Metamorphosing the Education System: Instigating Blockchain Technology to Universities for Generating Tamper Proof Certificates

Sini V. Pillai*

Assistant Professor, CET School of Management College of Engineering Trivandrum, Thiruvananthapuram

Abstract

Education sector is transforming day by day in terms of technological advancements and complexity. One of the potential problem education system facing, specifically by the Universities is in delivering authentic degree certificates which cannot be forged by anyone else. Fake certificates are a big problem in India, where six million students graduate over every year. The paper supports to deliver a solution in generating tamper proof certificates through the implementation of Block Chain and Inter Planetary File System (IPFS) in the University system.

A process model is reengineered which uses ethreum block chain as the core engine with smart contracts enabled in it, incorporating the application of IPFS. University can save the file in the IPFS system and can save hash into the block chain for double verification by implementing unique hashing algorithm called SHA-256 and asymmetric encryption. The process and application of Block Chain technologies in Universities for delivering digitally authentic certificates without any hassle is explored.

Keywords: Block Chain, IPFS, Ethreum Block Chain, Encryption, Decryption

1. Introduction

It's quickly becoming deceptive that Block Chain technology is practically far more than just Bit coin through, government, healthcare, education, finance and other sectors advanced uses are seen every day. Basically, block chain is a decentralized dispersed digital ledger collectively preserved by a network of computers called nodes, resembling a huge record book shared among many people. In block chain technique, data cannot be altered by a person without everyone else who maintains the histories agreeing to the change — this makes it safe. Inter Planetary File System (IPFS), a p2p system which helps to connect all devices or nodes with respect to content. In certain standpoints, IPFS is comparable to the World Wide Web, but IPFS may be seen as solitary Bit Torrent group, exchanging matters inside one Git repository. IPFS combines dispersed hash table, an incentivized block exchange, and a self-verifying namespace. Adding certificates like sensitive contents in IPFS and block chain it becomes impossible to alter the data and helps in providing authenticity.

The document data will be added to block chain by the university in which the candidate have the access and give online resume and share with employers. The block chain provides a determined public record, protected against changes to the institute or impairment of its personal confidential records. Further, the system opens chances for direct awarding of certificates and emblems by reliable experts and teachers. The block chain grants public indication that a student identity obtained an award from a recognized identity, but does not, confirm the reliability of either party. A university could still grant a fake certificate or a student can still trickster in an exam. The block chain can solve the problem quickly and reliably checking the presentation of a degree, but not its cogency.

1.1 Research Problem

One of the major problem universities addresses is the validity of the degree certificates and making it a tamper proof one. Fake certificates are a big problem in India, where six million student graduates over every year. The companies hiring thousands of fresher's every year find it

*Email: sini.mba@cet.ac.in, sinivinu140905@gmail.com, Tel.: +919846569727

very difficult to verify the certificates and records of the prospective applicants and for the purpose they have to spend crores of rupees. A digital certificate based on block chain technology could report this problem. Block chain technology is a highly potential one to alter how the current centralized system is employed and helps to eradicate its major flaws, it helps to disperse the entire process and bring transparency to it. Block chain has got a lot of demand in the university or in education system; one of such thing is to deliver a fiddle proof certificates with proper authenticity.

1.2 Scope of the study

Block chain is a fresh and highly evolving technology which has got a vast potential in various fields such as finance, education sector, governance, healthcare, land associated documents etc. The study will help to comprehend the current problems in universities about the validity of degree certificates and how presentation of Block chain can develop the situation. It helps to detect the various options of Block chain in Education Sector. The study will help in bordering an appropriate method for execution of Block chain in University for digitalized degree certificate

1.3 Objective

To explore the possibilities of Block chain applications and to develop a model for its effective implementation in Universities for generating tamper proof certificate.

1.4 Research Methodology

Exploratory study is conducted here. Primary and Secondary data were collected for the study. Primary data collected using a structured interview schedule and secondary data was collected from various journals and other related areas relevant to this study and from case studies of already existing practices. Qualitative type of analysis is carried out for the study.

2. Review of Literature

There were several disadvantages of a distributed system including statement overhead and security issues which were linked in misusing system access by treacherous nodes (Tama et al., 2017). The Bit coin system is considered to be the very first Block chain that were linked together in convinced sized groups known as blocks, where the wedges were created through the authentication of each signature were by the third parties known as miners. Miners practice the authority of computation in reaching the cryptographic proof of authenticity of a business, and further make Bit coins from Bit coin system software in implementing a block (DuPont, 2014). Block chain incorporates a shackle of transactions, where fresh contacts are authenticated, and then presented to the end of the present chains of blocks (Forte et al., 2015). One-way hash/cryptographic mess functions relate a mathematical meaning to data, then to convert data of random size and further into a new digital thread of a predefined and secure length called a hash (Zobrist, 1970)(Knuth, 1974).

To convert any data of random size it is easy to use cryptographic hash function, which converts data into a hexa numbers called hash (Zobrist, 1970). The hash needs to be easy to calculate in one direction, from data to hash, but the contrary calculation, from hash to data needs to be as tough as possible.

Public key or asymmetric cryptography systems works by delivering a unique pair of key to each one on the system named a public key and a private key (Fujisaki & Okamaoto, 1999). In turn, applying the two different keys in exact way, in communication with the public and private keys of other users can disturb privacy and substantiation. For privacy, a sender encodes a message with the public key of the designed recipient, and then creates the encrypted note public (or sends it directly to the proposed recipient), who then decrypts message with their private key. For confirmation, a contributor encrypts a message with their private key, and then makes this encrypted note open. At this position, anyone can use the sender's public key to verify that the encrypted data were definitely created by the sender. This stroke of using a private key to encrypt a message and then creating the encrypted message public for the analysis of others is called a digital signature (Diffie & Hellman, 1979). As a result, the overall public key cryptography systems distinct secrecy (privacy) and authentication (digital signatures) are done through these two-different means.

Block chain technology has already been embraced by Sony Global Education and University of Nicosia (UNIC). Both Universities uses bit coin block chain technology to save the hashes. Sony global education uses Hyperledger

platform which is an open foundation collaborative effort created to improvement of cross-industry block chain skills to save the certificates and UNIC operates with the help of proof of existence website, a facility in securely storing an online dispersed proof of existence for every file. The documents are not stored in file or in the bit coin block chain but as a cryptographic summary of the file.

Block chain can be the transformational strength in education providing a provable, by far shareable and enduring evidence of educational chronicles and rewards (Sharples and Domingue, 2016). The unique essentials of the block chain are that it is a solitary linked record of digital actions stored on each contributing computer.

2.1 Development and Protection of Reliable Digital Records

Reliability and Authenticity

Reliability of records embarks on with the procedure of record formation stating who created the record and by what means they created. Record reliability is the standards for existing records management such as ISO 15,489 (ISO, 2001) and ARMA's Generally Recognized Recordkeeping Principles, ARMA International 2013, two most broadly established universal international recordkeeping principles for management of existing records.

Authenticity is trusting upon launching and conserving the identity and veracity of a record from its creation and thereafter (Rogers, 2015). When ordinal records are created they are often preserved for a period of time in the schemes that have engendered. Assuring reliability include measures such as access control, user substantiation, audits trails and certification that demonstrate the normal functioning, steady maintenance and regularity of upgrades of records system. These activities are also closely linked to standard IT Security controls indicating that preserving the safety of a system will facilitate ensuring the honesty of the data within it.

Long-term digital preservation

The records having sustained value to society or of historical significance needs phases of long-term conservation even from the start of their creation. Long-term preservation of material in digital form requires addressing permanency of authentic information. Quick changes to software, hardware, and network links to associated information and failure to imprisonment or loss of semantic evidence are taken into account.

Bit coin Block chain technology

A distributed transaction ledger where different nodes work together as a unique system for grouping of bits which is then encrypted as one block or one piece and bound together comprises the Bit coin Block chain technology. The first and disreputable application of the Block chain technology is Bitcoin, a form of digital crypto currency. Bit coin Block chain technology essentially establishes a distributed public ledger comprising the payment history of every Bitcoin in movement and provides proof of who possess what at any specified juncture. The distributed ledger is replicated on thousands of computers called Bit coin's nodes around the world and is openly available (The Economist, 2015).

Proof of Existence

This is a facility for anonymously and securely storing an online dispersed proof of existence intended for any file. The documents are not stored in file or in the bitcoin block chain; all they store is a cryptographic summary of the file, related to the time in which you submitted the document. In this way, you can later certify that the data been at that time. This is the first online service letting you to publicly prove that you have convinced information without revealing the data or yourself, with a regionalized certification based on the bitcoin network.

The main advantages are guarantee and privacy and help to get a decentralized proof which cannot be altered by any person. The document's existence is forever validated by the block chain even if this site is cooperated or down, so no need to hinge on or need to trust any central consultant. All previous data time stamping keys lack this freedom.

SHA-256

It is a cryptographic hash function of 'signature' for a text or data file. SHA-256 creates an unique 256-bit signature for a transcript. A hash is not 'encryption' as it cannot be decrypted back to the original text. This crafts it fit to relate 'hashed' versions of texts. Such applications include hash tables, veracity verification, challenge handshake verification, digital signatures, etc.

3. Analysis: Existing Practices of Issuing Degree Certificates in University System

To issue a certificate, University process starts with entering marks of the corresponding subjects for the respective semesters and is kept in universities private server. It is then moved to the default certificate template, after getting confirmation and approval. University employers have to spend huge money in order to verify the certificates as it is cross checked twice and thrice. It is then given for printing and further arranged by office labors to be sent straight to the students address by means of enumerated post. All the printing effort happens in the university itself. The price estimated for the printer is approximately 20-30 lakhs and upkeep charge includes ink and other printing resources which emanate another 20 lakhs. One of the main costs other than printer is for the paper and in order to safeguard the certificate with suitable genuineness a hologram may be provided in the certificate.

In order to design that much numbers of certificates it is really time consuming and the procedure after printing is multifaceted too. Proper precautions need to be taken care as it's highly confidential. It will take more than one month to print the certificates and the distribution will take more than a month to reach all the graduates. For every certificate to be send over post to the graduates, the cost accounts to twenty five rupee per envelope. Each year about forty thousands of students are passing out from different streams, different specialization and from different academies across the state, hence the price included is enormous which may account to 10 lakhs a year. So roughly total cost including manpower for the certificate issuing process in Universities will be around 40-50Lakhs per year. And above all, Bogus Certificates is a vast problem in India as these certificates can be easily replicated.

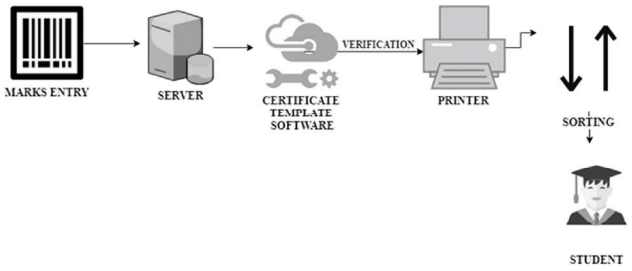

Figure 1: Existing process of issuing degree certificates in the University system

4. Possibility of Block Chain Applications in Universities

As education models evolve, technical innovation is predictable to diversify the ways in which tests are planned and individuals are estimated. Open and protected handling of academic data will become conceivable through the approval of application packages, leading to the appearance of new educational services in the upcoming. To study the possibility of block chain application, already executed real cases of Sony Global Education and University of Nicosia which applied Block chain in two different approaches is discussed.

4.1 Sony Global education

- Sony uses Hyper ledger which is an open foundation collaborative exertion created to advance cross-industry block chain technologies and updates its certificates in hyper ledger allowed block chain and uses it for authentication; this is done by giving Hyper ledger remuneration.
- Sony would let education and training administrations to donate data to the system and would bond together all education and training data about each individual and make it provable.
- Sony would make it possible for establishments with adequate permissions to analyse the data in order to recognize education and training tendencies among the population and to evaluate the efficiency of different education and training platforms.

4.2 University of Nicosia

- The document (PDF) is hashed with a protected hashing algorithm (SHA-256) and is encrypted. The Hash is kept to the Bitcoin transaction as enduring record with help of Proof of existence website.
- Can cross check the catalogue document or certificate with help of using the same SHA-256 algorithm and authenticate the diploma.

5. Implementation of Block Chain in University for Generating Tamper free Certificate

The marks entry is done with the help of a portal, which enables barcode scanning of paper and facilitates in the

entry of the marks. It is then transferred to the university private server. From the university private server it is transferred to certificate template software and is verified by an office staff, then the pdf of digital certificate is generated & this pdf document will be encrypted with students public key with the help of asymmetric encryption, then generate a private key too, which is transferred to the student by the university.

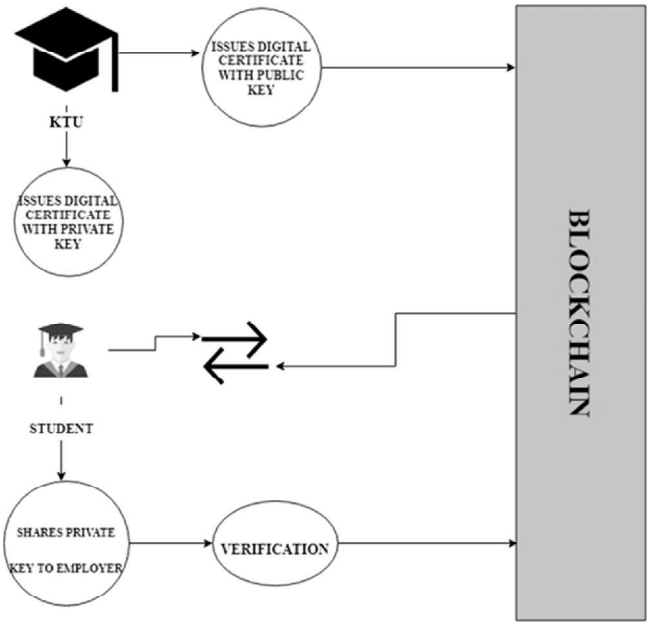

Figure 2: A framework of Block Chain application in University for generating tamper free certificate

When the pdf is uploaded to IPFS system, it generates a Hash value of SHA-256 hashing algorithm to create the value, this hash is then saved to the ethreum block chain and the value of the hash is also delivered to the university. Here ethreum block chain is used with a special program called smart contracts for the purpose of saving the hash of students. It will be saved in a directory called "Graduate MBA 2018" making it easy to search for the hash. One of the important features here is that, each hash in the directory is time stamped with exact time and date when the hash is uploaded. Student gets the hash value and private key from university where students can share the both to a prospective employer or any other authority, so that employer can crosscheck the authenticity.

Employer searches for the hash in the block chain and once found can assure whether the specific candidates degree is authentic or not. After cross checking in the block chain, the employer can also search for the pdf file in the IPFS system with the same hash key. Once the file is found it has to be decrypted using the private key and the original pdf degree certificate can be downloaded by the employer.

6. Proposed Model and Recommendations

The problem of university and employer in terms of cost and with the authenticity of the university certificates can be solved by implementing this proposed model in the university process. Basically it can be considered as a reengineering process where it completely focus in changing the process of physical certificate distribution system and provide all the stake holders transparency and authenticity of the process.

In the proposed model (figure 3), block chain technology can be implemented and IPFR system applied to provide authenticity and transparency to the document. The proposed model uses a hashing algorithm to hash the particular document and helps to save it in the blockchain where the hash saves to the ethreum block chain and is further time stamped so that no one can alter it or change it. It also uses asymmetric encryption system to ensure the certificate is only viewable to those the student needs. IPFR is incorporated in this proposed model in order to save the file in a distributed network, so that no can hack the file. In order to retrieve the file, the same hash can be used to save/restore to the block chain to search the pdf file in the IPFS system. The content can be viewed only with the help of a private key.

Here the block chain technology used is Ethreum block chain, where it contains a special program called smart contracts. It creates a directory to save the hashes that too according to the needs of the client. Overall this model helps to solve the current issue faced by the education sector in terms of the cost and the authentication issue.

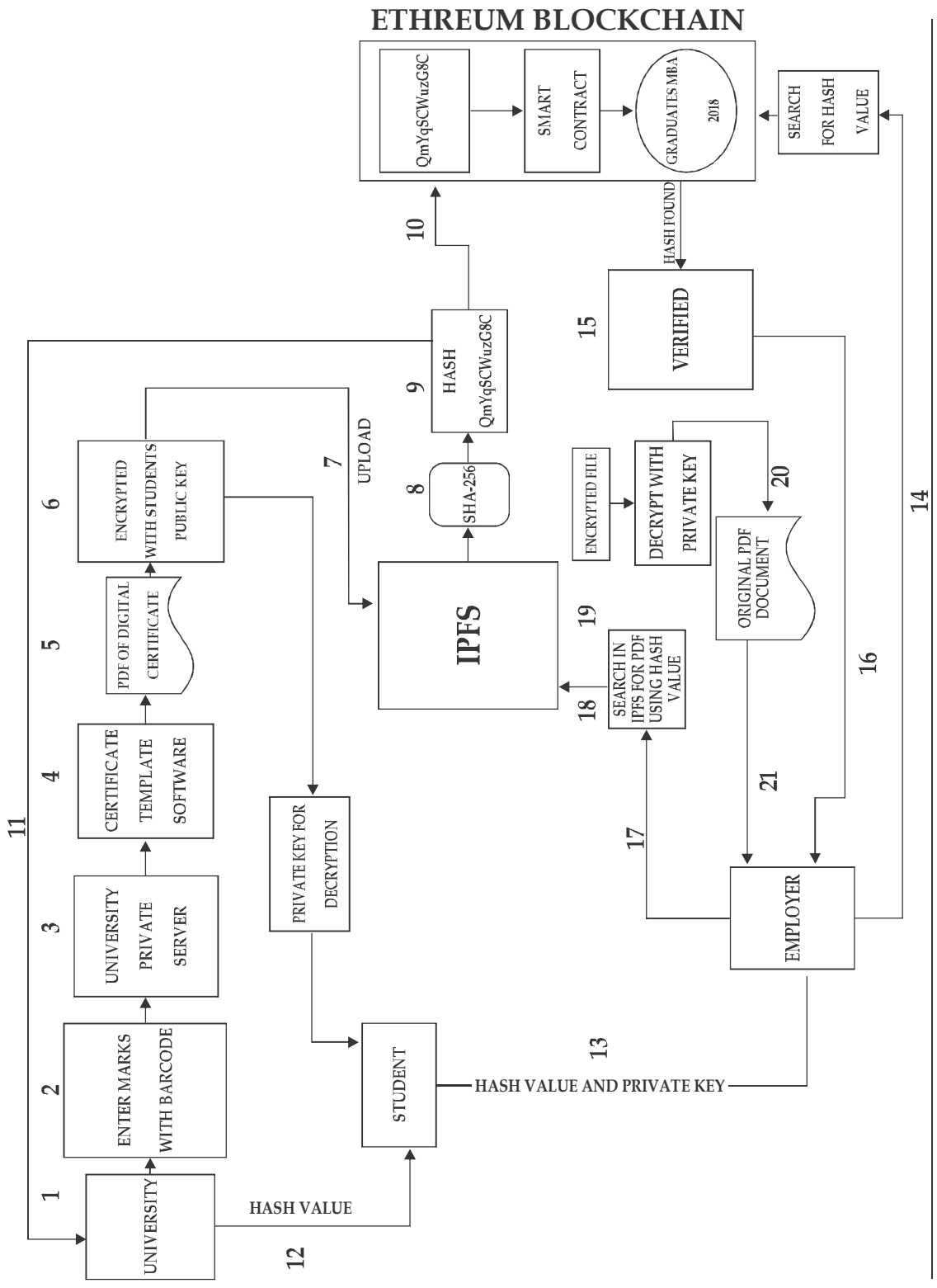

Figure 3: Proposed Model of Block Chain Implementation in Universities

6.1 Process Work Flow of the proposed model

University: The marks entry is done with the help of a portal, which enables barcode scanning of paper and facilitates in entry of the marks, then it is further transferred to the university private server. From the university private server it is transferred to certificate template software and is verified by an office staff, then the pdf of digital certificate is generated & this pdf document will be encrypted with students public key with the help of asymmetric encryption, there generate a private key too, which is transferred to the student by the university.

IPFS (Inter Planetary File System): When the pdf is uploaded to IPFS system, it generates a Hash value, they use SHA-256 hashing algorithm to create the value, this hash is then saved to the ethreum block chain and the value of the hash is also delivered to the university.

Block chain: Here ethreum block chain is used, which a special program has called smart contracts for the purpose of saving the hash of students. It will be saved in a directory called "Graduate MBA 2018" making it easy to search for the hash. One of the important features here is that, each hash in the directory is time stamped with exact time and date when the hash is uploaded.

Student: Student gets the hash value and private key from university where students can share the both to a prospective employer or any other authority, so that employer can crosscheck the authenticity.

Employer: Employer searches for the hash in the block chain and once found, can assure that the student's degree is authentic. After cross checking in the block chain, he can search for the pdf file in the IPFS system with the same hash key. After file is found it has to decrypt using the private key and will get the original pdf degree certificate to the employer.

7. Findings of the Study

- Certificate verification is done by the employer through email or seeking help with technical support.
- Employers are spending crores to verify certificates.
- Printing charge comes around 20 lakhs.
- Fake certificates are major problem in the country.
- Physical delivery of the certificate is time consuming and can take more than one month.
- Postal cost involved for university in each year will comes around 10 lakhs.
- The total cost for entire process comes around 40-50 lakhs.
- Universities use barcode mechanism to save the marks with the help of a portal.
- Universities use certificate template software in order to save the marks in the certificate in the preferred format.
- Hash value is used to save data to the block chain.
- Proposed model uses ethreum block chain and smart contract.
- Employer can verify the certificate by searching the hash in a particular directory in block chain.
- It is impossible to leak data from block chain because it used highly distributed ledger mechanism to store data.
- Employer can retrieve the file from IPFR using hash value and decrypt the file with a private key.

8. Conclusions

There is a need of technological advancement in the education sector in order to deliver proper outputs on time. Especially in the education sector, one important aspect equalent to delivery of knowledge is delivery of authentic certificates. Today, one of the major problem university facades is to deal with the process of traditional certificate delivery to the respective graduates. By proposing a model for the generation of tampers proof certificates with the help of latest technology called block chain and IPFR system solves the problem of traditional certificate delivery method.

The same type of methodology has already been adopted by the Sony global education and University of Nicosia, but in the proposed model it helps to deliver far better certificate issue system and storage by incorporating IPFR with Ethreum block chain. The proposed model delivers better process than other existing models, with the additional option for saving the document in distributed storage system in a secured manner. The documents that stored in any centralized storage can be easily deleted or can cause error. The IPFR system helps to retrieve the entire

file without any damage with the help of highly decentralized storage system. Considering the cost of physical delivery and printing, adoption of this process in university can save lakhs of rupees and will create a transparency in the process.

The world is changing radically day by day in terms of threat and in terms of technology so one should adopt the best practices available today in order to save the valuable contents and also for the security purpose, its better late than never.

References

ARMA International (2013), Generally-Accepted Recordkeeping Principles, available at: www.arma.org/docs/bookstore/theprinciplesmaturitymodel.pdf?sfvrsn_2).

Bayu Adhi Tama, Bruno Joachim Kweka, Youngho Park, Kyung-Hyune Rhee (2017), A critical review of block chain and its current applications, IEEE, INSPEC Accession Number: 17415171.

Diffie, W., & Hellman, M.E. (1979). Privacy and authentication: an introduction to cryptography, Proceedings of the IEEE Vol. 67, No. 3, Mar. 1979 pp. 397-427.

DuPont, Q. (2014). The politics of cryptography: Bitcoin and the ordering machines. *Journal of Peer Production,* 1(4).

Forte, P., Romano, D., & Schmid, G. (2015). Beyond Bitcoin-Part I: A critical look at blockchain-based systems. *IACR Cryptology ePrint Archive,* 2015, 1164.

Fujisaki, E., & Okamoto, T. (1999). Secure integration of asymmetric and symmetric encryption schemes. In Annual International Cryptology Conference (pp. 537-554). Springer Berlin Heidelberg.

ISO/IEC (2001), ISO 15489-1:2001 – *Information and Documentation – Records Management–Part I: General,* ISO, and Geneva.

Knuth, D. E. (1974). Computer science and its relation to mathematics. *The American Mathematical Monthly,* 81(4), 323-343.

Rogers C. (2015), "Virtual authenticity: authenticity of digital records from theory to practice", Unpublished PhD dissertation, University of British Columbia, available at: https://open.library.ubc.ca/cIRcle/collections/ubctheses/24/items/,1.0166169 (accessed 24 April 2018).

Sharples Mike., Domingue John. (2016). The Blockchain and Kudos: A Distributed System for Educational Record, Reputation and Reward. In: Verbert K., Sharples M., Klobučar T. (eds) Adaptive and Adaptable Learning, Proceedings of 11th European Conference on Technology Enhanced Learning (EC-TEL 2015), Lyon, France, 13 - 16 September 2016. DOI: 10.1007/978-3-319-45153-4_48

Sony Global Education (2017), Sony Global Education Chooses Hyper ledger Fabric for a Next-Generation Credentials Platform. Available at https://www.hyperledger.org/wp content/uploads/2017/12/Hyperledger_CaseStudy_Sony.pdf

University of Nicosia. (2017). Academic certificates on the block chain. Available at: https://digitalcurrency.unic.ac.cy/free-introductory-mooc/self-verifiable-certificates-on-the-bitcoin-blockchain/academic-certificates-on-the-blockchain/

Zobrist, A. L. (1970), A new hashing method with application for game playing. *ICCA journal, 13*(2), 69-73.

Sini V. Pillai earned her B Tech from Govt. Engineering College Thrissur Kerala, MBA and PhD in Management studies from University of Kerala. Her professional interests include Operations Management, Quantitative Techniques, Six Sigma and Information Systems. She has over 13 years of Industrial and Academic experience. She has undertaken various consultancy services, conducted several training programs, MDPs and is a life member of ISTE and IIIE.