IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

MODELING OF BLOCKCHAIN WITH ENCRYPTION BASED SECURE EDUCATION RECORD MANAGEMENT SYSTEM

[1]Goma E, [2]Panneer Selvam K, [3]kowsik R [4]Subramani R

[1]Assistant Professor, [2]UG Student, [3] UG Student, [4] UG Student

[1]Computer Science and Engineering,

[1]Adhiyamaan College of Engineering, Hosur, Tamil Nadu, India

Abstract: Blockchain technology can be employed in the education sector by building a decentralized system to store and share student records. The records can be encrypted to guarantee their confidentiality and security. With a blockchain- based system, student records can be saved in blocks that are linked and secured via cryptography. The records are decentralized and not controlled by any single entity, making them less susceptible to hacking or tampering. By using blockchain technology, educational institutions can create a more secure and efficient system for storing and sharing student records. This can streamline the process of transferring records between schools, and provide a secure and transparent way for students to access their own records. In this study, we provide a novel Merkle tree-based strategy for preserving the accuracy of student records and outline how to put it into practice. The software architecture resembled blockchain technology and was developed for private network deployment. The key components of our strategy are replacing conventional audit trails with their cryptographically secure equivalent and simplifying the Blockchain framework by avoiding mining. The cryptography system's framework is presented, and the new five dimensions of chaotic map academic records are proposed. Our study utilizes deoxyribonucleic acid (DNA) sequences and operations and the chaotic system to strengthen the cryptosystem in the blockchain authentication and authorization process. The significant advantage of this method is enhancing the generation of the hash function, which is the most critical challenge in the blockchain concept. The experimental outcomes and security analysis demonstrated that the proposed method works well in terms of different aspects. The suggested hash function's hash value distribution, sensitivity to tiny message modifications, confusion and diffusion qualities, resilience against birthday attacks, keyspace analysis, collision resistance, efficiency, and flexibility were all considered throughout the study.

Index Terms - Blockchain, Data Storage Blockchain, Access Model Blockchain, Authentication Blockchain, Ethereum, Smart Contract, Cryptography.

I. INTRODUCTION

All institutions collect data from their student for verification purposes and update their credits which accomplishes at the institutions. As the certifications are difficult to falsify, this step is done physically. But physical documents can be damaged easily and get mixed. And also, it'll take more time and resources to get verified. As the digital world is getting bigger, storing credit information digitally makes it easy to work on, but at the cost of high-security risk. Many institutions store data on a centralized database which is vulnerable to many security issues like data breaches, injection attacks, and buffer overflow attacks, and for any

hardware issues, the organization should completely shut down its server to solve the problem. Attacks like buffer overflow bottleneck the server hardware by raising various queries. These issues can be solved using blockchain distributed ledger technology. By handling a decentralized storage system, data storage, and authentication can equate parallelly, which makes the data stored more secure, contrary to the traditional database. Three layers of blockchain are employed to make this approach more secure. To authenticate the users who need to access the data, Authentication Blockchain is used. Here, the Authentication Blockchain was made using an open-source Ethereum-based model. Smart Contracts are used for creating and verifying the users and their credentials. All transactions should satisfy the Smart Contract to complete the job. The Data Storage Blockchain stores the student data on the blockchain in blocks. These blocks are interlinked using hash values between the blocks. If the data ever got tampered with, this model identifies the change by comparing the hash values of the blocks. And the Access Model stores all the changes made to the data storage blockchain. The user can see what was changed when using this access model. The main objective is to store the student's credit information using blockchain technology as securely as possible.

II. Related Works

Satoki Watanabe and Kenji Saito [1] uses the Merkle tree method for storing information and also uses it to retrieve a specific set of requested data to be validated. It authorizes partial signature to assure the authenticity of the data or the information received.

Norah Alilwit [2] uses a unique digital id to retrieve information for the user since it is more secure than the traditional authentication method. All types of legal documents can be stored and verified using a digital database.

Joberto S. B. Martins and Emanuel E. Bessa [3] stores the transcripts and certificates of the students on the blockchain. So, the transfer and verification of the documents can be a pushover compared to traditional hard copy verification, which takes more time and resources.

Patrick C. K. Hung, Qusay H. Mahmoud, Ahmed Badr, and Laura Rafferty [4] makes the application open to students as students can access their certificates and send them for verification and scholarships. The coordinator verifies the provided data before being added to the blockchain.

Omar Musa, Shu Yun Lim, Abdullah Almasri, and Pascal Tankam Fotsing [5] uses distributed ledger technology, by which authentication was more secure and data modification.

Xin Liu and Wentong Wang, Ning Hu [6], shared their services between domains through authentication. A Certificate Authority will verify the authenticity of the user.

Hui Lin, Xiaoding Wang, Fu Xiao, Quanwen He [7], made the consortium blockchain stores all transactions between the private blockchains for future reference.

Badis Hammi, Sherali Zeadally, Yves Christian Elloh Adja, and Ahmed Serhrouchni [8], the Certificate Authority verifies and revokes unwanted certificates by analyzing the validity of the certificates.

Hrithik Gaikwad, Navil D' Souza, Rajkumar Gupta, and Amiya Kumar Tripathy [9] uses the OCR module to extract details from the requested certificates. The extracted data is converted to a hash value and then verified by the server.

Shenyi Huang [10] uses asymmetric cryptography techniques for verification. It uses a private key to access data and a public key to verify data.

Xiangwu Ding and Jianming Yang [11] used an access model, which gives access to the data according to their role. The role varies based on the attributes assigned.

Aastha Chowdhary, Shubham Agarwal and Dr. Bhawana Rudra [12] converts the certificate to complex hash values and then compares the hash value to an existing certificate in the server.

Jintao Zhu, Yinzhen Wei, and Xiaoxiao Shang [13] used a decentralized blockchain to store the data securely. The data verification is done by using the public key and comparing the nonce of the data.

Oiza Salau, and Steve A. Adeshina [14] use the Interplanetary file system hash method for accessing and verifying data.

Untung Raharja, Qurotul Aini, Ninda Lutfiani, Fitra Putri Oganda, and Ahman Ramadan [15] used Distributed Ledger Technology for storing and verifying the data.

III. EXISTING SYSTEM

All Educational Institutes record their student credits and give them certificates for their accomplishments. Most of the schools store their data on centralized data servers. Centralized servers have their cons, like security issues and data breaches. Most cons can be solved using blockchain technology, as it is more secure and safe than the traditional storage system. Nowadays, many tech companies adapted to this technology. It's been in many areas, like access models, authentication, verification, and more. In [2], [5], [6], and [13], the blockchain network stores the user credentials. When the user enters their credentials, it gets verified from the blockchain network, but if the data ever tampers, the change can't be identified. In [1], [4], [8], and [9], the requested data gets verified, and also, the chain gets validated. The chain is validated by checking the current hash value, which should be equal to the next block's previous hash value. In [7] and [11], the access model gets requests and verifies the request according to the given attributes of the user. If the request is valid, it gets satisfied and records all the requests made by the users. But the data is stored in a centralized database on this model which makes it more vulnerable to some common security attacks. For example, in the authentication model, only the authentication part is stored in the blockchain, and the centralized server stores all other data. This makes the data more vulnerable to tampering and data loss.

IV. RESEARCH METHODOLOGY

A. System Model

This study has three characters, authority, student, and the school. The authority adds the given data to the blockchain. After completion of the course, the school where the student graduated sends the student credits and the certificate details to the authority. The authority adds the details to that particular student's blockchain. Both authorities and students have separate authentication for their needs. The students can view their data by entering their credentials on the platform. They can view all the data uploaded by the authority. If the student needs to apply for a new school, they should generate a unique key. A unique key and blockchain ID gave to the institution with the application. The institution can crossverify the data from the application with the blockchain using the key given by the student.

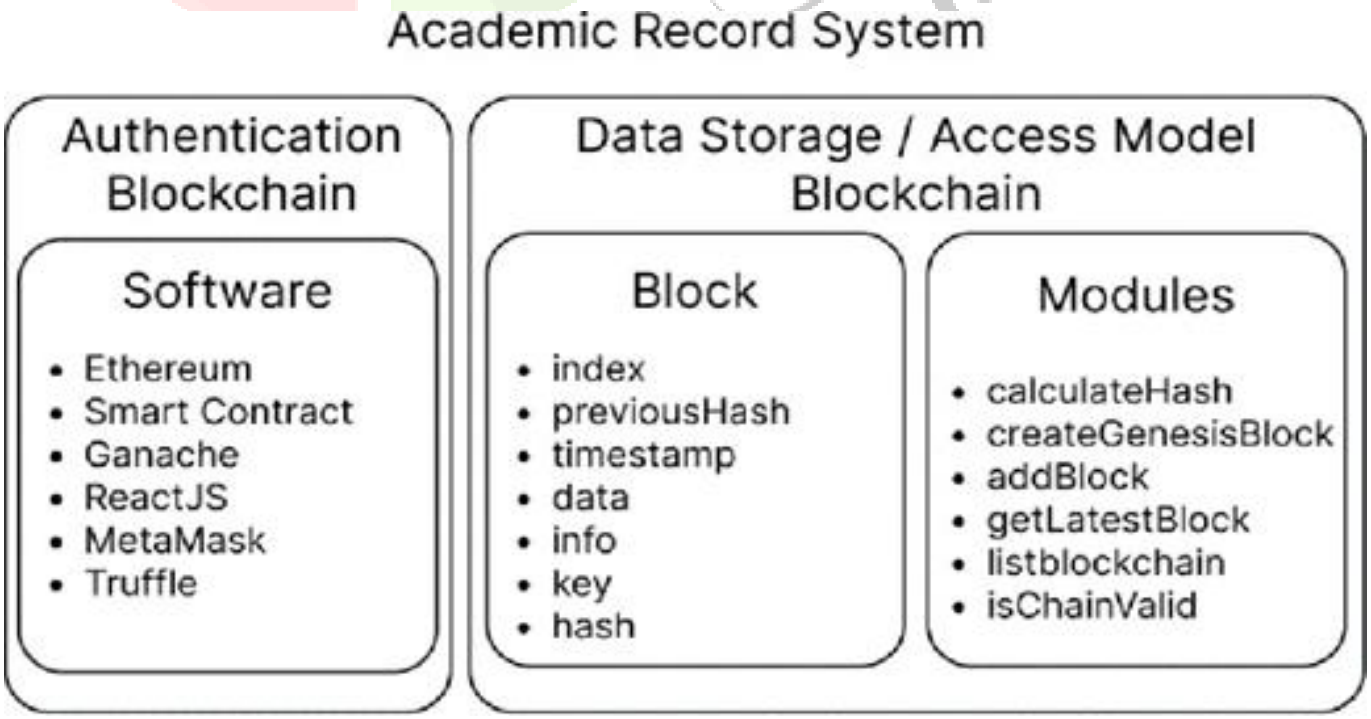

Fig. 1. Softwares and Modules of the Model

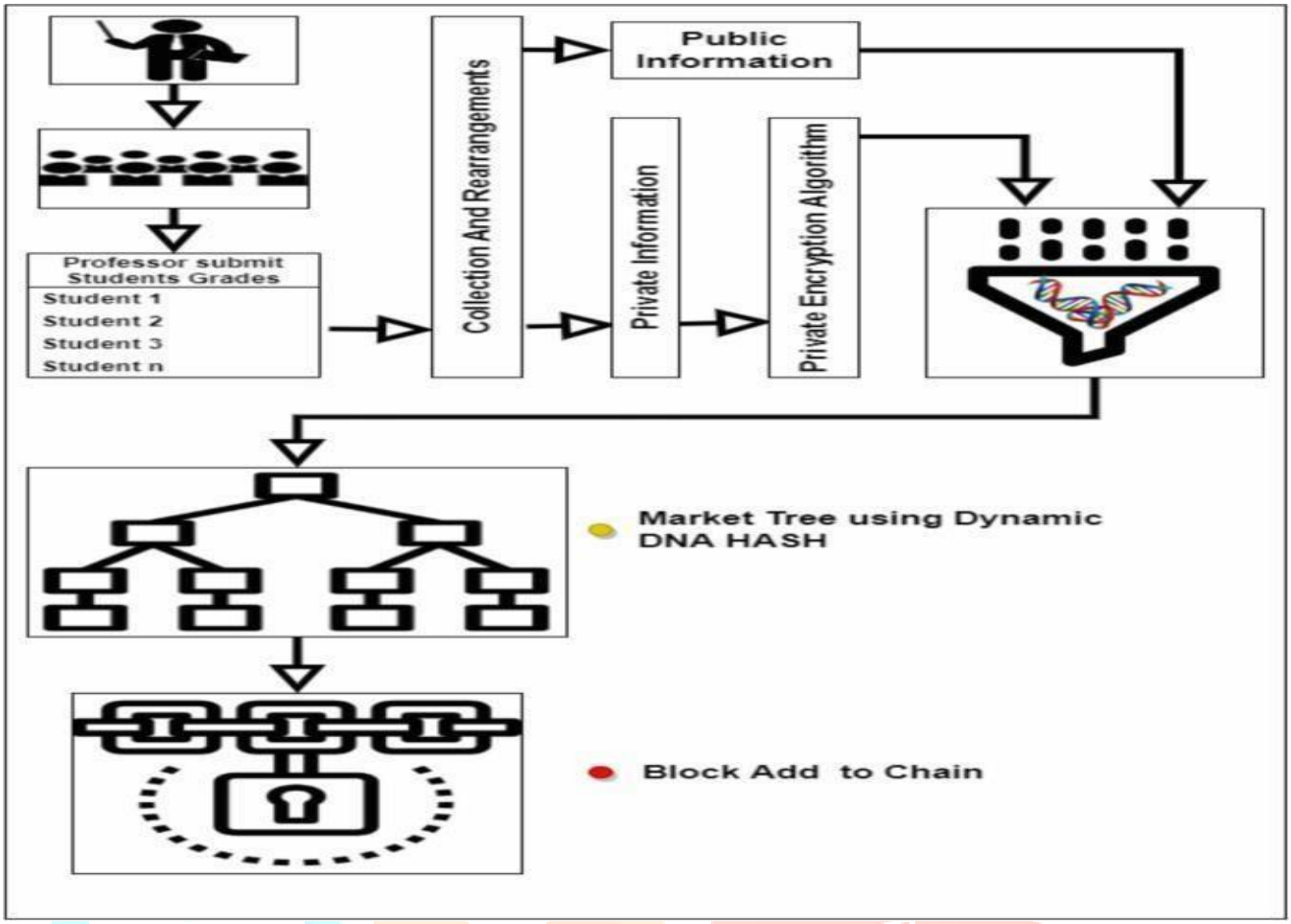

Fig. 2. Overall proposed architecture

B.Model Architecture

This model has three phases, Authentication, Accessmodel, and Storage. Each phase have their own blockchain. First, the authentication phase checks the authenticity of the user. After the user got verified, the access model records the user information and the request made by the user. If the user request is valid, the request will be satisfied.

Table 1: Software requirement

Operating Environment	Tools
Local Blockchain	Ganache v2.5.4
Server Environment	NodeJS v18.13.0
Pipeline for Blockchain	Truffle v5.4.29
ETH Wallet	Metamask v10.22.2

1. *Authentication:* In this phase, the user enters their credentials and sends them to the blockchain. The blockchain verifies the credentials and sends the transaction to the following model. If not, an error pops out saying the credentials are wrong.
    a. *Ethereum:* It is an open-source blockchain model. It uses smart-contract methodology.
    b. *Smart Contract:* It is a condition to validate the transaction undergoes smart contract validation. The smart contract should be satisfied to complete a transaction. Else, the transaction gets denied.
    c. *Ganache:* Ganache used to develop a private Ethereum blockchain. Each account holds 100 ETH. When the smart contract is satisfied, the ETH gets transferred.

d. *Truffle:* It creates an environment for ETH development. It is a testing framework for ETH. It uses Ethereum Virtual Machine for development.
e. *Web3JS:* Web3JS is used to interact with the local network blockchain protocols and servers. Using this, we can interact with the Ganache blockchain.
f. *Solidity:* It is an object-oriented programming language used to make smart contracts for Ethereum.
g. *ReactJS:* ReactJS is used to make the user interface interact with the web application and the local ETH blockchain.

Metamask: Metamask is the ETH wallet to store and transfer ETH between accounts to make transactions.

Access Model: In this phase, this blockchain records all the transactions approved by the authentication blockchain and the request by the user. This blockchain logs all the transactions that happen through it. *SHA256:* It is used to encrypt and decrypt the data and the hash value in each block. It is then calculated for hash value. All the variable of a single block it taken into consideration for the formula.

$$hash\_value = p(t*I)/d$$

- *previousHash(p):* It has the value of the hash value of the previous block.
- *timestamp(t):* It contains the period of the creation of the block.
- *data(d):* It is the information to be stores on the block.
- *index(I):* It is the position of the block in the blockchain.
  i. *Blockchain:* Data is stored in blocks, interconnected to other blocks in the chain. Every new block created is added to the end of the blockchain.
  ii. *Genesis Block:* It is the first block of the blockchain. This block ensures that there is no block before it.
  iii. *Blocks:* It contains the data and other information to the block to interconnect with the blockchain.
  iv. *Modules:* It contains the functions that builds the blockchain.
- *createGenesisBlock():* This module creates the first block of the blockchain.
- *getLatestBlock():* It returns the last block on the blockchain.
- *isChainValid():* It checks whether the blockchain is valid or not. Especially all the hash values of the current block should be equal to the previous hash of the next block.
- *addBlock():* It gets information from the authority and adds a new block to the blockchain.
  listBlockchain(): This module prints the entire blockchain.

Storage: In this phase, this blockchain stores all the data of the students. After recording the request on the access model, this blockchain displays the requested data. In this phase, the students can generate a key for their application for a new school.
Verification: The student can generate a key and attach the key to the application for their new institution. The new institution can verify the data with the blockchain ID and the key.

V. Working

There are mainly three characters, Authority, Student, and Institution. Authority is the person who creates an account for the student. The account was created using Ethereum transactions. First, the Authority enters the Username, Password, and Chain ID. All the credentials are updated in the Ethereum model with Smart Contract validation. If the student accomplishes anything in the school or institution, the credits are updated in the blockchain by the authority. The Authority adds data to the Data Storage Blockchain using the unique Chain ID for each student. The Student can access their data by logging in to their account and they can also copy the key for individual data. The key will be given to the institution along with the application. The key is used to compare the data given by the student and the existing data on the blockchain. The institution enters the chain ID along with the key and the data to verify. The verification process compares the given data to the existing data on the blockchain. All the changes made to the Data Storage Blockchain is being recorded by the access model blockchain for security purpose. Finally, the blockchains verify themselves by comparing the hash values with each other.

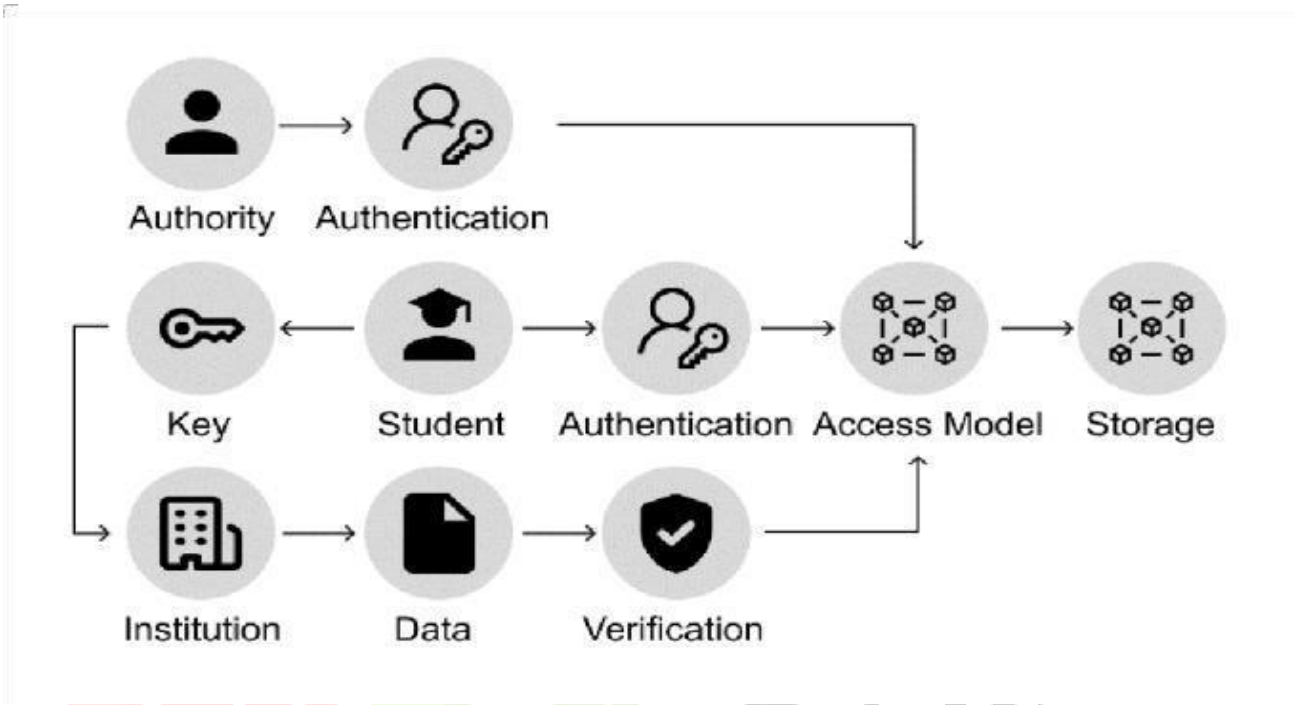

Fig. 3. Working of the Model

VI. Conclusion

To ensure the data given by the student is legit and to secure the student's credit information, authentication, access model, and storage model were made using blockchain. The authentication model is used to verify the user and the authority. The user is the student who owns the blockchain. Authority is someone who adds credit information to the blockchain. The access model records all transactions after verification. The storage model stores the credit information of the student. With this study, the student credit information is stored securely on the blockchain, and the access model records all updates, verification, and access undergone on the blockchain. This model avoids data theft, personal credit fraud, and more. More importantly, the student knows who accessed their data. And it also avoids the duplication of student credit information.

VII. Acknowledgment

I would like to express my heartfelt gratitude to all those who contributed to the successful completion of the Modeling of Blockchain with encryption secure based education record management system project. First and foremost, I extend my sincere thanks to our project supervisor, Mrs. Goma E, for their unwavering support, guidance, and valuable insights throughout the entire development process. I am deeply appreciative of the Head of our Department, Dr. G. Fathima, faculty members and staff who provided their expertise and resources, enriching the project with their knowledge. Special thanks to my fellow teammates for their collaborative spirit, dedication, and hard work, which played a pivotal role in achieving our shared goals. I am also thankful to the

academic institution for fostering an environment that encourages innovation and continuous improvement. Lastly, I extend my gratitude to friends and family for their understanding and encouragement during the project's journey. Each contribution, no matter how small, has been instrumental in making this project a success.

VIII. REFERENCES

[1] Gorkhali A, Li L, Shrestha A. Blockchain: a literature review. J Manag Anal 2020;7, (3):321–43. https://doi.org/10.1080/23270012.2020.1801529.

[2] Svejda M, Goldberg J, Belden M, Potempa K, Calarco M. Building the Clinical Bridge to Advance Education, Research, and Practice Excellence. Nurs Res Pract 2012;2012:1–10. https://doi.org/10.1155/2012/826061.

[3] Balcerzak AP, Nica E, Rogalska E, Poliak M, Klieˇstik T, Sabie OM. Blockchain Technology and Smart Contracts in Decentralized Governance Systems. Adm Sci 2022;12(3). https://doi.org/10.3390/admsci12030096.

[4] Z. Zheng, S. Xie, H. Dai, X. Chen, H. Wang. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. In: Proc. - 2017 IEEE 6th Int. Congr., Big Data, BigData Congr. 2017, pp. 557–564, 2017, 10.1109/ BigDataCongress.2017.85.

[5] M. Florian, S. Henningsen, S. Beaucamp, B. Scheuermann. Erasing Data from Blockchain Nodes. In: Proc. - 4th IEEE Eur. Symp. Secur. Priv. Work. EUROS PW 2019, pp. 367–376, 2019, 10.1109/EuroSPW.2019.00047.

[6] Raimundo R, Rosario A. Blockchain system in the higher education. Eur J Investig ´ Heal Psychol Educ 2021;11(1):276–93. https://doi.org/10.3390/ejihpe11010021.

[7] Tian HJ, Lei P, Wang Y. Image encryption algorithm based on chaos and dynamic DNA coding. Jilin Daxue Xuebao (Gongxueban)/J Jilin Univ (Eng Technol Ed) 2014;44(3):801–6. https://doi.org/10.13229/j.cnki.jdxbgxb201403035.

[8] Ghazal O, Saleh OS. A graduation certificate verification model via utilization of the blockchain technology. J Telecommun Electron Comput Eng 2018;10(3–2): 29–34.

[9] Daraghmi EY, Daraghmi YA, Yuan SM. UniChain: A design of blockchain-based system for electronic academic records access and permissions management. Appl Sci 2019;9(22). https://doi.org/10.3390/APP9224966.

[10] Islam A, Kader MF, Shin SY. BSSSQS: A blockchain-based smart and secured scheme for question sharing in the smart education system. J Inf Commun Converg Eng 2019;17(3):174–84. https://doi.org/10.6109/jicce.2019.17.3.174.

[11] Li H, Han D. EduRSS: A Blockchain-Based Educational Records Secure Storage and Sharing Scheme. IEEE Access 2019;7:179273–89. https://doi.org/10.1109/ ACCESS.2019.2956157.

[12] Noor MU. "Implementasi Blockchain di Dunia Kearsipan: Peluang, Tantangan, Solusi atau Masalah Baru?", Khizanah al-Hikmah. J Ilmu Perpustakaan Informasi dan Kearsipan 2020;8(1):81. https://doi.org/10.24252/kah.v8i1a9.

[13] Guo J, Li C, Zhang G, Sun Y, Bie R. Blockchain-enabled digital rights management for multimedia resources of online education. Multimed Tools Appl 2020;79 (15–16):9735–55. https://doi.org/10.1007/s11042-01908059-1.

[14] Hewa T, Ylianttila M, Liyanage M. Survey on blockchain based smart contracts: Applications, opportunities and challenges. J Netw Comput Appl 2021;177. https://doi.org/10.1016/j.jnca.2020.102857.

[15] Mitra D, Tauz L, Dolecek L. Polar Coded Merkle Tree: Improved Detection of Data Availability Attacks in Blockchain Systems. IEEE Int Symp Inf Theory - Proc 2022; 2022-June:2583–8. https://doi.org/10.1109/ISIT50566.2022.9834538.