International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue V, May 2019- Available at www.ijraset.com

Smart Contract for Digital Certificate using Blockchain Technology

Neethu Gopal[1], Vani V Prakash[2]
[1]*M.Tech, Computer Science & Engineering, Sree Buddha College of Engineering, Kerala, India.*
[2]*Assistant Professor, Computer Science & Engineering, Sree Buddha College of Engineering, Kerala, India.*

Abstract: ***The graduation certificate forgery has become a major problem in now a days and the lack of effective anti-forge mechanism, In order to solve the problem of counterfeiting certificates, the digital certificate system based on blockchain technology would be introduced. The system generate the electronic file of a paper certificate accompanying other related data into the database and calculates its hash value. It then store the hash value into the block in the chain system. The system will create a related QR-code and inquiry string code to affix to the paper certificate, this will verify the authenticity of the paper certificate through mobile phone scanning or website inquiries. By integrating the features of blockchain, the system improves the efficiency operations at each stage.***
Keywords: Blockchain, Digital Certificate, Ethereum, Hashing, Consensus

I. INTRODUCTION

Graduation certificates and transcripts contain information confidential to the individuals and should not be easily accessible to others. Hence, there is a high need for a mechanism that can guarantee that the information in such a document is original, which means that document has originated from an authorized source and is not fake. In addition, the information in the document should be confidential so that it can only be viewed by authorized persons. Blockchain technology is used to reduce the incidence of forgeries of certificates and to improve the safety, validity and confidentiality of graduation certificates. Technologies exist in related domains, such as digital signatures, which are used in e-documents to provide authentication, integrity, and non-repudiation. However, for the requirements of an e-qualification certificate, it has critical security holes and missing functions: for example, it uses the keys to verify the modification of the document, but doesn't start the validation of the public key certificates' status automatically. This may result in a forgery being accepted if the key has been compromised. Furthermore, even the signer's public key certificate has been validated, but the signed document itself hasn't. In our case of an e-qualification certificate, the signed document itself is also a certificate, which may have a valid period (e.g. The problem we are dealing with is a certificate issue), therefore, a simple digital signing of the document alone doesn't solve the problem. So the unmodifiable property of the block chain helps to overcome the problem of certificate forgery. Data security is one of the major features of blockchain technology [1]. The process of certificate application and automated certificate granting are open and transparent in the system.

Advances in information technology, the wide availability of the Internet, and common usage of mobile devices have changed the lifestyle of human beings. Virtual currency, digital coins originally designed for use online, has begun to be extensively adopted in real life. Because of the convenience of the Internet, various virtual currencies are thriving, including the most popular—Bitcoin, Ether, and Ripple[2]—the value of which has surged recently. People are beginning to pay attention to blockchain, the backbone technology of these revolutionary currencies. Blockchain features a decentralized and incorruptible database that has high potential for a diverse range of uses. Blockchain is a distributed database that is widely used for recording distinct transactions. Once a consensus is reached among different nodes, the transaction is added to a block that already holds records of several transactions. Each block contains the hash value of its last counterpart for connection. All the blocks are connected and together they form a blockchain. Data are distributed among various nodes (the distributed data storage) and are thus decentralized. Consequently, the nodes maintain the database together. Under blockchain, a block becomes validated only once it has been verified by multiple parties. Furthermore, the data in blocks cannot be modified arbitrarily.

A blockchain-based smart contract, for example, creates a reliable system because it dispels doubts about information's veracity. Information technology has developed rapidly in recent years, data protection is more necessary than ever. Graduates, whether they choose to continue studying or start job hunting, require various certificates for interviews. However, they often find that they have lost their educational and commendation certificates. Reapplying for hard copies can be time-consuming because certificates are granted by different organizations and in person application may be necessary. By contrast, applying for an e-copy can save paper and time. By providing information for identity verification, graduates are able to apply for any certificate easily. Nevertheless,

because of this convenience, forged degree certificates, licenses, and certificates are prevalent. Consequently, schools and companies cannot instantly validate the documents they receive[3]. To solve this problem, a certificate system based on blockchain was designed in this study. Data are stored in different nodes, and anyone who wishes to modify a particular internal datum must request that other nodes modify it simultaneously. Thus, the system is highly reliable.

II. SYSTEM OVERVIEW

A. *Existing System*

The E-certificate is a new concept to issue certificate to qualified candidates. Fast delivery a specialty of the E-certificate. There are two ways to deliver the E-certificate to a qualified candidate – a) through email or b) through log-in area on institution's website or portal. E-certificate is secured document as it is embedded in the lates technology and management tools available. it contains unique E-certificate number, Photo of concerned qualified candidate, online verification system for each candidate. The system is a good solution to minimize the limitation of paper based certificate's verification as this is fast and safe. To avoid the possibility of theft, no need to transfer/post the original document. But there are security issues concerns about the data stored in it.

B. *Drawbacks of Existing System*

Because information technology has developed rapidly in recent years, data protection is more necessary than ever. Graduates, whether they choose to continue studying or start job hunting, require various certificates for interviews. However, they often find that they have lost their educational and commendation certificates. Reapplying for hard copies can be time-consuming because certificates are granted by different organizations and in-person application may be necessary. By contrast, applying for an e-copy can save paper and time. By providing information for identity verification, graduates are able to apply for any certificate easily. Nevertheless, because of this convenience, forged degree certificates, licenses, and certificates are prevalent. Consequently, schools and companies cannot instantly validate the documents they receive.

C. *Proposed System*

The proposed system title is "Smart contract for Digital certificate using blockchain technology**".** In order to solve the problem of counterfeiting certificates, the digital certificate system based on blockchain technology would be proposed. The digital certificate with anti-counterfeit and verifiability could be made through the unmodifiable property of blockchain. In the system, three groups of users are involved. Schools or certification units grant certificates, have access to the system, and can browse the system database. When students fulfilled certain requirements, the authorities grant a certificate through the system. After the students have received their certificate, they are able to inquire about any certificate they have gained. The service provider is responsible for system maintenance. Instead of sending conventional hard copies, schools grant e- certificates containing a quick response (QR) code to the graduates whose data have been successfully verified. Each graduate also receives an inquiry number and electronic file of their certificate. When applying for a job, a graduate simply sends the register number or e-certificate with a QR code to the target companies. The companies send inquiries to the system and are informed if the serial numbers are validated. The QR code enables them to recognize if the certificate has been tampered with or forged.

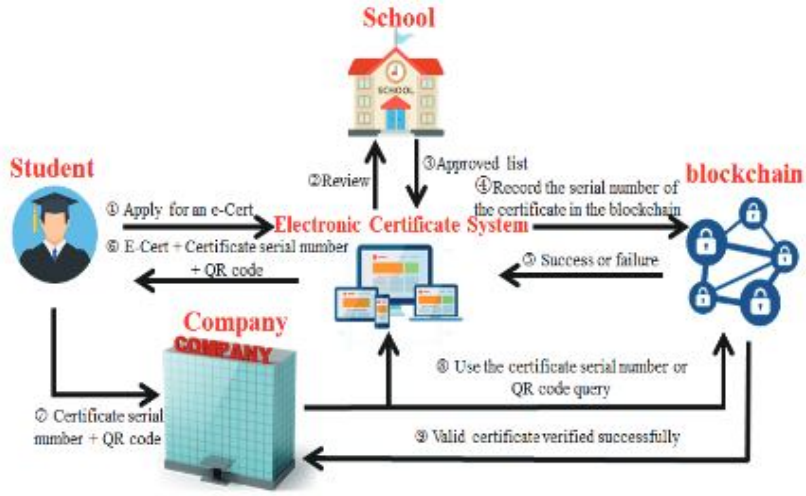

Fig 1: Architecture of the system

D. Advantages of Proposed System

A few features of an e-degree as compared to a paper degree:

1) E-degree is very fast to generate
2) High security is guaranteed with multiple authentications and encryption schemes
3) Blockchain technology is used to protect the certificate from modification
4) No longer have to wait for several weeks or months for the certificate to be mailed
5) After reception of the certificate the candidate can print it immediately or resend it through email to their potential employers/institutions
6) The candidate can print as many copies of the e-degree as it may be required for presentation purposes
7) E-Certificate is a soft file which does not require paper, for its production. In other words it saves paper consumption and in other word saves trees.

III.SYSTEM DESIGN

A. Modules and their functionalities

The blockchain based digital certificate system consist of four modules:

1) Student
2) University
3) Admin
4) Company

B. Student

The proposed system mainly consist of three users and the student is one among them. The Student module include the registration and application for e-certificate to the system. Once a student is registered, then he/she can apply for the e-certificate through the system by making proper payment through online. Then they can download their certificate from their corresponding student profile. They must give a valid digital signature send by the university to open and download the certificate from the system. The signature is send by the university at the time of issuing certificate to the student. In addition to the certificate a unique serial number, certificate number and a QR code is also obtained along with this. Later the student can use these information to prove their genuinity.

C. University

The main part of the proposed system is university module. The registered universities will add their students to the database. In the university registration phase the university will upload details like their emblem, sign of controller and vice chancellor, seal etc. These details are used for the certificate generation. The student database management is done here by adding details of students to the university, they can update the data and mark information of each student. The university can approve or reject the request send by the student. The university will generate a QR code and a unique serial number and certificate number to the approved list of students. The certificate number is a combination of the course, date of issuing and register number of the student. Then the QR code is generated for the certificate number using a QR code generation algorithm.

D. QR Code generation

QR code (abbreviated from Quick Response Code) [4] is the trademark for a type of matrix barcode (or two-dimensional barcode) first designed in 1994 for the automotive industry in Japan. A barcode is an optical label readable by a machine containing information about the item it is attached to.

QR code (abbreviated from Quick Response Code) is the trademark for a type of matrix barcode (or two-dimensional barcode) first designed in 1994.The Quick Response system became popular outside the automotive industry due to its fast readability and greater storage capacity compared to standard UPC barcodes. Applications include product tracking, identifying items, time tracking, managing documents and general marketing.

A QR code consists of black squares arranged in a square grid on a white background that can be read by a camera like imaging device, and processed using Reed–Solomon error correction until the image is properly interpreted. The required data is then extracted from patterns that are present in both horizontal and vertical components of the image.

QR codes have become common in consumer advertising. A smartphone is used as a QR code scanner, displaying the code and converting it to some useful form (such as a standard URL for a website, thereby obviating the need for a user to type it into a web

browser). QR code has become a focus of advertising strategy as it gets a way to provide access to a brand's website more quickly than by manually entering a URL. The importance of this capability is that it increases the conversion rate beyond the mere convenience of the consumer: the chance that contact with the advertisement will convert to a sale. It coaxes interested prospects further down the conversion funnel with little delay or effort, bringing the viewer to the advertiser's website immediately, where a longer and more targeted sales pitch may lose the viewer's interest.

Although initially used to track parts in the manufacture of vehicles, QR codes are used across a much wider range of applications. These include commercial tracking, ticketing for entertainment and transport, product and loyalty marketing and product labelling in-store. Examples of marketing include where a company's discounted and percentage discount can be captured using a mobile app's QR code decoder or storing a company's information.

The process (and high-level algorithm) for generating a QR Code symbol [4] is as follows:

1) Choose the text (Unicode string) or binary data (byte string) to encode.
2) Choose one of the 4 error correction levels (ECL). A higher ECC level will yield a barcode that tolerates more damaged parts while preserving the payload data, but will tend to increase the version number (i.e. more modules in width and height).
3) Encode the text into a sequence of zero or more segments. A segment in byte mode can encode any data, but using alphanumeric or numeric mode is more compact if the text falls into these subsets.
4) Based on the segments to be encoded and the ECL, choose a suitable QR Code version to contain the data, preferably the smallest one.
5) Concatenate the segments (which have headers and payload) and add a terminator. The result is a sequence of bits.
6) Add padding bits and bytes to fill the remaining data space (based on the version and ECL).
7) Reinterpret the bit stream as a sequence of bytes, then divide it into blocks. Compute and append error correction bytes to each block. Interleave bytes from each block to form the final sequence of 8-bit code words to be drawn.
8) Initialize a blank square grid based on the version number.
9) Draw the function patterns (finders, alignment, timing, version info, etc.) onto the appropriate modules. This is formatting overhead to support the QR Code standard, and does not encode any user data.
10) Draw the sequence of (data + error correction) code words onto the QR Code symbol, starting from the bottom right. Two columns at a time are used, and the scanning process zigzags going upward and downward. Any module that was drawn for a function pattern is skipped over in this step.
11) Either manually or automatically choose a mask pattern to apply to the data modules. If masking automatically, then all 8 possibilities are tested and the one with the lowest penalty score is accepted. Note that the format information is redrawn to reflect the mask chosen.
12) We are now finished the algorithmic parts of QR Code generation. The remaining work is to render the newly generated barcode symbol as a picture on screen, or save it as an image file on disk.

A digital signature is generated for each student using DES algorithm. At the time of issue of the e-certificate this signature is also send to the student via email. The student need to upload the respective signature to download the certificate from the system, this will add more security. The algorithm used to generate the digital signature is explained below:

E. Data Encryption Standard (Des)

DES has been found vulnerable against very powerful attacks and therefore, the popularity of DES has been found slightly on decline. DES is a block cipher, and encrypts data in blocks of size of 64 bit each, means 64 bits of plain text goes as the input to DES [6], which produces 64 bits of cipher text. The same algorithm and key are used with minor differences for encryption and decryption. The length of key is 56 bits. Actually, the initial key consists of 64 bits. However, every 8th bit of the key is discarded before the DES process even starts to produce a 56 bit key. That's the position of the bit 8, 16, 24, 32, 40, 48, 56 and 64 are discarded. Thus, the discarding of every 8th bit of the key produces a 56-bit key from the original 64-bit key.

DES is based on the two fundamental attributes of cryptography: substitution (also called as confusion) and transposition (also called as diffusion). DES consists of 16 steps, each of which is called as a round. Each round performs the steps of substitution and transposition.

Steps in DES

1) In the first step, the 64 bit plain text block is handed over to an initial Permutation (IP) function.
2) The initial permutation performed on plain text.

3) Next the initial permutation (IP) produces two halves of the permuted block; says Left Plain Text (LPT) and Right Plain Text (RPT).
4) Now each LPT and RPT to go through 16 rounds of encryption process.
5) In the end, LPT and RPT are rejoined and a Final Permutation (FP) is performed on the combined block
6) The result of this process produces 64 bit cipher text.

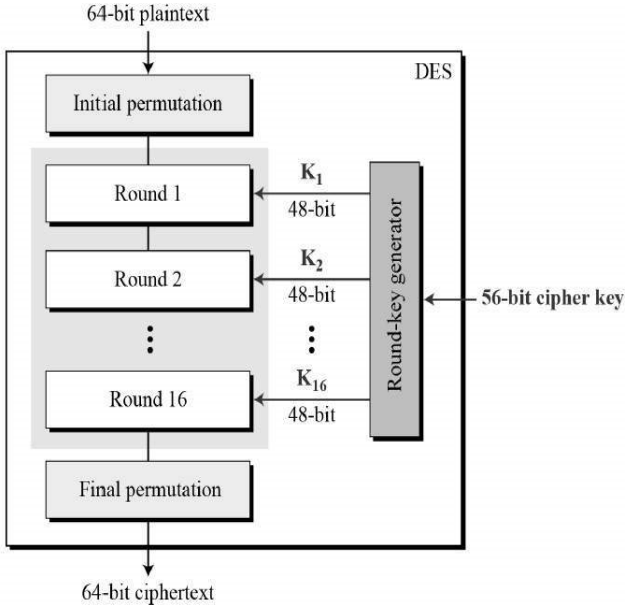

Fig 2: DES Structure

F. Crystal Report

The E-certificate is generated using a tool called crystal report. Crystal Reports [7] enables users to design and report the layout of data connection(s) graphically. In the Database Expert, users can select and link tables from a wide variety of data sources, including MicrosoftExcel spreadsheets, Oracle databases, MicrosoftSQLServer databases, MicrosoftAccess databases, Business Objects Enterprise business views, and local file-system information. Report designers can place fields from these sources on the surface of report design, and can also deploy them in custom formulas (using either BASIC or Crystal's own syntax), which are then placed on the design surface. Formulas can be evaluated as specified by the developer at several phases during report generation. Both fields and formulas have a wide range of formatting options available, which can be applied absolutely or conditionally by designers. It is possible to group the data into bands, each of which can be further split and suppressed conditionally as necessary. Crystal Reports also supports sub-reports, graphing, and a limited number of GIS features. At the time of preview the certificate generated by this is protected again using a password validation. The password used for this is the date of birth of the student.

G. Admin

The admin has an overall control on the management of the system. University management involves addition of new universities and their details into the system, can update and delete information regarding the existing ones. Such existing universities can thus login to the system for the any kind of updations. Then the most important portion in the proposed system blockchain protection is done here. A blockchain is created for the students whose certificate are issued. There are three types of blockchain. They are private, public and consortium blockchain. The Consortium or Federated Blockchain is a hybrid of the Public and Private Blockchain. It is partly decentralized. The consensus process is controlled by a pre-selected set of nodes, for instance, financial institutions. SHA 256 is the algorithm used to compute hash for blocks in the blockchain.

H. SHA 256

NIST (The National Institute of Standards and Technology) standard specifies the adoption secure hash algorithms such as SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512 [5]. Hash Function algorithms are used during data transmission to produce the message digest. Therefore, it becomes an essential tool for embedded security in e-mail, internet banking, and other applications. A hash function takes an arbitrary-length message input to produce a fixed-length output. A hash function is a one-way hash function; it is difficult to invert a hash value to a message input. Furthermore, it is computationally infeasible to find a message that produces

the same hash value. These properties become an important aspect to ensure that a hash function can work properly.SHA-2 consists of four different types of hash functions such as SHA-224, SHA-256, SHA-384, and SHA-512. The output length of these hash algorithms depends on the SHA-2 length ranging from 256 to 512-bit. In this paper, the SHA-256 hash function has been designed. This section describes the SHA-256 algorithm together with the block diagram of this algorithm. Each SHA-256 algorithm can be divided into two stages: pre-processing and hash computation. Pre-processing involves padding a message and parsing the padded message into m-blocks. Initialization values are set to be used in the hash computation. Hash computation produces a message schedule from the padded message. The output hash value generated by hash computation is used to determine the message digest. Hash computation comprises message schedule, functions, constants and word operations that are generated iteratively in order to obtain a hash value. The security of SHA-256 hash function depends on the size of the hash value. The first step of the SHA-256 hash function is pre-processing; the input message is padded. The process of padding the message starts after getting the message input, and a single 1-bit is added at the end of the message. Then, it is followed by n 0-bit until the length of the message is congruent to 448 modulo 512. The last 64-bit is reserved for calculating the length of the message. Thus, the overall message input is 512-bit.

I. Company

The company can login to the system to verify the genuinity of the graduation certificates and documents of the candidates in the recruit list using the register number/serial number/certificate number of the candidate. The company will firstly search and send a request to access the blockchain for the chosen candidate. On reception of the request the admin will verify the company and send an encrypted key to access the blockchain, which is send via email to the company mail. This key is generated randomly using Base64 encoding. The secret key is used to check whether the certificate is in the blockchain or not. If present the certificate is valid.

J. Base 64 Encoding

Base64 is a group of binary-to-text encoding schemes that represent binary data in an ASCII string format by translating it into a radix-64 representation. The term Base64 originates from a specific MIME content transfer encoding. Each Base64 digit represents exactly 6 bits of data. Three 8-bit bytes (i.e., a total of 24 bits) can therefore be represented by four 6-bit Base64 digits. Common to all binary-to-text encoding schemes, Base64 is designed to carry data stored in binary formats across channels that only reliably support text content. The particular set of 64 characters chosen to represent the 64 place-values for the base varies between implementations. The general strategy is to choose 64 characters that are both members of a subset common to most encodings, and also printable. This combination leaves the data unlikely to be modified in transit through information systems, such as email, that were traditionally not 8-bit clean. For example, MIME's Base64 implementation uses A–Z, a–z, and 0–9 for the first 62 values. Other variations share this property but differ in the symbols chosen for the last two values. The earliest instances of this type of encoding were created for dialup communication between systems running the same OS — e.g., uuencode for UNIX, BinHex for the TRS-80 (later adapted for the Macintosh) — and could therefore make more assumptions about what characters were safe to use. For instance, uuencode uses uppercase letters, digits, and many punctuation characters, but no lowercase.

IV. RESULT AND ANALYSIS

This section discusses the experimental results of the smart contract for digital certificate based on blockchain technology. The system that uses the operating system for windows 10 and windows platforms here is c#.net. And the database created is a SQL server. The proposed system is using synthetic data for results assessment. Synthetic data is developed data. The synthetic data is created to attain specific needs or specific criteria that may not be establish in the original real data. Synthesizing data is very helpful for designing any type of system because this data can be used as a simulation. The proposed system is implemented using four modules and different sub-modules.

The administrator has a whole control over the system especially blockchain processing. It manages various Universities, Blockchain by applying hashing and rehashing and can approve Company requests. The main part is the Blockchain protection phase. It includes blockchain creation and validation at each stage. The blocks are created for every students for securing their certificates. SHA256 algorithm is used for hashing in blockchain. For e-certificate generation Crystal Report is used. The details for the certificates are collected from the corresponding student database and from the university database. Only after the certification generation blockchain protection is done. Also the companies can use the system to verify the genuinity of the graduation certificates and documents of the candidates in the recruit list using the register number of the candidate by checking whether there is a block for the student exist in the blockchain or not. Various cryptographic algorithms are used in different stages like DES for creating digital signature, QR code generation algorithm etc.

The analysis of the proposed system performed are:

1) Time complexity for DS generation
2) Blockchain scalability
3) Blockchain performance

The time complexity for generating digital signature increases with increase in file size, here the size of all files are similar because all contains the same details but the contents are different for different students. The result shows in fig 3. The scalability of blockchain shows that the time complexity for blockchain creation increases with increase in number of records and storage space used. The result is shown in fig 4. Blockchain performance determines the efficiency of different SHA algorithms for hashing. The result is shown in fig 5.

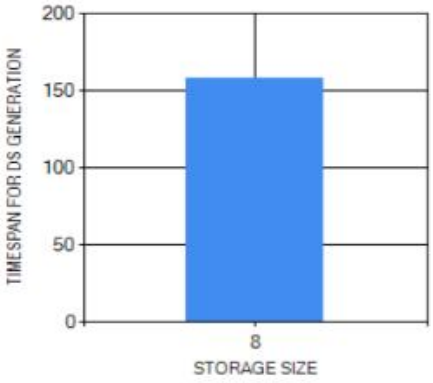

Fig 3: Time complexity for DS generation

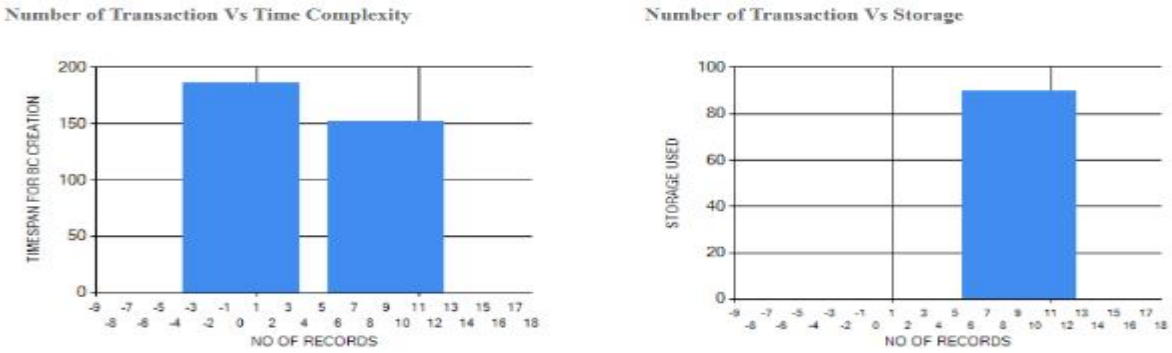

Fig 4: Blockchain scalability

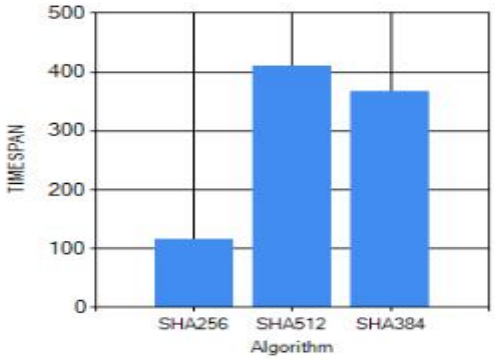

Fig 5: Blockchain performance

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue V, May 2019- Available at www.ijraset.com

V. CONCLUSIONS

Various technologies has been discussed to reduce the incidence of certificate forgeries and ensure that the security, validity and confidentiality of graduation certificates, even though there are many limitations regarding the security and privacy of data. The proposed blockchain-based system reduces the certificate forgery. Automated certificate granting are open and transparent in the system. Companies or organizations can thus inquire for information on any certificate from the system. Thus the system prevents document forgery and provides accurate and reliable information on digital certificates.

As a future work the work can be extended to design on a building platform like ethereum so that it will be more easy to manage and help to detect and prevent attacker attempts before they take place, which will reduce the number of document forgery in every sector.

REFERENCES

[1] Tengyu Yu, Blockchain operation principle analysis: 5 key technologies, iThome, https://www.ithome.com.tw/news/105374
[2] Jingyuan Gao, The rise of virtual currencies! Bitcoin takes the lead, and the other 4 kinds can't be missed. Digital Age,https://www.bnext.com.tw/article/47456/bitcoin-ether-litecoin-ripple-differences-between-cryptocurrencies
[3] Weiwei He, Exempted from cumbersome auditing and issuance procedures, several national junior diplomas will debut year.iThome,https://www.ithome.com.tw/news/119252
[4] Qr code generation Algorithm, https://www.nayuki.io/page/qr-code-generator-library
[5] SHA 256 Algorithm, https://en.bitcoinwiki.org/wiki/SHA-256
[6] DES, https://www.geeksforgeeks.org/computer-network-data-encryption-standard-des-set-1/
[7] Crystal Report, A report generating tool:https://en.wikipedia.org/wiki/Crystal_Reports