Certificate Verification System Based on Blockchain Technology

Thin Zar Ko Ko
University of Computer Studies, Hinthada
thinzarkoko.rzk@gmail.com

Abstract

One of the most important documents is certificates for graduates from universities and other educational institutions. A certificate is a certificate of qualification for a graduate that is used for a job or other matters relating. Advancement of IT and low cost and high quality office supplies on the marketplace have contributed to the development of essential documents such as certificates, identification cards and passports. However, it is costly and time consuming to check certificates using traditional methods. The aim of this paper is to introduce a theoretical model, which can give the possible solution for the issue and verification of academic certificates using blockchain based. There are many functions such as hash, public and private key cryptography, digital signatures, peer-to-peer networks and work evidence in blockchain technology. The models formulate a system divided into two principal processes using different elements, namely the issuance of a digital certificate of academic signature and the academic certificate verification. The paper proposed to use blockchain technology to validate university certificates. This meets all the criteria for a modern verification program for academic certificates. In addition, the new approach for confirming academic certificates validity fills up the gaps and challenges.

Keywords: Blockchain, Education, Verification, Digitalization

1. Introduction

Certificates distributed in schools or universities square measure largely within the form of hard copy. Whenever applicants apply for the task at any public or private sector they have to supply those hard copies, whereas the organizations ought to verify all certificates manually that is very time-consuming process and there are chances that some might need turn out the certificate that is not legitimate which could get unremarked by the verifier throughout the method as results of this ineligible candidate can get an opportunity. There had been various cases in past where people are caught selling fake certificates various organization at low value. To eradicate such problem and diminish the production of fake certificates we are able to use the blockchain technology. Blockchain can be used to store the data of the certificate that may be valid by anyone from anyplace.

2. Related Work

The goal of Blockchain Technology is to create a decentralized environment [9]. Because of its benefits, it has been implemented to be used in different fields. In the healthcare sector Blockchain has been implemented [1]. It is also applied in business [8], smart government [16] and e-government [5]. The main focus of the paper is the potential for blockchain in education. This paper is therefore intended to use blockchain for the verification of documents, in particular for certification of graduations. The technology of blockchain is an acceptable technology that authenticates learning results as well as protects shares [14]. With a robust decentralized framework which improves network durability due to the multiplicity of package duplicates, where the signatures are kept, the central authority has been changed by Public Key Infrastructure (PKI). Blockchain decentralization prohibits third parties, unless they remove the proof-of-work condition that has verified the blocks, from modifying or removing transactions. Blockchain technology uses a digital ledger that is incorruptible. This ledger will be used to record financial transactions and anything with or without economic interest. It technology was introduced in 2008 for Bitcoin and is now used in many fields [17]. A blockchain can identify certificate issuers and recipients. The public database (blockchain) holds document records (hash) worldwide on thousands of computers. In a single blockchain, digital certificates are secure and have important advantages over standard digital certificates. Anyone able to access the blockchain will authenticate their certificates with an open source app that is readily accessible. There is no longer need for third parties. Thereby, even after the company is dissolved or has no access to the given record, the certificate may be validated. If all copies on all the computers running software are lost, records and certificates received on a blockchain can be deleted. The hash connection is created and held by the user to the original text. The process requires the document signature to be published and does not require the document itself to be published. The confidentiality of records is protected by this process.

3. Blockchain Technologies

The blockchain is an emerging technology as well as many functions such as public and private key cryptography, hash, peer-to-peer networks and digital signatures. The followings explain each of them.

- **Public and Private Keys** – For coding and cryptography, public and private blockchain keys originate from the concept of generating entirely different keys. The approach used and involving the generation of a private key for personal use and a
public key for public use is perpetually the public-key cryptographic approach in blockchain as shown in Figure 1. This technique is discreet from the key cryptographic isobilateral technique, which is used to both encrypt and decrypt the similar key and when the delivery mechanism is safe for the applicable party [18]. Public key encryption allows secure file delivery and receipt only when both a private and a public key is produced by the party that certifies the document and the general public key is provided to the sender in advance. When the checking party controls the private key’s privacy, it maintains protection for the group action despite the fact that everyone has the public key.

Figure 1. The Public Key Encryption

- **Hash** – A hash is a short constant length code. Data entry into the hash-generator leads together with a correct number of digits to a hash from a document output. A unique identification code is created by hash. If the same data is inputted to hash generator, the hash value is the same. But even small input differences lead to completely different hash [13]. The execution of hash generation is shown in Figure 2. It is stated in Figure 2, that even a slight change in the data input takes place in a quite different hash. This feature of a hash is also accepted for the finding of data fraud and is accepted for verification purposes by a very blockchain technique.

- **Peer-to-Peer (P2P) Network** – This means the development of networks or computers which start sharing work or files and tasks with each other. In the network, peers are equal authorities and skills within the environment. Each user or computer on a P2P network is referred to as a node and is connected with a P2P node network.

- **Digital Signatures** – In order to construct the digital signature system to validate the authenticity of the data sent over the Internet, the hash as well as the public key cryptographic methods is used. The digital signature is created by encrypting the hash value of the file to the verifier with a general sender public key [4]. The file is also sent to the certificate authority on-line. To generate a hash value, the verifier uses the data in the package. Together, the verifier keeps its private key for decoding the digital signature and drawing the hash value. This means that the digital signature is valid if two hash values are duplicated and the data involved in the certificate was also not faked.

Figure 2. The Hash Generator

3.1 Blockchain's Development Potential

Technology via blockchain has the ability to speed up the elimination of a document based certificate system. To present, the use of digital certificates has been stopped from being falsified with ease. The blockchain enables organizations to grant indefinitely valid, unchangeable digital certificates because they are genuine against the blockchain. Such benefits with existing systems significantly increase the business model of digital certificates and would probably lead to the introduction of digital certificate. Software blockchain eliminates the need to verify certificates from educational organizations. Since blockchain certificates can be automatically scanned, education service providers do not need to fully commit any longer to that task [4].

Blockchain platform is perfect for protecting, sharing and authenticating educational objectives [4]. PKI, with a highly stable decentralized structure, is replacing the central authority and improving network durability as many block duplicates store the signatures. Decentralization of blockchain prevents the modification or the elimination of block transactions, if the conditions of proof-of-work which had been checked do not go unnoticed. Blockchains do have independent time stamping, thereby improving privacy.

In situations where certificates can expire, having a reliable time stamp is critical. In response to a key leak, the generator must also rotate issuing keys on a regular basis for privacy. In deciding whether the record was published within the validity of the key by a different issuer, an independent time stamp is required. In comparison to other PKI schemes, file format signatures are independent of blockchain. Any document can use the same signature software irrespective of its proprietary standards [4].

4. Work on the proposal

Universities have long advanced to accommodate a huge increase within the school base, student base and various relevant institutions. It is an enormous task for
university officers and workers to face practical challenges and arrangement of services for massive students and graduate communities. Deliberately, the file service given to the network of educators and graduates has begun to act on the standard created by encrypting the hash value. In universities, several more causes have resulted in reduced functional authority in student affairs. The verification method for academic certificates and connected documents is one of the most important reasons that have negative result to university services. The built model shown in Figure 3 wants to use blockchain technology for degree certification validation. The newest blockchain technology is that can explain for individual employers and students the authentication process of educational qualifications.

![Figure 3. Flow of System](image)

Despite educational qualifications, getting a white-collar career is unlikely. Companies must provide evidence of academic credentials to new graduates. Students who wait for certificates are validated by university certification. Verification takes a lot of time because it normally takes days or even weeks. Job seekers and companies, with impeccable expertise and skills, expend their precious time arranging testing with the relevant universities to receive their best workers. The verification of documents is difficult but important for the legitimacy of the applicant, whether in the area of education, employment or visas. The blockchain is now the newest model to modify both job seekers and students’ authentication procedures for educational credentials. Blockchain technology permits users to store essential documents as cryptographically signed digital certificates such as academic certificates. These digital documents facilitate data protection and file sharing for recruitment or admission with employers or other authorities. This unquestioned technological trend involves issuing authorities to supply a blockchain network with digital certificates. Their storage takes the form of a single hash code [3]. When a company requires a copy from a job applicant, the educational institution can obtain academic credentials or documents via its blockchain. This student will give the public key to the university he or she graduated from. An applicant must submit their digital educational qualifications with the potential employer.

Blockchain principles indicate that this composite technology contained a large number of existing functions, including hash, public and private cryptography, digital signatures, peer-to-peer networks and proof of labor, already analyzed during the previous section. The block which is classified into two teams during this paper consists of the issuance of a digitally signed academic certificate and the certificate verification is associated with the truthfulness of components. Figure 3 shows sophisticated statistical design.

### 4.1 Digitally Signed Academic Certificate Issuance

The academic association is in the first place to digitally issue a signed certificate. This paper aims to victimize the blockchain as explained in Figure 3 using the following ideas.

- **Generation of hash** – This paper approves the use of the hash generation program SHA-256 to get hashes due to its truth and research, which is an online open source tool that could produce the SHA-256 hash of any data set.

- **Public and Private Keys** – This built model uses private and public keys together throughout this paper. The university must have public key. In turn, the university issues the student a private key that is credible.

- **Digital Signatures** – A unit is used for the construction of a digital signature mechanism to confirm the accuracy of information sent over the internet, both hash and public key cryptographic strategies. The digital signature is sent to the verifier with the general sender public key, according to the analysis administrated in [7]. The verifier delivers file via on-line. The verifier uses the data stored in the file to construct a hash value. The verifier also keeps its private key for decrypting and drawing the hash value of the digital signature in that matter. This means that the digital signature is real if the two hash values match and the data involved in the certificate have not been faked.

- **Timestamping** – It applies to the digital university certificate another security layer. This model helps the peer-to-peer network system issue a digital form attached to the document, which confirms the accuracy of the day, month and year when a digital
certificate is issued. The key to timestamp generation is to analyze the time taken to obtain digital signatures, as an information block which is then encrypted to obtain a code indicating the date the document was issued and a digital certificate on it.

- **Signing of the Document Digitally** – Four elements consisting of (i) hash generated by hash generator, (ii) public key, (iii) private key and (iv) timestamps indicating the accuracy of time the certification is issued. The model's digital signature is combined with the models. The document recognizes the signature by combining a hash produced with a private key issued to the student to generate one unique digital signature code. This code is combined with timestamps to unique a single digital signature, which is then indicated in the paper. In addition, the signature is secured by a combination of hash, private/public keys and timestamps. The signature is therefore unique to the document issued to the student and may only be decrypted using the private key held by the student. Private student key can never be decrypted by conversational digital signature engineering. If only a tiny part of the document at the end of the day changes illegally and generates a completely new hash value.

- **Certificate issuance and hosting** – Both a paper copy of the certificate and a digitally signed student document are given. Using a hash generator, the university provides a hash of the final document signed. This hash is a unique alphanumeric string, which with the certificate and its content no one has illegally modified. Then, the hash is stored on the blockchain, and a record is created that states that the certificate was issued to the abovementioned graduate at this time.

### 4.2 Academic Certificate Verification

The employer may want to know the validity of the university certificate when students apply for a job. The steps listed in this paper demonstrate that the digital signature in table 1 is verified and validated.

#### Table 1. Digitally signed document issuance

<table>
<thead>
<tr>
<th>Step No</th>
<th>Specific details</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Education groups can easily access public keys in public directories or internet. They may also be provided by the graduates to the employer.</td>
</tr>
<tr>
<td>2</td>
<td>The employer is scanning and inputting the digitally signed document and the public key through verification software.</td>
</tr>
<tr>
<td>3</td>
<td>Software for verification uses digital signature and a public key for hash generation.</td>
</tr>
<tr>
<td>4</td>
<td>Software for verification generates hash comparisons of the original certified copy file.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step No</th>
<th>Specific details</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>In addition, the verification software tests if the digital signature is connected to the university's general public key.</td>
</tr>
<tr>
<td>6</td>
<td>Both steps should display students’ private keys without being demanded.</td>
</tr>
<tr>
<td>7</td>
<td>When all conditions are valid, the verification software must inform the future employer of the legal validity of the certificate.</td>
</tr>
<tr>
<td>8</td>
<td>If any or both conditions are false, the software for the verification generates an output to inform the future employer that the certificate is not legal.</td>
</tr>
</tbody>
</table>

### 5. Conclusion

Within this paper, an improvement of the verification process was proposed as a blockchain model for graduation certificate verification. The occurrence of certificate falsifications will thus be reduced and the confidentiality, security and validity of certificates will be increased. To authorizing authorities, receivers and customers alike, this paper provides several advantages. The benefit of this paper is that the blockchain itself contains all information needed to verify and validate the certificate. The job applicant does not need to contact the university to verify the certificate. It is only necessary to ensure that the hash generated through the validation software fits with the digital certificate and that the university’s key corresponds to the key included in the digital signature. This paper in selected academic institutions would be applied and adapted for future research. This will be expanded further to include smart contracts.

### References