockchain-boosting-tech/

See White Paper at: https://github.com/Azure/coco-framework/blob/46596b4cb83ad759cd6dd8fd1cd5bce1629f3d3b/docs/Coco%20Framework%20whitepaper.pdf

(94) See https://www.hyperledger.org/wp-content/uploads/2017/08/Hyperledger_Arch_WG_Paper_1_Consensus.pdf

building alternatives to these. There is the B2 Chain in Hong Kong, RChange, scalable blockchains - interesting ideas trying to be proof of concept, but shipping other consensus mechanisms to a higher level. There are hybrid blockchains emerging. It is possible to build above private blockchains, IBM's Hyperledger. Microsoft are trying to build on top of a provision-less chain, and their identity project is working with Ethereum alliance as well as Blockcstack on Bitcoin. Ethereum has the capacity to build to private chains. Experimentation will be good enough for now. If you cannot build to scale on Bitcoin blockchain then build a private chain but be prepared to shift on to a permissionless chain at some stage.

What we can do is to build interoperability in our solutions. The solution is not whether the Blockchain or the Ethernet proves to be a winner - but whether we can deliver on the promise of a trustless, permission- less future". (Casey, 2017)

JRC Mission

As the science and knowledge service of the European Commission, the Joint Research Centre's mission is to support EU policies with independent evidence throughout the whole policy cycle.

EU Science Hub
ec.europa.eu/jrc

@EU_ScienceHub

EU Science Hub - Joint Research Centre

Joint Research Centre

EU Science Hub

Publications Office