THE EMERGING TREND OF BLOCKCHAIN FOR VALIDATING DEGREE APPRENTICESHIP CERTIFICATION IN CYBERSECURITY EDUCATION

I. Bandara[1], F. Ioras[2], M.P Arraiza[3]

[1]*Open University (UNITED KINGDOM)*
[2]*Bucks New University (UNITED KINGDOM)*
[3] *Universidad Politecnica de Madrid (SPAIN)*

Abstract

The network-centric world of the 21st century and explosive growth of the internet related technologies brought modern cybersecurity culture with complex threat landscape in the Higher Education environment. Cybersecurity landscape is always changing and education providers often do not have remit or in fact the means and capacity to cover the range of activities learners engage with, which attest their achievements, knowledge, and skills. Currently the awarding and validation of qualifications occurs exclusively under centralised management of an education institution or an employer take more ownership of the learning experience and its outcomes without compromising on safety, security, and accessibility. The centralised model of the present awarding and validation is no longer sustainable because learning happens increasingly on online platforms, and learning is far more international than it used to be. Key higher educational providers introduced degree apprenticeships which are new way to 'do both' higher level skills and provide progression routes to improve their employability prospects.

The 'Blockchain' (BC) facilitates digitized, decentralized, public ledger of all cryptocurrency transactions. It embraces a set of inter-related technologies. This paper expounds a novel BC-based architecture for transform centralised model of awarding and validation in to decentralized ledger of secured database. This database is shared, replicated, and synchronized for validation among the universities, partner institutions, professionals, statutory or regulatory bodies and industry bodies across the internet. The architecture offers secured collaborative validating system by qualification exchange with BC using trust methods within the decentralized topology.

Keywords: Blockchain (BC), Cybersecurity (CS), Degree Apprenticeship (DA), Internet, Secure Database, Peer-to-Peer (P2P), Decentralized Topologies, Inter-related technologies.

1 INTRODUCTION

A blockchain (BC) is fundamentally a distributed public ledger database of all transactions or digital events that have shared among participating parties. Transaction in the distributed public ledger is verified by a majority of the associated participants in the system [1]. Once entered, information can never be erased. The blockchain contains a certain and verifiable record of every single transaction ever made. The BC technology itself is non-controversial and has worked flawlessly over the years and is being successfully applied to both financial and non-financial world applications [1].

Degree Apprenticeships are combinational study of university and work-based learning to enable apprentices to gain a full bachelor's degree. This provision of an academic undergraduate degree is integrated with the development of experience, practice and learning in the workplace. Degree Apprenticeships (DA) are co-designed by training providers (the University) and employers ensuring that apprentices are equipped with the skills employers need and to develop their own future career. The quality management process of degree apprenticeship courses is inspected and acknowledged by group of experienced peers including internal and external academic representatives. The course validation procedure follows the principles of the quality assurance (QA) guidelines (e.g. QAA UK Quality Code for Higher Education [3]). The universities make an academic contribution to the design and development of degree apprenticeship courses but in cybersecurity (CS), modules must be developed to provide the most up-to-date cyber security principles, practice, tools and techniques. To enable consistency and effectiveness of SCDA validated programmes have to managed and governed by academic expertise and external input (industry partners). The validation framework also makes provision for a strategic level group where both partners deem this to be of benefit. Many DA

programmes incorporate a placement in industry in home country or different country. The placements are based on an agreed programme of work acceptable to both the home university and the external partner. For minimising the subjects on course accreditation and certificate validation the BC technology is considered as an appropriate system for supporting the entire process of validation.

The purpose of this paper is to investigates the viability, benefits and challenges of BC technology in validation of qualifications, with a focus on the application of the BC to academic and non-academic authorisations [2]. It is an exploratory study which is aimed at architecture for transform centralised degree apprenticeship certification awarding and validation in to decentralized ledger of secured database.

2 UNIQUE ADVANTAGES OF USING BLOCKCHAIN IN VALIDATING DA DOCUMENTS

In the Internet protocol suite, application layer provides services for an application program to ensure effective communication with another application program on the Internet [4]. The BC is more likely an application layer to run on the existing stack of Internet protocols, adding an entire new tier to the Internet to enable economic transactions in a cryptocurrency [5]. BCs are ledgers recording groups of transactions, known as blocks, which are linked together cryptographically in a linear temporal sequence. Key properties associated with a BC are high security, immutability, programmability depend on the architecture of the BC and the character of the consensus protocol it runs by that BC [6].

2.1 Building digital trust

Trust in cyberspace is a risk judgement between two or more people, institutions or organisations, it is based on two key requirements:

a) **authentication** – prove that process or action is true, genuine, or valid.

b) **authorisation** – prove actual checking of the permission values that have been set up when a user is getting access.

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 because there is no viable relationship unless the parties trust one another. In this sense, being trustworthy in a society is analogous to being creditworthy. The basic concept of trust remains unchanged in the cyberspace where it's rely upon many actors, whom we will never meet. 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 are becoming increasingly expensive, time-consuming, and inefficient [7].

BC technology provide a viable alternative to the current procedural, organisational, and technological infrastructure required to create institutionalised trust. Digital trust underpins every digital interaction by measuring and quantifying the expectation that an entity is who or what it claims to be and that it will behave in an expected manner [8].

2.2 Technical Characteristics of Blockchain Technology

The main role of BC is to establish a system of distributed consensus in the digital online world. This allows participating entities to know for certain that a digital event happened by creating an undisputable record in a public ledger [9]. The blocks are produced by encryption algorithm, each block contains the Bitcoin network transaction information on centralized ledger which is used for verifying the information effectiveness, then to generate the next block. A variation of a centralized ledger, with an element of distribution, involves several parties sharing responsibility for different parts of the single authoritative ledger. Decentralising and distributing a ledger involves the removal of the central controlling authority entirely by creating a system that several persons keep copies of the entire ledger. Making changes or writing to distributed ledger requires consensus from the persons who have copies and each addition or change is recorded in each copy of the ledger and it's equally authoritative [10].

2.2.1 A cryptographic hash function

A hash is a short code of defined length which serves as a fingerprint for a digital document [11]. To generate hash function for any digital document, require hash-generator program and it is 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 [12]. This will allow 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 because any small change in the document will automatically generate a completely different ID.

2.3 Blockchain-Secured Digital Syllabus

The DA cybersecurity syllabus, transferred to hash-generator to generate a hash from the document and each module in the syllabus will be document (hash) in a public database (the BC) which is identically stored on thousands of computers on internet [13].

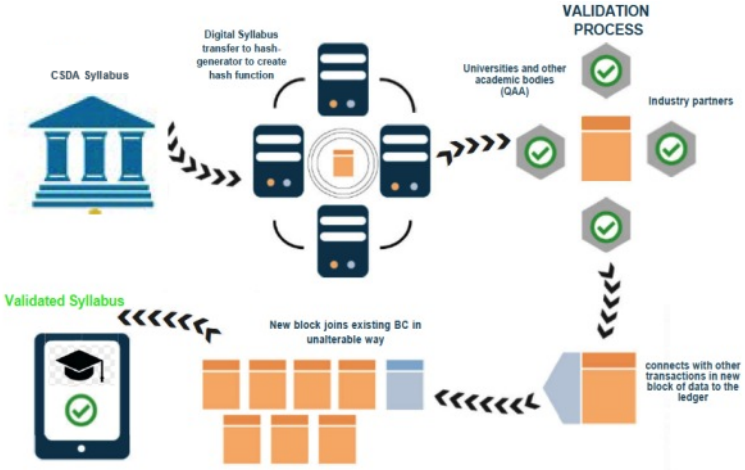

Figure1. Digital syllabus validation process using BC.

Figure 1 shows the DA course syllabus validation using BC. The data needed to verify the integrity and authenticity of a digital course syllabus is stored on a BC. To validate syllabus, University (or an academic body offering verification services) and industry partners will essentially follow the process above to ensure that the hash corresponds to the original digital file is to the right institution.

- The digital course syllabus created contains some course syllabus summary and description, briefly describing the course content, the goals, and desired objectives of the course. Also it stated learning goals and objectives and explain what subject background the student should be familiar with in order to comprehend the material presented in the DA course.
- The Issuer (university) then cryptographically signs the contents of the course syllabus using a private key to which only the issuer has access.
- The Issuer creates a cryptographic hash of the course syllabus file to verify that nobody has tampered with the content of the syllabus.

2.4 CSDA Digital Certificate Authority (CA) and Digital Syllabus

Validating the existence or the possession of signed documents (certificates) is very important and traditional document validation models rely on central authorities for storing and validating the documents, which presents some obvious security challenges. These models become even more difficult as the documents become older. The BC technology provides an alternative model to proof-of-existence and possession of certificates. A digital certificate is an electronic document and all solutions for digital certification use a system of digital signatures to issue certificates [14]. Digital certificate signature in BC is different from the electronic signature, which is simply a traditional signature drawn onto an electronic document or a scanned physical signature. Electronic signatures can be easily copied or forged, and provide no mechanism for verification or standardisation [15]. Blockchain technology is ideal new solution for secure, share, and verify certificates. The

decentralisation of the BC gives it a further advantage in that no third-party can alter digital certificates in the blocks without undoing the proof-of-work requirement that had verified. Beyond removing the necessity upon any certificate authority or trusted third-party, BC provide independent time stamping, which creates significant security benefits [2].

2.4.1 Combining Blockchain-Secured Digital Certificates with Digital Syllabus

In the case of certifications, a BC keeps a list of issuer and receiver of each certificate, together with document from a hash in a BC which is identically stored on thousands of computers around the world. By combining the DA certificate with a syllabus will ensure successful development and provision of degree apprenticeships. Key challenges to develop degree apprenticeships are faced by universities which have to bring together teams across their organisation, including teaching and learning, quality assurance and widening participation teams to respond quickly to employers' demand [16], such as:

- Lack of awareness of degree apprenticeships among employers
- Lack of degree apprenticeships in key occupational areas
- Difficulty of delivering degree apprenticeships to multiple employers
- Uncertainty of quality assurance oversight of degree apprenticeships
- Requirement to create programmes flexible and adaptable to different needs
- The reputation of apprenticeships

Universities are relatively more concerned about every challenges on DA, but their main concern is reputation of DA programs and validation. Concerning most up-to-date cyber security principles, practice, tools and techniques into DA syllabus and course validation it is required widespread expertise participation in course and certificate validation. Majority of the universities have designated teams working on DAs in order to make them easier to implement [17]. Considering the lack of support from industry partners for the CSDA degree program, the proposed method of combining syllabus with certificate will priorities to overcome potential obstacles mentioned above.

3 IMPLEMENTATIONS OF BC TECHNOLOGY IN COMBINED DIGITAL CERTIFICATE AND SYLLABUS IN CSDA PROGRAM

When BC technology is used in the issue of certificates, there is many advantages to verify credentials without an intermediary, but to enrich and add value to the existent digital certification ecosystem; BADGR and Mozilla Open Badge are already being used to provide digital certifications in some academic institutions [18] [19]. The objective of notarising combined certificates on a BC is therefore to transform a digital certificate received privately into an automatically verifiable by third parties through an immutable proof system, on a BC.

3.1 Combined CSDA certificate for digital self-sovereignty using BC Technology

The purpose of making combined CSDA certificate with self-sovereign identity is that all participants can enable recipient control of their claims through easy-to-use tools like digital certificate wallet with recipient ownership and vendor independence [20]. Within this context:

- **certificate ownership** means that individuals control the private keys that allow them to demonstrate ownership of their combined digital certificate.
- **vendor independence** means that access, display, and verification do not rely on any particular institution. When based on open-source standards, records can therefore be verified sovereign of any authorized institution (university) and/or industry partner.

Figure 2 shows the issuing a BC-secured certificate for CSDA program that certificate includes an adscription of CS course syllabus.

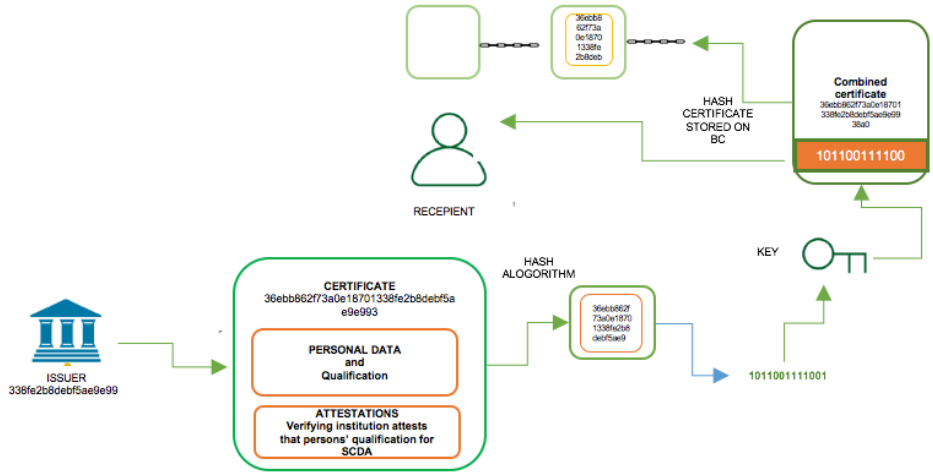

Figure2. Issuing a BC-Secured certificate for CSDA program.

Figure 3 shows the architecture of a verified BC-secured Self-Sovereign identity for CSDA program certificate and syllabus. The data needed to verify the integrity and authenticity of a certificate and syllabus is stored on a BC. To validate credentials, institution (university) and industry partners 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.

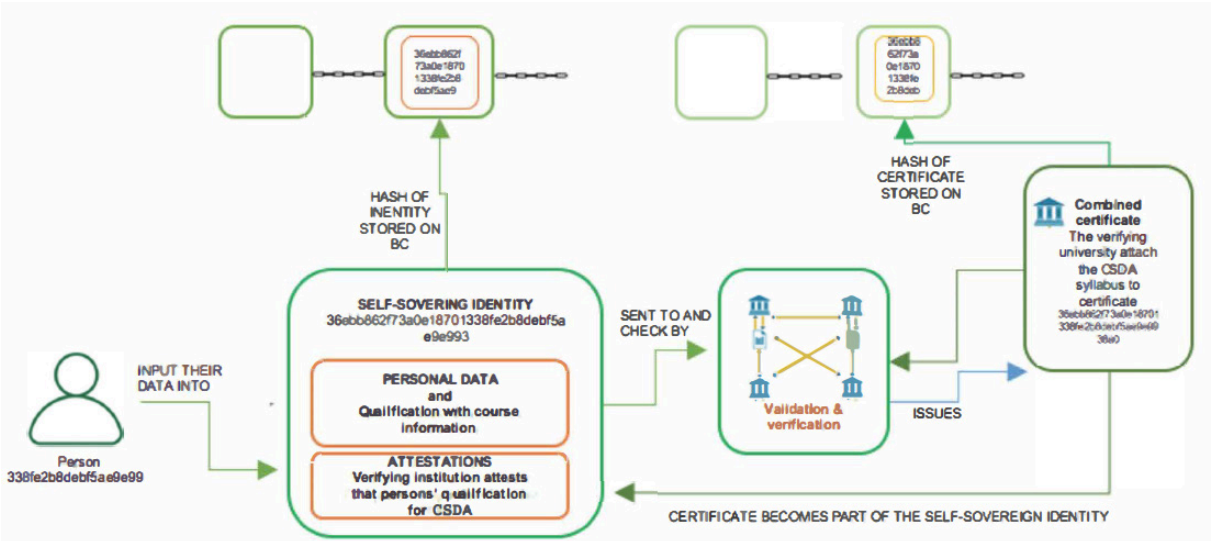

Figure3. Architecture of a Verified BC-Secured Self-Sovereign Identity for CSDA program.

The major advantages of this service is security and privacy that allow a user to give decentralized proof of the certificate and course information that can't be modified by a third party. The existence of the document is validated using BC that does not depend on a single centralized entity.

Academic institutes and companies will not be the only ones to take advantage of the accountability and consistency of the information available on BC platform. Students could in turn use the public metadata to seek similar profiles and, in doing so, foster the creation of new models of CS and related subjects without requiring a centralized authority to vouch for the validity of the information. Checking the data, the third-party (industry partners and other institutions) could then issue a certificate certifying the information as true with a statement. If this statement is uploaded to a BC, it provides a public attestation that the person's identity details are true, without needing to reveal any information about the person from their public key.

4 CONCLUSIONS

DA offer a wide range of benefits, providing opportunities for young people, meeting the skills needs of employers and reinforcing partnerships between universities and employers (industry partners). The distributed ledger functionality coupled with the security of BC makes it a very attractive technology to solve the current validation and certifying issues in education. It is relevant in all sorts of contexts: schools, colleges, universities, MOOCs, and degree apprenticeships. BC technology in DA validation process is greater encouragement to employers to engage with universities in a systematic way from the early stages of degree apprenticeship standard development.

Employers are very concerned about the programme specification and concise summary of the main features of the degree apprenticeship programme. To counteract this problem, implementations of BC technology in combined digital certificate and syllabus validation will increase relationships with thousands of employers, and to raise awareness of degree apprenticeship program.

REFERENCES

[1] Crosby, M., Pattanayak, P., Verma, S. and Kalyanaraman, V., 2016. Blockchain technology: Beyond bitcoin. *Applied Innovation*, *2*, pp.6-10.

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

[3] Jackson, N., 2001. Benchmarking in UK HE: an overview. *Quality Assurance in Education*, *9*(4), pp.218-235.

[4] Forouzan, B.A., 2002. *TCP/IP protocol suite*. McGraw-Hill, Inc..

[5] Xu, X., Pautasso, C., Zhu, L., Gramoli, V., Ponomarev, A., Tran, A.B. and Chen, S., 2016, April. The blockchain as a software connector. In *Software Architecture (WICSA), 2016 13th Working IEEE/IFIP Conference on* (pp. 182-191). IEEE.

[6] de la Rosa, J.L., Torres-Padrosa, V., el-Fakdi, A., Gibovic, D., Hornyák, O., Maicher, L. and Miralles, F., 2017. A SURVEY OF BLOCKCHAIN TECHNOLOGIES FOR OPEN INNOVATION. In *4rd Annual World Open Innovation Conf. WOIC* (pp. 14-15).

[7] 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

[8] Kelton, K., Fleischmann, K.R. and Wallace, W.A., 2008. Trust in digital information. *Journal of the Association for Information Science and Technology*, *59*(3), pp.363-374.

[9] Crosby, M., Pattanayak, P., Verma, S. and Kalyanaraman, V., 2016. Blockchain technology: Beyond bitcoin. *Applied Innovation*, *2*, pp.6-10.

[10] Peters, G.W. and Panayi, E., 2016. Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money. In *Banking Beyond Banks and Money* (pp. 239-278). Springer International Publishing.

[11] Swan, M., 2015. Blockchain thinking: The brain as a dac (decentralized autonomous organization). In *Texas Bitcoin Conference* (pp. 27-29).

[12] Guay, Y. and Morin, J.G., 2007. *System and method for digital signature and authentication*. U.S. Patent Application 11/181,506.

[13] Unitt, A., Newvoicemedia, Ltd., 2017. *System and methods for tamper proof interaction recording and timestamping*. U.S. Patent 9,553,982.

[14] Halevi, S. and Krawczyk, H., 2006, August. Strengthening digital signatures via randomized hashing. In *Crypto* (Vol. 4117, pp. 41-59).

[15] Zyskind, G. and Nathan, O., 2015, May. Decentralizing privacy: Using blockchain to protect personal data. In *Security and Privacy Workshops (SPW), 2015 IEEE* (pp. 180-184). IEEE.

[16] Degree apprenticeships: realising opportunities - Universities UK, Hefce report, 2017, Universities UK publications, Available at: www.universitiesuk.ac.uk

[17] Thomas, S. and Grimes, D., 2003. Evaluating the integration of key skills and NVQs into an undergraduate degree programme: a case study from the graduate apprenticeship initiative. *Education+ Training*, *45*(7), pp.383-391.

[18] Goligoski, E., 2012. Motivating the learner: Mozilla's open badges program. *Access to Knowledge: A Course Journal*, *4*(1).

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

[20] Yan, Z., Gan, G. and Riad, K., 2017, April. BC-PDS: Protecting Privacy and Self-Sovereignty through BlockChains for OpenPDS. In *Service-Oriented System Engineering (SOSE), 2017 IEEE Symposium on* (pp. 138-144). IEEE.