Journal of Namibian Studies, 35 S1 (2023): 3670-3689 ISSN: 2197-5523 (online)

The Academic And Commercial Circles In Block Chain Security, Privacy And Scalability At Block Chain Technologies

Sony Kumari[1], Dr. Manoj Eknath Patil[2]

Research Scholar[1], Research Guide[2]
[1,2]Department of Computer Science & Engineering,
Dr.A.P.J.Abdul Kalam University, Indore(M.P)
sony.nayan@gmail.com[1] , mepatil@gmail.com[2]

ABSTRACT

It was first utilized for bitcoin as a more secure means of conducting financial transactions. The scientific and financial sectors have been more interested in blockchain-based computer systems in recent years. a peer-to-peer network that is not controlled by a trustworthy third party. There are several blockchains available today, including Ethereum, Hyperledger, Tezos, and others. Blockchains are appealing to a wide range of applications because each one has a unique operating mode and transaction validation consensus. All required stakeholders in the field of education must have access to a dependable technology in order to progress the educational system and bring it to the next level. The blockchain possesses all of the necessary characteristics to do this mission, but in order to be deployed on a broader scale, it must also provide data security and privacy.

Keywords: Academic , Commercial, Circles, Block Chain, Scalability, Security, technologies.

INTRODUCTION

Blockchain Concept

The blockchain is a decentralized, collaborative, and open ledger that is used to record payments across several devices in a way that prevents subjective changes to the data without reformatting every compliance mount and platform user. Blockchain technology, which Satoshi Nakamoto developed, is the "technology behind Bitcoin".

This provides the support investors need to evaluate remittances or payments and to evaluate them fairly. With a peer-to-peer model and a scattered session casting database, the blockchain platform has been operating in an unusual manner. They are enigmatically supported by external self-interests that are furthered through continual collaboration. There is a little misunderstanding of the investment's information security or customer data since the final strategy utilized is static.[1-3]

A chain or system of blocks known as a "blockchain" preserves data in a safe manner protected by encryption methods and hashing processes utilizing a variety of hashing algorithms, including SHA256 and Keccak256. This secure technique of data storage is protected by the name of the blockchain. Both the sending and receiving parties will have separate sets of private and public keys that will allow them to decode any encrypted data that has been sent to them. This increases the level of security for data transfers inside blockchains. It is also possible to describe it as a common, immutable ledger that makes it easier to record and maintain track of data and transactions inside a network. Another name for this idea is "blockchain."[4-7]

Principal Features of Blockchain

The principles of decentralization, security, accountability, anonymity, and durability are the foundation of blockchain technology. [8]Blockchains employ distributed ledger technology and have a decentralized architecture. Miners on each node in the network are the only individuals with the authority to validate, maintain, and update new block entries that are posted to a distributed ledger. Miners are the only nodes capable of adding new blocks. The system is typically governed by everyone who is a part of the blockchain network, and depending on the sort of architecture, its precise operation may differ greatly. The differences and similarities between the various blockchain topologies are depicted in Figure 1. Additionally, it helps define the kind of architecture needed for the software depending on the characteristics it has.[9-13]

Characterstics	Public blockchain	Private blockchain	Consortium blockchain
Determination of consensus	All miners participating in network	Group head / Lead node	Set of identified nodes
Accessibility	Public	Could be public / restricted	Could be public / restricted
Efficiency	Low	High	High
Immutability	Can't be tampered	Could be tampered	Could be tampered
Centralized	No	Yes	Partial
Process of consensus	Permission less	Permission required	Permission required
Examples	Bitcoin, Ethereum, Litcoin etc	Ripple (XRP) and Hyperledger	Quorum, Hyperledger and Corda

Figure 1. A comparison of several blockchain architectural types

Architecture of SecuSca:

The architecture of the proposed SecuSca technique. Transactions are started by users, recorded in a block, and then added to and copied across the network's chain of blockchains. In order to maintain the blockchain as safe and scalable as possible while simultaneously reducing the number of total replications it does, SecuSca achieves a balance between security and scalability. The method has two phases that take place concurrently. The process of sharding is made simpler by the addition of an optimization function, which is as follows.:[14-16]

Effective replication: The replication has boosted both the storage and the safety. Dynamic sharding duplicates and distributes the blockchain's current state over a fraction of the network's nodes while maintaining data integrity. The main objective is to maintain the blockchain's security and scalability while also storing data for use in future blockchain applications, which may take many various forms. Even nodes with limited memory capacity will be able to participate in the protocol's execution..[17-19]

Efficient reduction: A reduction phase is trying to reduce the duplication of certain blocks so that the blockchain may subsequently be scaled up when each newly contributed block is duplicated across the network. As a result, the blockchain's network could be able to hold more data. In the part that follows, we will go into further depth about the SecuSca strategy..[20-22]

Blockchain applications in academic

The twelve distinct applications in their extensive investigation of blockchain-based applications in education. These categories may have subcategories as well.[23-24]

1. Identity management and certificates: Blockchain technology, in accordance with Devine (2015), makes it simple to share student academic data with organizations and corporations in order to expand prospects for personal growth.[25-28]

2. Encouraging and promoting lifelong learning
Additionally, blockchain technology offers a wide range of uses in the educational process, making it more engaging and enjoyable for all parties.Devine (2015) claims that due to the typical online learning tools' inability to successfully engage students in the learning process, both instructors and students exhibit. As a possible tool that "may improve or enhance the current online teaching and learning experience," he views the open source blockchain technology architecture.."

The difficulty of scaling
The "slow speed blockchain transactions" problem lies at the heart of the scalability dilemma. This method causes the blocks to grow in size since educational institutions collect a lot of information about a lot of students. Transactions will take longer to complete when more blocks are uploaded to the blockchain since each block needs to be validated by other peers. The maximum transaction pace, for instance, for the Bitcoin system is between three and seven per second. As a result, the problem of scalability could prove to be a major barrier for research into and possible widespread implementation of blockchain-based educational solutions.[29-31]
Gaining a thorough understanding of each blockchain-based solution (such as its technical implications and market acceptance factors) is one of the most important first steps that must be taken when conducting an investigation into the challenges associated with scaling blockchain technology within the educational sector. This is one of the most crucial first steps. It is crucial to emphasize this concept. The providers of these solutions will therefore be able to evaluate the characteristics of the educational software they offer and determine whether or not scalability is a valid concern with relation to their products.

Since just a small number of transactions may need to be recorded on the blockchain in this case—for the sake of credentialing, for example—scale may not be a significant issue. When utilizing the blockchain to pay for college tuition or transferring educational tokens to encourage lifelong learning, scalability may prove to be a more difficult obstacle to overcome. This is due to the fact that the blockchain can only execute a certain number of transactions per second.[32]

Data security and privacy

It ensuring anonymity and security on the blockchain is quite difficult. Despite this, it is essential since privacy and security must coexist in circumstances when a student's career may be in danger (such as while obtaining school credentials and certifications). In addition to the difficulty of maintaining the privacy of particular transactions through the use of public and private keys, making transactions visible to anybody with access to the blockchain is a concern. This is concerning since the data contained in the transactions may be acquired elsewhere and made public. One approach to solving this problem, though, is to encrypt the data stored on the blockchain. As a result, there will be a lower chance of unauthorized access to information. Only a hash of the data may be saved on the blockchain; the entire information must be stored elsewhere. This is an additional choice.[33]

Framework for Digital academic Credentials Based on Blockchain

Online users have access to a broad variety of digital credentials, such as certificates and badges. In the context of the digital world, the equivalent of diplomas, awards, and medals that are printed on paper. Digital credentials are simple to provide, store, and validate. Examples that regularly come up are awards for finishing a course or subject, diplomas from academic institutions, and prizes for advancing one's technical or personal proficiency. Another example is being acknowledged after finishing a course or subject.

The ability of the credential holder and the organization or authority that has validated that knowledge are key details that digital certificates reflect and transmit. [34]A symbol that identifies the institution that awarded the certificate and the skill that was obtained is typically included on

certificates. One example of such a sign is the Faculty Development badge of Course and Curriculum Mastery from the Colorado Community College System. University transcripts will become less important as digital credentials become more prevalent, which is a bad trend. Even though the completion of a degree program is still highly valued by employers, job applicants are not required to provide their transcript's course grades. The ability to evaluate and convey whole learning successes is one advantage of digital credentialing...

Digital certificate problems

In the past ten years, as the value of professional credentials has increased in the market, the production of phony academic The credentials issue now affects everyone. Numerous individuals believe that the current state of the economy is to blame for the increase in the number of fake degrees since desperate people would produce false documentation to gain qualifications for jobs. On the other hand, recent data suggests that, in addition to lower-level employees, credential theft also impacts activists, public servants, and university applicants. A recent study's findings indicate that controlling and administering the transcript-issuing process presents a number of difficulties.[35]

OBJECTIVES OF THE STUDY

1. To learn about SecuSca's blockchain concept and architecture.
2. To research how blockchain may be used in education and to develop a blockchain-based framework for digital credentials in the field of education.

RESEARCH METHOD

We vary the number of duplicated blocks and the depth of the block chain in two different experiments to evaluate and compare our approach to the bitcoin standard blockchain. We run several simulations with different values for the α and γ parameters to establish the upper bound α N and lower bound γ 0. The entire size of the blockchain that has been sharded throughout the network will then be provided. This section explains how the design of the study was created, as well as the methodology approach that was used to produce the desired results. How the study was carried out as well as why specific tools and

techniques were chosen. The study made use of data from Ethereum..

Workflow for Blockchain Technology

Blockchain uses a range of contemporary technologies, including as automated scripting, smart contracts, data production and updating, and data transport between nodes, to construct logic applications. In contrast to traditional databases, which can only maintain data security on one side of the system, blockchain technology can do so on both sides of the system. Block generation, consensus verification, and ledger maintenance make up the three main parts of a blockchain's workflow. These processes make up a blockchain's whole operating system.[36-38]

Algorithm for Blockchain Encryption

The blockchain application will get compute requests from applicants whenever they want assistance with their computing requirements. The application first sends a request to the kernel and any auxiliary components to compute the feedback value, and then transmits the computed feedback value behind the requester's back. The applicant checks the accuracy of the feedback value using the verification key. As soon as n reliable feedback data have been collected, it will be possible to acquire the precise calculation result.

The startup phase of the process is the first

. F_a is a finite field with the property a. A polynomial F(x) of degree n-1 with the following form is chosen at random by the distributor in F_a (x):

Based on the characteristics of the data they contain and how they are utilized, blockchains can be classified as consortium, private, or public. The public chain of information is available to everyone. Any public chain member has the ability to take part in the data consensus process and can function as a basic node or an absentee node. The position and management authority of each node are decided by a centralized manager within the company that controls the private chain. The information relating to the private chain is only accessible to and usable by a restricted number of the appropriate internal staff personnel; it is not accessible to the general public.. [39]

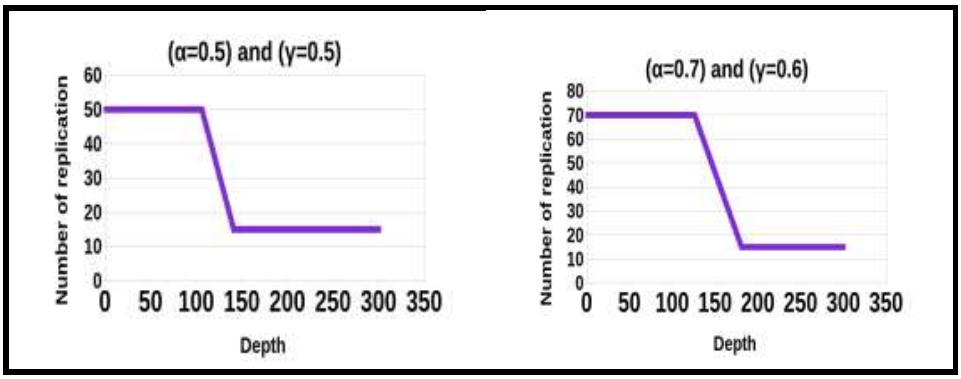
Table 1 Blockchain categorization.

Attributes	Public chain	Alliance chain	Private chain
Efficient	Low	Low	High
Consensus mechanism	Pow, PoS, dPoS	PBFS, RaFt	Solo PBFS
Represent	Bitcoin	Hyperledger fabric	MultiChain
Read permission	Public	Public or restricted	Restricted
Participants	Anyone	Alliance member	Members in the organization

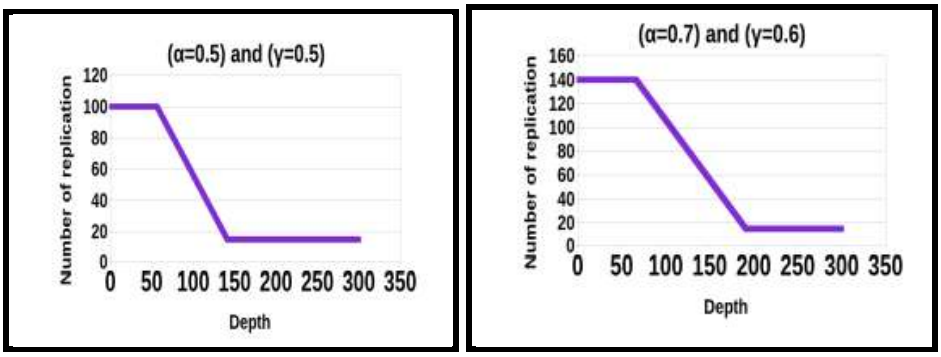
DATA ANALYSIS

In the trials, we looked at the size of the blockchain and the block replication efficiency.[40-41]

Repetition of the contested blocks. The data is transferred over the network and saved on the local disks of the network nodes when a miner generates a new block. A simulation of the function R(d) is first conducted on 100 nodes, each of which has 200 GB of storage. Figure 2's (a) α and γ (b) parts. Each node is in charge of performing the R sharding optimization algorithm. The new block's depth will be 0 at the beginning of the operation. Despite the fact that no block is connected to it, it is heavily copied. The parameter's values were changed to (α = 0.5) and (α = 0.5), then (γ = 0.7) and (γ = 0.6). For the initial simulation, the upper restriction is set to 50, and the block is repeated over all 50 nodes in the network. This main replication will continue until it reaches a depth of zero at a constant rate. The outcomes of a second simulation with 200 nodes and 100 GB of storage are shown in Fig. 2 (c) α and γ (d). How many times each block is copied depends on how many blocks have been added to a blockchain. As the block depth increases, its value decreases. Block replication is reduced by our method to zero percent. Each transaction's block in the blockchain will only contain the replication level that is lower than the block before it. Our investigations have led us to the conclusion that in order to maintain the state of the blockchain as its size increases, there must be 15 copies of each block (γ O = 15).[42-43]



a) 100 nodes, 200GB of memory **b) 100 nodes with 200GB of RAM**



(c) 100 nodes, 200GB of memory **(d) 100 nodes, 200GB of memory**

Fig. 2: Block replication with respect to block depth

The network's size is established. In the next experiment, the algorithm will be executed on 100 nodes, resulting in 300 blocks, each of which is 1 megabyte in size. Figure 3 provides an overview of how the common blockchain and the SecuSca blockchain have grown in size over time. The experiment demonstrates that the overhead of blockchain dramatically rises in common blockchains, which are indicated by the color red. The total number of blocks stored on each node increases the overall size of the SecuSca database when counting backwards from the earliest block to the most recent block. The total number of transactions across all shards is shown by the blue line. Every block is substantially replicated starting at [0-200], and the size increases linearly. The nodes will begin to minimize the amount of replication once we reach the bottom bound of our approach.[44-45]

Each shard's size t in each node n is defined at different stages by:

$$t_n = \sum_{i=0}^{b} \frac{R(i,t)}{N}$$

.....(1)

N is the number of nodes, i is the location of a block in the chain, bi is the length of the blockchain, and t is its size..

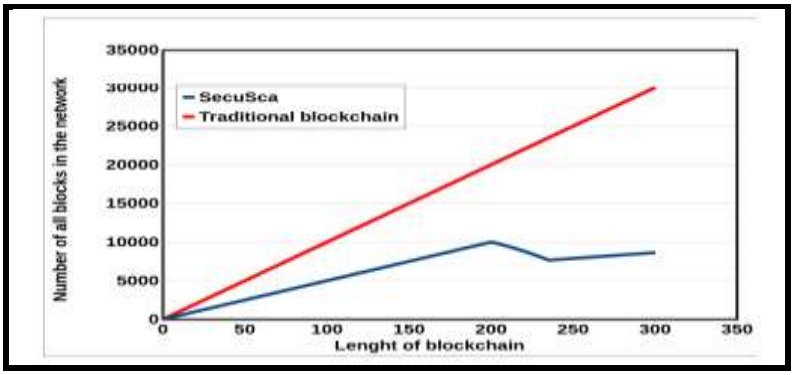


Fig. 3: Traditional blockchain and SecuSca blockchain sizes are contrasted.

Analyzing the Comprehensive Student Information Management System's Security A random sample of the data should be selected from the enormous amount of academic data accessible as the first stage in the process of building an academic information model. In order to verify the security of this standard student information management system, this paper uses the blockchain technology's security test methodology and its blockchain encryption algorithm. The data gathered from scholarly sources is displayed in Table 2 below. [46]

Table 2 Educational data.

Area name	Type	Method of encryption
Student ID	String	Symmetric encryption
Name		
Major		
Entity ID		
Phone		

We will evaluate the security of the commercial student information management system A in accordance with the model's design. The assessment of how difficult it is to read and transfer account information is one of the two components of the security test for the student information management system. In the first component, the link between account security and login password length is looked at, and in the second, the readability of account information is assessed. The next step is to conduct an experiment to see whether the length of a login password for the Student Information Management System has any

bearing on account security. Figure 4 displays the test results.47]

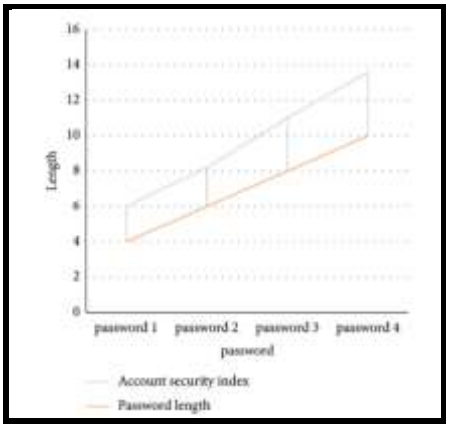


Figure 4 The correlation between system length and Security for accounts and passwords.

Using blockchain technology, the student information management system B underwent security testing.

The student information management system B's degree of data protection is assessed using distributed ledger technology employed by blockchain. First, we established a relationship between blockchain technology and the academic data model (Table 2). Then, in order to safeguard the confidential data stored within the system, we encrypted it using the blockchain encryption approach. The system should then be upgraded, and you should reevaluate the assessments of the read and transfer difficulty coefficient for account information as well as the relationship between the security of the new system B's accounts and the length of the login password. The update should be finished last. Figure 5 displays the outcomes of a blockchain technology test conducted on the account security and password length of the student information management system B...[48]

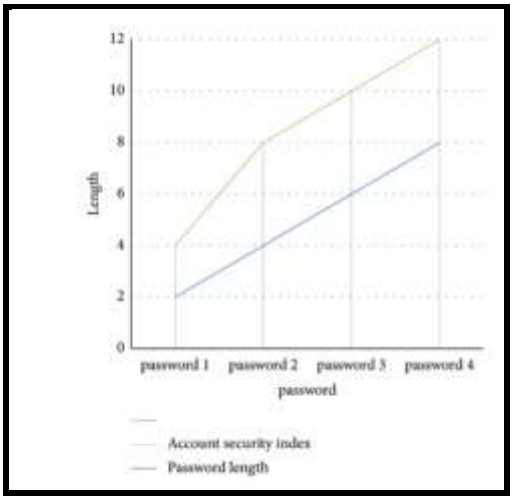


Figure 5 The association among password length and account security for system B.

Figure 5 shows that when implementing blockchain technology and blockchain encryption methods, the account security of the brand-new student information management system B strongly relates to the length of the password. This was discovered thanks to the usage of blockchain technology and blockchain encryption techniques. In contrast to system A, system B does not maintain a proportionate relationship between account security and password length from the beginning to the finish of the operation. The degree of account security, however, will no longer rise as the password length grows after it reaches six characters. This suggests that in the blockchain-based student information management system, there is a predetermined limit value between account security and password length. The password for accessing the account must thus contain at least six digits. Once this condition is satisfied, the account's security will continue to remain constant and unaffected by the password's length.

The difficulties of using blockchain in the educational space

The major challenges that businesses and organizations looking to implement blockchain technology in education must overcome are discussed in the paragraphs that follow. In this context, we will look at two different sorts of problems:

The difficulty of scaling

The "scalability challenge" is allegedly brought on by "slow speed blockchain transactions." The blocks get larger as a result of educational institutions collecting extensive data on a large number of pupils. Since each transaction on the blockchain requires peer-to-peer verification (for example, Bitcoin technology can only handle three to seven transactions per second), the processing time for transactions on the blockchain will grow as the number of blocks keeps growing. Scalability may therefore prove to be a substantial barrier to the investigation of and possible widespread adoption of blockchain-based educational solutions.[49]

The difficulty associated with innovating

According to Thayer (2018), blockchain businesses are usually "prone to failure and abandonment with upwards of 90% never coming to fruition." This is due to the fact that blockchain technology is currently developing quickly. According to one of the findings, "the realization of these benefits and disruptions is likely to take a longer time than the current hype would suggest." The development of blockchain-based educational solutions, according to academics, requires adopting a pilot mentality, and all stakeholders engaged in the process should routinely do detailed risk assessments.

Table 3: A list of difficulties encountered while adopting blockchain-based educational solutions.

Challenge	Description
Innovation	The success rate of blockchain-based educational solutions may be impacted by the relative youth of the technology....
Market adoption	The delayed market adoption some such developments might be attributed to a lack of faith in technology and a lack of knowledge about how to fully utilize the potential of blockchain-based educational solutions....
Scalability	The relatively slow transaction rates of blockchains may pose challenges for the worldwide expansion of blockchain-based educational solutions...
Data privacy and security	It may be challenging to maintain security and anonymity on the blockchain....
Legal	The European Union's General Data Protection Regulation (GDPR) and California's Consumer Privacy Act of 2018 (CCPA) might place limitations on blockchain transactions containing personally identifiable information. As an added complication, the legal definition of "personal data" is hazy at best.

Discussion. This part emphasizes the effectiveness of our methods as well as certain details that weren't included in the earlier sections. The purpose of this study is to develop a function that increases blockchain scalability without sacrificing security. The aforementioned numerical and analytical results show how the SecuSca technique we recommend promotes scalability and enables users to store more transactions by freeing up space on their local disk. Despite this, SecuSca still has opportunity for development. For instance, the blockchain should continue to function correctly even if some nodes delete transactions from the local chain they are utilizing. Despite the fact that nodes share their states, a node must still obtain the required information from another node in order to verify a transaction if it is not already on its local chain. The

consensus protocol must incorporate inter-shard communication methods. The diversity of applications across numerous industries is expanding over time. The academic community makes up a major portion of the market. A trustworthy privacy protection technology is needed to protect a sizable amount of important educational and teaching data as well as the involved student privacy data when digitizing education and teaching processes, such as the creation and implementation of a student information management system. The names, addresses, and other personally identifying details of the pupils are included in this data. In addition to its technological advantages, blockchain technology offers a wide range of practical applications. [50] Some of the people who have benefited from blockchain technology in education who were interviewed for this paper assert that if major multinational corporations and/or governments don't start using and valuing academic digital credentials in the very near future, they may go extinct within the next five years. As a result, the demand for credentials that are backed by blockchain technology may increase given that lifelong learning is becoming more and more important in a society that is driven by fast technological innovation.

CONCLUSION

A distinctive blockchain design that balances scalability and security leads to a blockchain with increased storage capacity overall. We created a dynamic sharding method that views the optimization of the blockchain as a problem to be resolved in order to maintain its level of security while increasing its capacity. A number of simulation-based research projects have been dabbled in by us. The research's findings have been encouraging and represent a substantial advancement over the state of blockchain technology today. In the future, we want to look at querying our newly built blockchain to have access to the data. This will be a part of our next work. It's critical to modernize instructional strategies, educational resources, and delivery mechanisms in order to modernize education through the use of technology. Computer technology, multimedia technology, big data, artificial intelligence, and network information technology will all be heavily utilized throughout the process of informatizing the educational system. The fact that this information or data typically

contains a sizable quantity of vital information pertaining to education and training as well as the private and personal information of students makes it necessary for it to be stored and managed appropriately. The student information management system is one of the education and teaching information management systems that came out of this. This system is set up to thoroughly process and store this data. To lessen the significant amount of administrative labor involved in managing student information, the school developed a management system called the student information management system. The primary function of the student information management system inside of educational institutions is to handle student data. The upkeep of student data should ideally be mechanized, scientifically standardized, and systematized as the primary objective and obligation, respectively. Computers are used by the student learning management system to store and organize the many different types of student data. India's continued commitment to developing its educational system and infrastructure is closely tied to the introduction and widespread usage of the student information management system in that nation. Due to the fact that the procedure will entail a large quantity of educational and instructional information about students as well as information about students' private lives, a trustworthy data security technology will need to be linked in order to secure the security of the student information management system. Blockchain technology, a data security technique, connects significant data and information pieces that are temporally tied to one another. The study concentrated on efforts that support lifelong learning (BitDegree, Odem.io), projects that deal with certification and identity management (Digital Credentials Consortium, Open Source University, BCDiploma), and projects that deal with certification and identity management. The study concentrated on blockchain applications for education..)

REFERENCES

[1] Ali Alammary, A., Alhazmi, S., Almasri, M., Gillani, S.: Blockchain-based applications in education: a systematic review. Appl. Sci. 9(12), 2400 (2019)

[2] Arenas, R., Fernandez, P.: CredenceLedger: A Permissioned Blockchain for Verifiable Academic Credentials (2018)

[3] Chen, G., Xu, B., Lu, M., Chen, N.S.: Exploring blockchain technology and its potential applications for education. Smart Learn. Environ. 5(1), 1 (2018)

[4] Farah, J.C., Vozniuk, A., Rodríguez-Triana, M.J., Gillet, D.: A Blueprint for a BlockchainBased Architecture to Power a Distributed Network of Tamper-Evident Learning Trace Repositories (2018)

[5] Franzoni, A.L., Cárdenas, C., Almazan, A.: Using Blockchain to Store Teachers' Certification in Basic Education in Mexico (2019)

[6] Ghaffar, A., Hussain, M.: BCEAP - A Blockchain Embedded Academic Paradigm to Augment Legacy Education through Application (2019)

[7] Gilda, S., Mehrotra, M.: Blockchain for Student Data Privacy and Consent (2018)

[8] Yumna, H., Khan, M.M., Ikram, M., Ilyas, S.: Use of blockchain in education: a systematic literature review. In: Intelligent Information and Database Systems, January 2019

[9] Han, M., Li, Z., He, J., Wu, D., Xie, Y., Baba, A.: A Novel Blockchain-based Education Records Verification Solution (2018)

[10] Al Harthy, K., Al Shuhaimi, F., Al Ismaily, K.K.J.: The Upcoming Blockchain Adoption in Higher-Education: Requirements and Process (2019)

[11] Petersen, K., Feldt, R., Mujtaba, S., Mattsson, M.: Systematic mapping studies in software engineering. In: Proceedings of the 12th International Conference on Evaluation and Assessment in Software Engineering, June 2008

[12] Kanan, T., Obaidat, A.T., Al-Lahham, M.: SmartCert BlockChain Imperative for Educational Certificates (2019)

[13] Lizcano, D., Lara, J.A., White, B., Aljawarneh, S.: Blockchain-Based Approach to Create a Model of Trust in Open and Ubiquitous Higher Education (2019)

[14] P. Yeoh, "Regulatory issues in blockchain technology," Journal of Financial Regulation and Compliance, vol. 25, no. 2, pp. 196–208, 2017.

[15] M. Benchoufi and P. Ravaud, "Blockchain technology for improving clinical research quality," Trials, vol. 18, no. 1, pp. 335–35, 2017.

[16] E. Ittay, "Blockchain technology: transforming libertarian cryptocurrency dreams to finance and banking realities," Computer, vol. 50, no. 9, pp. 38–49, 2017.

[17] S. Saberi, M. Kouhizadeh, and J. Sarkis, "Blockchain technology: a panacea or pariah for resources conservation and recycling?" Resources, Conservation and Recycling, vol. 130, no. 30, pp. 80-81, 2018.

[18] Y. Li, J. Wei, J. Yuan, Q. Xu, and C. He, "A decentralized music copyright operation management system based on blockchain technology," Procedia Computer Science, vol. 187, pp. 458–463, 2021.

[19] Bartolomé Pina, A.R., Torlà, C.B., Quintero, L.C. and Segura, J.A.2017. "Blockchain en Educación: Introducción y crtica al estado de la cuestión [Blockchain in education: introduction and critical review of the state of the art]," RevistaElectrónica de TecnologiaEducativa, 61: a363. doi: https://doi.org/10.21556/edutec.2017.61, accessed 28 April 2020.

[20] Chowdhury, M.J.M., Colman, A., Kabir, M.A., Han, J. and Sarda, P. 2018. "Blockchain versus database: A critical analysis," 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/ 12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), pp. 1,348–1,353. doi: https://doi.org/10.1109/TrustCom/BigDataSE.2018.00186, accessed 28 April 2020.

[21] Holotescu C. Understanding blockchain opportunities and challenges. in Conference proceedings of» eLearning and Software for Education «(eLSE). " Carol I" National Defence University Publishing Househttps. 2018. Available from: //www.ceeol.com/search/article-detail?id=669617

[22] Adejo OW. E-learning to m-learning: framework for data protection and security in cloud infrastructure. Int J Inf Technol Comput Sci(IJITCS). 2018;10(4):1–9.

[23] Alammary, et al. (2019). Management of elearning platforms security. eLearning & Software for Education. 2016;(1)

[24] Rahman A. Cloud based E-learning, security threats and security measures. Indian Journal of Science and Technology. 2016;9(48):1–8

[25] Devine (2015). IGI Global. 2020. Available from: //bit.ly/3a1yc6k.

[26] Mihai I, Pruna CS, Petrica G, National Defence University. A COMPREHENSIVE ANALYSIS ON CYBER-THREATS AGAINST ELEARNING SYSTEMS. In: The International Scientific Conference eLearning and Software for Education. 2017. doi:10.12753/2066-026X-17-225.

[27] Bhatia M, Maitra J, IEEE. E-learning Platforms Security Issues and Vulnerability Analysis. In: International Conference on Computational and Characterization Techniques in Engineering & Sciences (CCTES).. 2018.

Available from:
https://doi.org/10.1109/CCTES.2018.8674115.

[28] Ali, M.S.; Vecchio, M.; Pincheira, M.; Dolui, K.; Antonelli, F.; Rehmani, M.H. Applications of Blockchains in the Internet of Things: A Comprehensive Survey. IEEE Commun. Surv. Tutor. 2019, 21, 1676–1717. https://doi.org/10.1109/COMST.2018.2886932.

[29] Saura, J.R.; Ribeiro-Soriano, D.; Palacios-Marqués, D. Setting Privacy "by Default" in Social IoT: Theorizing the Challenges and Directions in Big Data Research. Big Data Res. 2021, 25, 100245. https://doi.org/10.1016/j.bdr.2021.100245.

[30] Li, R.; Song, T.; Mei, B.; Li, H.; Cheng, X.; Sun, L. Blockchain for large-scale internet of things data storage and protection. IEEE Trans. Serv. Comput. 2018, 12, 762–771.

[31] Arcadius Tokognon, C.; Gao, B.; Tian, G.Y.; Yan, Y. Structural Health Monitoring Framework Based on Internet of Things: A Survey. IEEE Internet Things J. 2017, 4, 619–635. https://doi.org/10.1109/JIOT.2017.2664072.

[32] Dorri, A.; Kanhere, S.S.; Jurdak, R.; Gauravaram, P. LSB: A Lightweight ScalableBlockchain for IoT security and anonymity. J. Parallel Distrib. Comput. 2019, 134, 180 – 197. https://doi.org/10.1016/j.jpdc.2019.08.005.

[33] Zamani, M.; Movahedi, M.; Raykova, M. RapidChain: Scaling Blockchain via Full Sharding. In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. Association for Computing Machinery, 2018; p. 931–948. https://doi.org/10.1145/3243734.3243853

[34] Zhang, L.; Wu, Q.; Domingo-Ferrer, J.; Qin, B.; Zeng, P. Signatures in hierarchical certificateless cryptography: Efficient constructions and provable security. Inf. Sci. 2014, 272, 223 – 237. https://doi.org/10.1016/j.ins.2014.02.085

[35] Guo, J.; Yang, W.; Lam, K.Y.; Yi, X. Using Blockchain to Control Access to Cloud Data. In International Conference on Information Security and Cryptology; Springer: Cham, Switzerland, 2018; pp. 274–288

[36] Kamil, I.A.; Ogundoyin, S.O. An improved certificateless aggregate signature scheme without bilinear pairings for vehicular ad hoc networks. J. Inf. Secur. Appl. 2019, 44, 184–200. https://doi.org/10.1016/j.jisa.2018.12.004

[37] Mehedi, S.T.; Anwar, A.; Rahman, Z.; Ahmed, K.; Rafiqul, I. Dependable Intrusion Detection System for IoT: A Deep Transfer Learning-based Approach. IEEE Trans. Ind. Inform. 2022, 1, 1. https://doi.org/10.1109/TII.2022.3164770.

[38] Dongre, J.G.; Tikam, S.M.; Gharat, V.B. Education degree fraud detection and student certificate verification using blockchain. Int. J. Eng. Res. Technol. 2020, 9, 300–303.

[39] Neisse, R.; Steri, G.; Fovino, I.N.; Baldini, G. SecKit: a model-based security toolkit for the internet of things. Comput. Secur. 2017, 54, 60–76.

[40] Neisse, R.; Steri, G.; Nai-Fovino, I. A blockchain-based approach for data accountability and provenance tracking. In Proceedings of the ACM 12th International Conference on Availability, Reliability and Security, Vienna, Austria, 17–20 August 2021; p. 14.

[41] Dorri, A.; Kanhere, S.S.; Jurdak, R.; Gauravaram, P. Blockchain for IoT security and privacy: The case study of a smart home In Proceedings of the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Big Island, HI, USA, 13–17 March 2017; pp. 618–623.

[42] Hyperledger Architecture Volume 1. Introduction to hyperledger business blockchain design philosophy and consensus. accessed on May 20, 2021 https://www.hyperledger.org/wpcontent/uploads/2017/08/Hyperledger Arch WG Paper 1 Consensus.pdf

[43] Mohammad Javad Amiri, Divyakant Agrawal, and Amr El Abbadi. On sharding permissioned blockchains. In IEEE International Conference on Blockchain, Blockchain 2019, Atlanta, GA, USA, July 14-17, 2019, pages 282–285. IEEE, 2019

[44] Mohammad Javad Amiri, Divyakant Agrawal, and Amr El Abbadi. Sharper: Sharding permissioned blockchains over network clusters. CoRR, abs/1910.00765, 2019.

[45] Jing Chen and Silvio Micali. Algorand: A secure and efficient distributed ledger. Theor. Comput. Sci., 777:155–183, 2019.

[46] Hung Dang, Tien Tuan Anh Dinh, Dumitrel Loghin, Ee-Chien Chang, Qian Lin, and Beng Chin Ooi. Towards scaling blockchain systems via sharding. In Proceedings of the 2019 International Conference on Management of Data, SIGMOD Conference 2019, Amsterdam, The Netherlands, June 30 - July 5, 2019, pages 123–140. ACM, 2019.

[47] Derek Leung, Adam Suhl, Yossi Gilad, and Nickolai Zeldovich. Vault: Fast bootstrapping for the algorand cryptocurrency. In 26th Annual Network and Distributed System Security Symposium, NDSS 2019, San Diego, California, USA, February 24-27, 2019. The Internet Society, 2019

[48] Yuan Lu, Qiang Tang, and Guiling Wang. Generic superlight client for permissionless blockchains. CoRR, abs/2003.06552, 2020.

[49] Loi Luu, Viswesh Narayanan, Chaodong Zheng, Kunal Baweja, Seth Gilbert, and Prateek Saxena. A secure sharding protocol for open blockchains. In Edgar R. Weippl, Stefan Katzenbeisser, Christopher Kruegel, Andrew C. Myers, and Shai Halevi, editors, Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, October 24-28, 2016, pages 17–30. ACM, 2016

[50] Petar Maymounkov and David Mazi`eres. Kademlia: A peer-to-peer information system based on the XOR metric