A Graduation Certificate Verification Model via Utilization of the Blockchain Technology

Osman Ghazali and Omar S. Saleh
School of Computing, Universiti Utara Malaysia, 06010 UUM Sintok, Kedah, Malaysia
osman@uum.edu.my

***Abstract*—The graduation certificates issued by universities and other educational institutions are among the most important documents for graduates. A certificate is a proof of a graduate's qualification and can be used to apply for a job or other related matters. The advance of information technology and the availability of low-cost and high-quality office equipment in the market have enabled forgery of important documents such as certificates, identity cards, and passports. However, verification of certificates using traditional methods is costly and very time-consuming. Therefore, the goal of this paper is to propose a theoretical model that can offer a potential solution for academic certificate issuing and verification using blockchain technology. The blockchain technology contains several functions including hash, public/private key cryptography, digital signatures, peer-to-peer networks and proof of work. The model uses various elements to formulate the block which is divided into two main processes, namely issuing a digitally signed academic certificate and verifying the academic certificate. The proposed model showed that academic certificate authentication could leverage the blockchain technology. It meets all the conditions necessary for a modern academic certificate verification system. In addition, it closes the gaps and challenges in the existing methods to verify academic certificate authenticity.**

***Index Terms*—Blockchain Technology; Graduation Certificate Verification; Graduation Certificate Authentication; Graduation Certificate Forgery**

I. INTRODUCTION

Institutions issue certificates to students who have completed graduation requirements. A graduation certificate is mostly in the form of a paper-based document as an electronic document cannot effectively replace a physical certificate [1]. However, due to the presence of advanced and cheap scanning and printing technologies, the forgery of certificates has increased. This threatens the integrity of the certificate holder and the university that issued the certificate [2].

Therefore, document validation and verification have become important tasks. It is necessary to validate that the graduation certificate presented by the graduate is genuine and the holder is the rightful owner. Moreover, a graduation certificate has to be verified to ensure that its content is correct and also to ensure that the certificate comes from an authentic source [3].

Educational institutions attempt to combat fraud and forgery in several ways. However, most of the methods are time-consuming because they are manual and involve human interaction [4]. During the process, much time will be spent in either reaching out to the university to verify a certificate or in awaiting a reply from the university to confirm that the certificate is valid, and the information is accurate. This process can be extremely laborious and expensive especially if a company needs to check the certificates of several hundreds of applicants. Hence, this research attempts to propose a theoretical model that can offer a potential solution for academic certificate verification using blockchain technology.

II. THE PROBLEM OF FAKE CERTIFICATES

Academic certificates are highly esteemed as they serve as an indicator of the human capital of the bearers [5]. Human capital refers to the skills, competencies, knowledge, and aptitudes achieved through education [6]. Academic qualifications are particularly crucial in employment situations as they serve as a guarantee of not just the knowledge, expertise and skills of the holders but also of their abilities, reliability, and dedication [7].

From the perspective of some researchers, Baum [8] found a positive correlation between educational attainment levels and better employment prospects and economic security. Moore points out that academic qualifications are considered to be genuine when they are conferred by a university that is legally authorized to award such certificates [9]. As they are so valuable, people often lie about their academic qualifications by producing fake certificates.

Grolleau [10] stated that in the United States there are currently 2 million fake degree certificates in circulation and 300 unauthorized universities are operating. Cohen and Winch [11] indicated that the United States has the highest number of fake institutions in the world followed by the United Kingdom which has about 270 fake institutes. Healy [12] found that up to 35% of candidates in Australia falsified their academic credentials for the sake of employment.

The Association of Certified Fraud Examiners stated that 41% of applicants submit fake certificates annually [13]. The Wall Street Journal stated that 34% of credential/certification information submitted by applicants reveal discrepancies and misrepresentations about the applicants' experience and education [14]. A survey observed that most candidates lie at least about some part of their educational credentials and experience [15]. Academic certificate fraud costs employers about $600 billion every year [12].

There are five different sources of fake academic certificates. These include:

1. 'Degree Mills' where bogus qualifications are generated and sold to clients.
2. 'Fabricated Documents' that represent a fictitious degree or institute.
3. 'Modified Documents' that are alterations in legitimate documents such as changes in enrollment or graduation dates, grades, course content, date of birth, specialization, etc.
4. 'In-House Produced' which are fake documents

fabricated by the employees of legitimate institutions and printed on authentic paper and bearing the seals, stamps, and signatures of the institution.

5. ‘Translations’ or documents inaccurately translated to match requirements in a receiving country.

Obtaining a white-collar job is impossible without academic credentials. Employers require fresh graduates, who apply for jobs, to present proof of their academic credentials. The employer will make the applicant waiting for their credentials to be authenticated by their colleges. Verification is time-consuming, usually takes days or weeks. Employers or organizations spend their valuable time coordinating the verification with the respective colleges to obtain the best employees with impeccable skills and knowledge. Though document verification is burdensome, it is necessary for establishing applicant authenticity, whether for education, employment or visa application. The blockchain is the latest technology that can simplify the authentication process for academic credentials for both employers and students.

III. Limitations of Traditional Verification System

This section discusses the limitations of the traditional verification system. Existing verification methods do not guarantee records that are not sealed, secured, tamper-proofed, and authenticated [16]. In [16] the authors stated five limitations of traditional verification system which are ownership, availability, dependency on third-party agencies, time consumption and cost. Explanation of each limitation as follows:

1. ***Ownership*** – Certificates are awarded to and are owned by individuals. However, the issuing authority still needs to reissue or authenticate certificates. The certificate ownership does not automatically appertain to the individuals.
2. ***Availability*** – Physical documents may be lost or damaged. Hence, individuals who lose them cannot readily obtain duplicates. Moreover, records cannot be retrieved if the issuing authority stops its operation.
3. ***Dependency on third-party agencies*** – Many organizations depend on third-party verification agencies to contact issuing authorities and verify document authenticity.
4. ***Time consumption*** – The process is time-consuming. The speed of verification depends on the response time of issuing authorities and their location.
5. ***Cost*** – Verification and notarization are costly. A fee is charged for each verified document.

IV. Related Work

Blockchain Technology aims to create a decentralized environment, so third-party control is not needed [17]. It has been introduced to be applied in several domains due to its advantages. Blockchain has been introduced to be applied in healthcare domain [18]. It is also applied in smart government [19], e-government [20] and business [21]. The potential of blockchain in education domain is the main focus of this research. Hence, this research aims to use blockchain on document verification, more specifically graduation certification verification.

The blockchain technology is an ideal infrastructure that protects, shares and authenticates learning achievements [22]. Public Key Infrastructure (PKI) has changed the central authority with a highly robust decentralized structure, which enhances network longevity because of the numerous block duplicates, where the signatures are stored. Blockchain decentralization restricts third parties from altering or deleting transactions kept in the blocks unless they undo the proof-of-work requirement that had verified them.

Blockchain technology utilizes an incorruptible digital ledger. This ledger can be set to document financial transactions and anything with economic or non-economic value. Such technology was developed for Bitcoin in 2008 and is now applied in many fields [23]. A blockchain can list issuers and receivers of a certificate. The public database (blockchain) stores document signatures (hash) on thousands of computers globally.

Digital certificates that are kept safe on a blockchain have significant advantages over regular digital certificates. Anyone who can access the blockchain can easily authenticate the certificate using an easily available open source software. Hence, intermediary parties are no longer needed. Thus, the certificate can be authenticated even after the organization is dissolved or it no longer has access to the issued record. Issued records and received certificates on a blockchain can be removed if all copies on all computers that host the software are destroyed. The hash creates a link to the original document and is held by the user. The mechanism allows the publishing of the document signature and does not require the publishing of the document itself. This mechanism preserves the confidentiality of documents.

V. The Main Technologies Comprising a Blockchain

The blockchain is a composite technology containing several functions including hash, public and private key cryptography, digital signatures, peer-to-peer networks, and proof of work. Each of these is explained as follows.

- ***Hash*** - A hash is a shortcode of fixed length. Data input from a document into hash-generator results in a hash output containing a certain number of digits. This hash then forms a unique ID. Inputting the same data into the hash generator results in the same hash value. However, even minor differences (such as changing a single letter of text) in data input results in a completely different hash [24]. Figure 1 shows the mechanism of generating a hash.

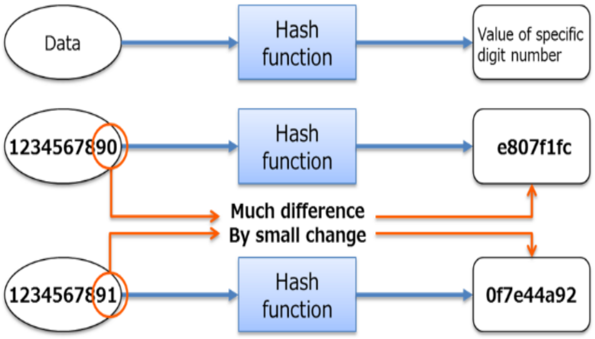

Figure 1: The Hash Generator

In Figure 1 it is observed that even a small change in the data input will result in a very different hash being generated. This characteristic of a hash may be used for the detection of any falsification of data and is used in a blockchain mechanism for authentication purposes.

- ***Public and Private Keys*** – This element of the blockchain is based on the principle of generating different keys for encryption and decryption. In a blockchain, it is always the public-key cryptographic method that is used and involving the generation of a private key for private use and a public key for public use as indicated in Figure 2.

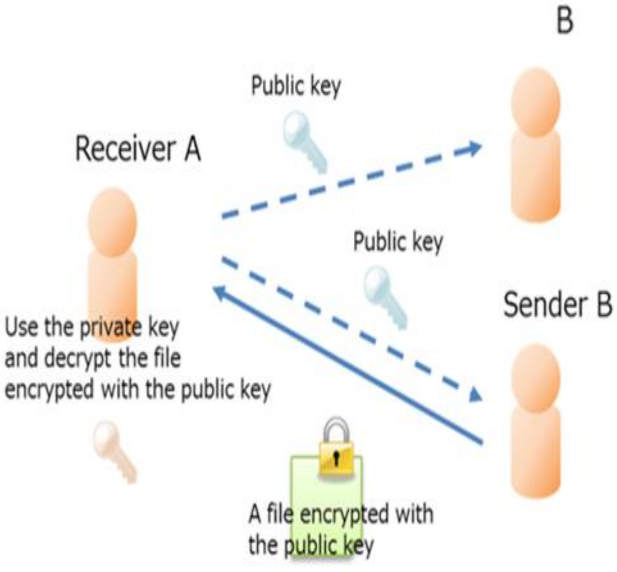

Figure 2: The Public Key Encryption

This method is different from the symmetric key cryptographic method which uses the same key for both encryption and decryption and where the delivery mechanism to the relevant party must be secured [25]. Public key cryptography facilitates safe delivery and receipt of files only when the party verifying the document creates both a private and a public key and sends the public key to the sender beforehand. If the verifying party maintains the confidentiality of the private key, the safety of the transaction is maintained even though the public key is easily accessible to everybody.

- ***Digital Signatures*** – Both the hash and the public key cryptographic methods are used to create a digital signature mechanism which may be used to validate the authenticity of information sent over the Internet. The digital signature is made by encrypting the hash value of the file being sent to the verifier with the public key of the sender [12]. The file is also sent online to the verifier. The verifier uses the data contained in the file to generate a hash value. The verifier also uses its private key to decrypt the digital signature and extract the hash value contained therein. If the two hash values matched, this means that the digital signature is authentic, and the data contained in the certificate has not been forged.

- **Peer-to-Peer (P2P) 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 of a P2P network of nodes [16].

VI. POTENTIAL OF BLOCKCHAIN TECHNOLOGY

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 organizations to issue immutable digital certificates which are valid in perpetuity since their authenticity can be verified against the blockchain. These advantages over current systems significantly increase the value proposition of digital certificates and will likely push digital certification into the mainstream [16]. Blockchain technology removes the need for educational organizations to validate credentials. Since certificates issued on the blockchain can be automatically verified, educational organizations will no longer need to commit resources to this task [12].

The blockchain technology is ideal as a novel infrastructure that protects, shares and authenticates learning achievements [12]. PKI changes the central authority with a highly robust decentralized structure, which enhances network longevity because of the numerous block duplicates, where the signatures are stored. Blockchain decentralization restricts third parties from altering or deleting transactions kept in the blocks unless they undo the proof-of-work requirement that had verified them. Blockchains also offer independent time stamping, which increases security.

Having a reliable timestamp is important in situations where credentials can expire. The issuer must also rotate issuing keys regularly for security and in response to a key leak. An independent timestamp is needed when determining whether a record was issued by a specific issuer during the validity of the key. Unlike many PKI systems, Blockchain signatures are file-format independent. Any document, regardless of the proprietary standards with which it was created, can utilize the same software for signature [12]

VII. PROPOSED MODEL FOR GRADUATION CERTIFICATE VERIFICATION

Over the years, universities have increased in size to accommodate the huge growth in the student base, faculty base, and other related entities. This has resulted in operational challenges for university officials and staff and providing services to large student and alumni communities have become an enormous task. Gradually, it has started to affect the quality of service provided to the student and alumni network. Many factors have led to reduced operational efficiency in student services at universities.

One of the most significant factors that have had a detrimental effect on the quality of university services is the verification process for educational certificates and related documents. Hence, the proposed model shown in Figure 3 aims to utilize the blockchain technology for graduation certificates verification. The blockchain is the latest technology that can simplify the authentication process of academic credentials for both employers and students.

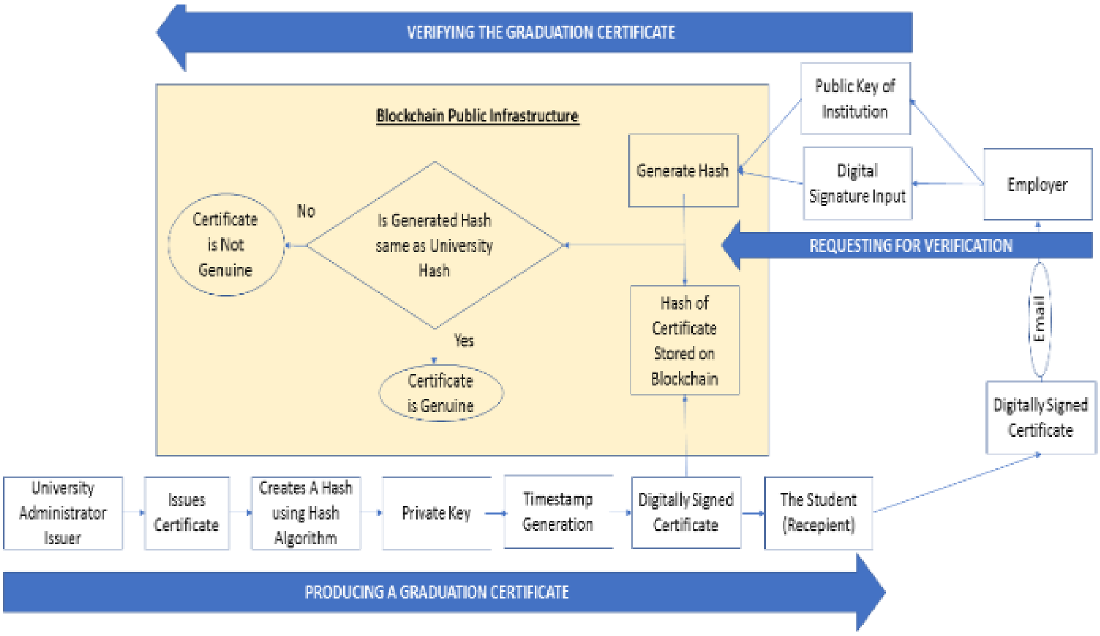
VERIFYING THE GRADUATION CERTIFICATE
Blockchain Public Infrastructure
Public Key of Institution
Generate Hash
Digital Signature Input
Employer
Certificate is Not Genuine
No
Is Generated Hash same as University Hash
REQUESTING FOR VERIFICATION
Hash of Certificate Stored on Blockchain
Email
Yes
Certificate is Genuine
Digitally Signed Certificate
University Administrator Issuer
Issues Certificate
Creates A Hash using Hash Algorithm
Private Key
Timestamp Generation
Digitally Signed Certificate
The Student (Recepient)
PRODUCING A GRADUATION CERTIFICATE

Figure 3: Blockchain-based Model for Graduation Certificate Verification

VIII. Discussion

Obtaining a white-collar job is impossible without academic credentials. Employers require fresh graduates to present proof of academic credentials. Students waiting for their certificates have their credentials authenticated by their colleges. Verification is time-consuming as it usually takes days or weeks. Employers/organizations spend their valuable time coordinating the verification with the respective colleges to obtain the best employees with impeccable skills and knowledge.

Document verification is burdensome but necessary for establishing applicant authenticity, whether for education, employment or visa application. The blockchain is the latest technology that can simplify the authentication process for academic credentials for both employers and students. Blockchain technology allows users to store important documents like academic certificates, as cryptographically signed digital documents. Such digital documents simplify transparency and file sharing with employers or other authorities for recruitment or admission.

This indisputable technological phenomenon requires issuing authorities to bring out digital certificates to a blockchain network. Their storage is by one-way hash coding [26]. An employer requesting a copy from a prospective employee can receive academic credentials/documents from the educational institution through his or her blockchain. This individual must send the public key to the academic institution where he or she graduated. An individual applying for a job must share his or her digitalized academic credentials with the prospective employer.

IX. Analysis of the Proposed Solution

An analysis of blockchain principles indicates that it is a composite technology containing several existing functions already explored in the previous section including hash, public and private key cryptography, digital signatures, peer-to-peer networks and proof of work.

Various elements are combined to formulate the block which in this research are categorized into two broad groups including issuing a Digitally Signed Academic Certificate and verifying the academic certificate. The theoretical model developed is presented in Figure 3.

A. *Issuing the Digitally Signed Academic Certificate*

The educational institution has the primary responsibility to issue a digitally signed academic certificate. This research proposes that this can be done using the blockchain as shown in Figure 3 using the following concepts.

- ***Hash Generation*** – This research recommends the use of SHA-256 hash generator to generate hashes because of its reliability and because it is an open-source online tool which can be used to generate the SHA-256 hash of any string of data.
- ***Public and Private Keys*** – the model proposed in this paper also uses private and public keys. The public key is issued to the university. The university, in turn, issues the student with a private key which is to be kept confidential.
- ***Digital Signatures*** – both the hash and the public key cryptographic methods are used to create a digital signature mechanism which may be used to validate the authenticity of information sent over the Internet. According to research conducted in [27], the digital signature is made by encrypting the hash value of the file being sent to the verifier with the public key of the sender. The file is also sent online to the verifier. The verifier uses the data contained in the file to generate a hash value. The verifier also uses its private key to decrypt the digital signature and extract the hash value contained therein. If the two-hash values match, this means that the digital signature is authentic, and the data contained in the certificate has not been forged.

- ***Timestamping*** – adds another layer of security to the digital academic certificate. This model uses a peer-to-peer network-based system to issue a digital stamp that is affixed to the document and indicates the precise day, month and year when the digital certificate was issued. The principle of generating the timestamp is to consider the entire time taken to generate the digital certificate and the digital signatures as a block of data that is then encrypted to produce a code that indicates the date on which the document was issued.
- ***Digitally Signing the Document*** – The digital signature generated by the model is composed of four elements including (i) the hash produced by the hash generator, (ii) a public key, (iii) a private key and (iv) a timestamp indicating the precise time that the certificate was issued. The document gets signed by combining the hash that has been generated using the private key issued to the student to create a unique code which is the initial digital signature. This code is combined with the timestamp to create a unique digital signature that is then stamped onto the document. Moreover, the signature is secured using a combination of hash, private/public keys, and timestamps. The signature is thus unique to the document issued to the student and can only be decrypted using the private key held by the student. Never can the private key of the student be deciphered through reverse engineering of the digital signature. If in future, even a small element of the document tampers, a completely different hash value will be generated.
- ***Issuing and Hosting the Certificate*** – The university issues to the student both a hard copy of the educational certificate and the digitally signed document. The university then uses the hash generator to create a hash of the final signed document. This hash comprises of a unique alphanumeric string that indicates nobody has tampered with the certificate and its contents. The hash is then hosted on the blockchain and the private university key is used to create a record that indicates the certificate was issued to the said student on the said date.

B. Verifying the Academic Certificate

When the student (the second party) applies for a job, the employer (who is the third party) will want to know the authenticity of the certificate from the university (the first party). In order to do this, the steps listed in Table 1 are proposed to validate and verify the digital signature.

X. Benefits of Issuing Certificates Using Blockchain Technology

The use of the blockchain technology in issuing certificates offers an opportunity to authenticate credentials even without an intermediary and to improve the existing digital certification ecosystem. Therefore, notarizing certificates on a blockchain transforms a digital certificate, which is privately received by a student. This document is automatically verifiable and can be consulted by third parties through a public blockchain.

Students may gain access to a public platform if they share sensible metadata, which includes private information. A blockchain can be used as proof of knowledge, and private data may not be revealed during an open consultation of metadata that is related to certifications [16, 28, 29]. Students may approach academic institutions and employers and at the same time maintain confidentiality. Information marked as public during proof generation process can be accessed by third parties. Blockchain certification bridges the gap between research practices of universities and the necessity for pragmatic market solutions. Many university admission offices are concerned about payment fraud from international students and of the tampering of the number of student cohorts of higher education institutions.

Some countries are ready to entice central authority for a semi-authentic seal of authenticity. For the meaning and utility of an actual credential, a third-party verifier, such as an organization that receives applicant credentials, must be won over by the authenticity of the certificate [26, 28] The standard requirements are integrity and authenticity. Integrity means the content has not been altered and should match the original message of the issuer, it means the issuer must be the one who declared the certificate and the name should not be forged.

Table 1
Issuing a digitally signed document

Step No	Particulars
1	Public keys of educational institutes are easily available on the internet or in public directories. In addition, they can be provided to the employer by the graduates.
2	The employer uses verification software to scan and input the digitally signed document and the public key.
3	The verification software uses the digital signature and the public key to generate a hash.
4	The hash generated by the verification software is compared with the hash of the original certified copy.
5	The verification software also checks if the digital signature is linked to the public key of the educational institution.
6	Both steps are done without the requiring students to disclose their private keys.
7	If both conditions are true, the verification software creates an output that informs the prospective employer that the certificate is valid
8	If anyone or both conditions are false, the verification software creates an output that informs the prospective employer that the certificate is fake

XI. Benefits of Proposed Model

This section discusses the benefits of the proposed model for the issuing authorities and recipients and consumers. Issuing authorities, recipients, and consumers would get special benefits from the proposed model as shown below:

1. *Issuing Authorities Benefits*
   - Only cryptographically-sealed data that cannot be falsified are issued.
   - All data are stored securely and can be referenced.
   - Spending unplanned time for the transmission of official records to individuals is not needed.
   - Records can be verified instantly without depending on issuing authorities.

- Official records can be owned and shared easily.
- Records are not lost because transactions are recorded on the blockchain.
- Records can be checked by third parties anytime.
- Calling separately for the deletion of certificates that are expired or errored is not needed.

2. *Recipients and Consumers Benefits*
   - Cryptographically sealed data are owned and shared.
   - All records can be stored in one wallet.
   - Requesting authenticated records has no waiting time.
   - Verification of information is instant and does not depend on issuing authorities.
   - Verifying agencies and employers should have access to the virtual verification process.
   - Records are not lost because transactions are listed on the blockchain.
   - Certificates can be accessed, and sheets can be marked anytime.
   - The latest record can be verified because of the easily integrated blockchain lookup services.

XII. Conclusion and future work

In this paper, a blockchain-based model for graduation certificate verification was proposed to enhance the verification mechanism. Thereby will reduce the incidence of certificate forgeries and ensure that the security, validity, and confidentiality of graduation certificates would be improved. The proposed model offers many benefits for both the issuing authorities and recipients and consumers. The advantage of the proposed model is that all the information that is required to validate and authenticate the certificate is hosted on the blockchain itself. In order to validate the certificate, the prospective employer need not contact the university at all. All it needs to do is to ensure that the hash generated by the verification software matches that which is contained in the digital signature and that the key issued by the university matches the one incorporated into the digital signature. For future work, the proposed model will be implemented and adopted in selected educational institutions. It will be further extended to be based on smart contracts.

Acknowledgment

This research is funded by the University Research Grant Project no. 13560 (2016). The authors would like to thank Universiti Utara Malaysia and Ministry of Higher Education for supporting this research.

References

[1] M. Warasart and P. Kuacharoen, “Paper-based Document Authentication using Digital Signature and QR Code,” no. Iccet, 2012.

[2] Z. Chen, “Anti-Counterfeit Authentication System of Printed Information Based on A Logic Signing Technique.”

[3] S. Balasubramanian, R. Prashanth Iye, and S. Ravishankar, “Mark sheet verification,” *2009 3rd Int. Conf. Anti-counterfeiting, Secure. Identify. Commun. ASID 2009*, 2009.

[4] A. Singhal, “Degree Certificate Authentication using QR Code and Smartphone,” vol. 120, no. 16, pp. 38–43, 2015.

[5] T. Healy, S. Cote, J. Helliwell, and S. Field, “The Well-Being of Nations - The Role of Human and Social Capital,” *Oecd*, p. 118, 2002.

[6] S. Baum, S. Baum, and J. Ma, “Education Pays 2010 The Benefits of Higher Education for Individuals and Society," Baum Ma Payea 2010.pdf,” 2013.

[7] S. Marginson, Dynamics of national and *global competition in higher education*, vol. 52, no. 1. 2006.

[8] S. Baum, “Higher Education Earning Premium Value, Variation, and Trends,” *Urban Inst.*, no. February, pp. 1–12, 2014.

[9] M. G. Moore, “A Sad Reminder That Diploma Mills Are Still With Us,” *Am. J. Distance Educ.*, vol. 23, no. June, p. 175-178--, 2009.

[10] G. Grolleau, T. Lakhal, and N. Mzoughi, “An introduction to the Economics of Fake Degrees,” *J. Econ. Issues*, vol. 42, no. 3, pp. 673–693, 2008.

[11] E. Ben Cohen and R. Winch, “Diploma and accreditation mills: New trends in credential abuse,” 2011.

[12] E. Chiyevo Garwe, “Qualification, Award and Recognition Fraud in Higher Education in Zimbabwe,” *J. Stud. Educ.*, vol. 5, no. 2, pp. 119–135, 2162.

[13] Association of Certified Fraud Examiners, “Report to the Nation on Occupational Fraud & Abuse,” *Glob. Fraud Study*, pp. 1–92, 2016.

[14] N. M. Musee, “An Academic Certification Verification System Based On Cloud Computing Environment,” 2015.

[15] E. Share, M. Memorable, and L. They, “Fifty-eight Percent of Employers Have Caught a Lie on a Resume,” 2014.

[16] X. Technologies, “Blockchain imperative for educational certificates,” *Xanbell Technologies*, 2017.

[17] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, *Where is current research on Blockchain technology? - A systematic review*, vol. 11, no. 10. 2016.

[18] A. Roehrs, C. A. da Costa, and R. da Rosa Righi, “OmniPHR: A distributed architecture model to integrate personal health records,” *J. Biomed. Inform.*, vol. 71, pp. 70–81, 2017.

[19] R. Arendsen, M. J. Ter Hedde, and H. Hermsen, *Electronic Government*, vol. 6846. 2011.

[20] H. Hou, “The application of blockchain technology in E-government in China,” *2017 26th Int. Conf. Comput. Commun. Networks, ICCCN 2017*, 2017.

[21] J. Sidhu, “Syscoin : A Peer-to-Peer Electronic Cash System with Blockchain-Based Services for E-Business,” 2008.

[22] N. Smolenski and D. Hughes, “Academic Credentials In An Era Of Digital Decentralization Academic Credentials In An Era Of Digital Decentralization Learning Machine Cultural Anthropologist contents preface,” 2016.

[23] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” *Www.Bitcoin.Org*, p. 9, 2008.

[24] Nomura Research Institute, “Survey on Blockchain Technologies and Related Services,” 2016.

[25] S. Thompson, “The preservation of digital signatures on the blockchain - Thompson - See Also,” *Univ. Br. Columbia iSchool Student J.*, vol. 3, no. Spring, 2017.

[26] C. F. Bond, F. Amati, and G. Blousson, “Blockchain, academic verification use case,” 2015.

[27] J.-F. Blanchette, “The digital signature dilemma Le dilemme de la signature numérique,” *Ann. Des Télécommunications*, vol. 61, no. 7, pp. 908–923, 2006.

[28] MIT Media Lab, “What we learned from designing an academic certificates system on the blockchain,” *Medium*, no. December, p. 2016, 2016.

[29] P. Schmidt, “Certificates, Reputation, and the Blockchain,” *MIT Media Lab*, 2015.