ISSN (Online): 2583-648X

IJIRID

International Journal of Ingenious Research, Invention and Development

An International, High Impact Factor, Double-Blind Peer-Reviewed, Open-Access, Multidisciplinary Online Journal

Volume 3 | Issue 2 | April 2024

www.ijirid.in

Implementation of Blockchain-Based Higher Education Credit Platform

Tushar Pawade[1], Fatebahadur Nandwanshi[2], Abhishek Pinge[3], Shailesh Rathod[4], Shreya Mendhe[5], Prof. A. D. Shah[6]

[1,2,3,4,5]*Undergraduate Student, Sipna College of Engineering and Technology, Amravati, India*

[6]*Assistant Professor, Sipna College of Engineering and Technology, Amravati, India*

Abstract: *The paper proposed a novel blockchain-based system for higher education credential management, aiming to revolutionize verification and transfer processes. Current methods often suffer from inefficiencies and vulnerabilities, necessitating a more secure and efficient solution. Leveraging blockchain's decentralized and immutable ledger, the proposed system ensures the integrity and security of academic records. Institutions can issue digital credentials via smart contracts, stored securely on the blockchain, simplifying verification. Moreover, the platform facilitates seamless credit transfer, enhancing interoperability and privacy. Ultimately, this system promises to foster trust, efficiency, and innovation in higher education.*

Keywords: IoT, Blockchain with IoT, Security, etc.

I. INTRODUCTION

Based on the idea of the European Credit Transfer and Accumulation System (ECTS) this dissertation proposes a blockchain-based higher education credit platform. The proposed system can exploit the advantages of the blockchain, as a decentralized design [5], giving security, anonymity, longevity, integrity, transparency, immutableness and system simplification [7], to create a trusted proof credit and grading system. As a proof of concept, this dissertation will present a prototype implementation of the platform.

The scientific contribution is to provide a distributed and interoperable architecture model for the higher education credit system which addresses a viewpoint for students, institutions, universities and companies. Potential employers can benefit from the proposed system. Students can take advantage of having their completed course history in a single and transparent view, as well as universities that have this data accessible and up to date, regardless of a student's educational origins. On the other hand, different organizations (such as employers, universities, etc.) as potential users of the system, can validate the provided information after a student's permission is obtained [9].

1. Motivations

There is further concern about cybercriminals trying to hack the university's databases to alter the data. Moreover, corrupt officials may be bribed to illegally change a student's academic data without fulfilling the requirements. So, the basic motivation behind this dissertation is to propose a higher education credit platform. It constitutes a trusted, decentralized higher education credit and grading system that can offer a viewpoint for students and higher education institutions

DOI: 10.5281/zenodo.11061377

(HEIs) [12], as well as for other potential stakeholders such as companies, institutions and universities.

2. Objectives

The main objectives of the higher education credit platform are:

- To facilitate planning, delivery and evaluation of study programs.
- To facilitate student mobility by recognizing prior learning achievements, qualifications, experience and learning periods.

II. LITERATURE SURVEY

1. Background

A Blockchain can be referred to as a distributed database, that chronologically stores a chain of data packed into sealed blocks in a secure and immutable manner. The chain of blocks, also called a ledger, is constantly growing, thus new blocks are being appended to the end of the ledger, whereby each new block holds a reference (more precisely a hash value) to the content of the previous block. The content of the blocks can be predefined or randomly generated by the blockchain users. Nevertheless, the data is structured into so-called transactions according to the predefined structure of the blockchain and is cryptographically sealed.

The public key encryption mechanism is used to ensure the security, and thus consistency, irreversibility and non-repudiability of the distributed ledger content. Before the sealing of a data block, a cryptographic one-way hash function is applied (e.g., SHA256), ensuring anonymity, immutability and compactness of the block. The ledger and its contents are replicated and synchronized across multiple peers in a P2P network [11], therefore becoming a distributed ledger. Although the blockchain is a part of distributed ledger technologies (DLT), not all DLT employ a chain of blocks. We will henceforth refer to the above-mentioned description of the technology as the blockchain.

There are three main types of blockchains:
(1) public – permissionless,
(2) private - permission, and
(3) consortium blockchains.

The permissionless blockchain type emphasizes the public part, hence all the blockchain data is accessible and visible to the public. However, some parts of the blockchain could be encrypted to preserve a participant’s anonymity [2]. Furthermore, in these public blockchain types, everyone can join the network as a network node. Examples of such a blockchain are the Bitcoin and the Ethereum blockchains. On the contrary, a private blockchain enables only chosen nodes to join the network, thus being regarded as a form of a distributed but still centralized network [2]. The consortium blockchain is a mixture of the two and enables only a selected group of nodes to participate in the distributed consensus process [1].

2. Related Work

[4] Muhamed Turkanovic, Marko H olbl, Kristjan Ko si c, Marjan Heri cko and Aida Kami sali c, selected the ARK Blockchain as the underlying technology of our EduCTX platform. ARK is not only a cryptocurrency but is also an ecosystem meant for blockchain mass adoption. By building the EduCTX platform on top of a highly secure and fast ARK core blockchain, and integrating key decentralized technologies, the platform becomes a user-university-friendly ecosystem to increase the adoption of blockchain technology as a whole.

The main reasons for selecting the ARK technology as a code base are its flexibility and open sources, and the overall availability of client API implementations. At the time of writing, ARK provides more than 12 different programming languages for client implementations, thus enabling other actors (HEIs, students, employers) to join the platform in the programming language of their choice.

In [5], Yli-Huumo J, Ko D, Choi S, Park S, and Smolander K have conducted a systematic mapping study to collect all relevant research on Blockchain technology. the objective is to understand the current research topics, challenges and future directions regarding Blockchain technology from a technical perspective. authors have extracted 41 primary papers from scientific databases.

The results show that focus in over 80% of the papers is on the Bitcoin system and less than 20% deals with other Blockchain applications including e.g., smart contracts and licensing. The majority of research focuses on revealing and improving the limitations of Blockchain from privacy and security perspectives, but many of the proposed solutions lack concrete evaluation of their effectiveness. Many other Blockchain scalability-related challenges including throughput and latency have been left unstudied.

In [6], Alex Roehrs, Cristiano André da Costa, and Rodrigo da Rosa Righi presented a distributed architecture proposal named OmniPHR. The solution seeks to address recurrent needs in adopting PHR by patients and healthcare providers. The OmniPHR purpose consists of partitioning PHR in data blocks distributed on a P2P network [10]. Thereby OmniPHR maintains characteristics of datablocks distribution having spread copies of these parts on the network.

The user can access PHR data through different devices. Consequently, OmniPHR is a mobile-health model that uses the diversity of computing devices connected to the patients or to the environment where they are inserted at any time, to be part of a collaborative and distributed network. The PHR data appear to be centralized from the logical viewpoint of the patient and healthcare provider but are physically decentralized.

III. SYSTEM DESIGN

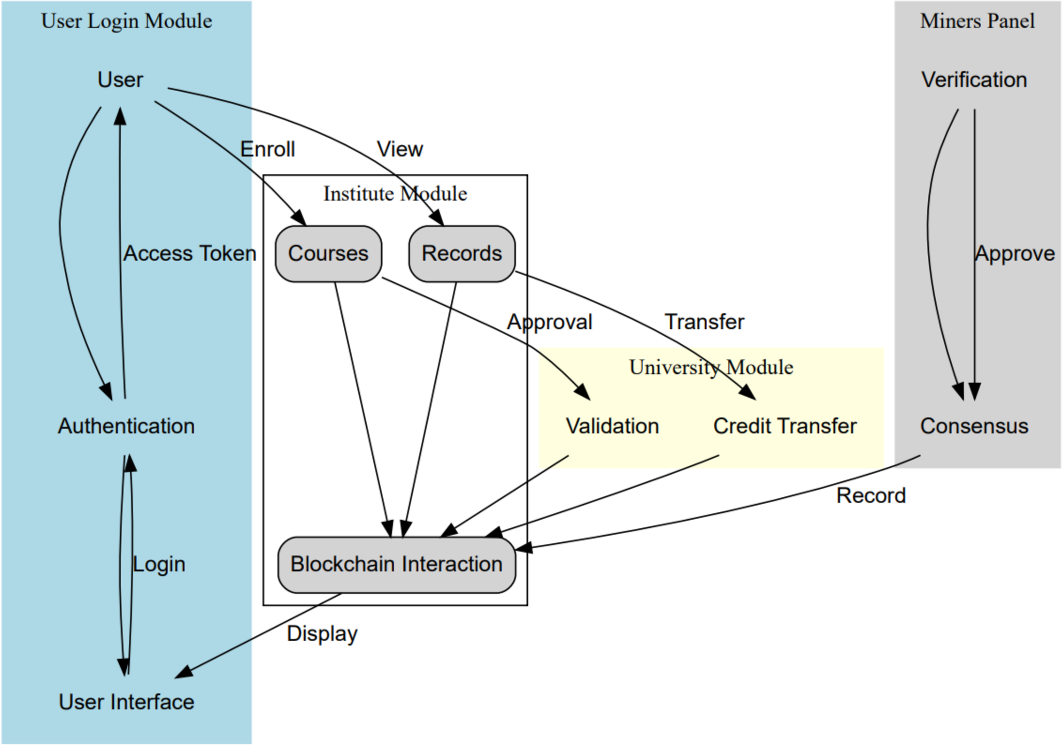


Figure 1: Block Diagram of a Blockchain-Based Higher Education Credit Platform

IV. IMPLEMENTATION

Blockchain Technology

The integration of blockchain technology into a higher education credit platform aims to revolutionise credential verification and transfer processes. Traditional methods often encounter inefficiencies and security risks, prompting the need for a more robust solution. By harnessing the decentralized and immutable nature of blockchain, the proposed platform ensures the integrity and security of academic records. Through the use of smart contracts, academic institutions can issue and manage digital credentials [3, 8], which are securely stored on the blockchain. This not only streamlines verification processes but also enables seamless credit transfer between institutions, fostering interoperability and data privacy. Ultimately, the integration of blockchain technology promises to enhance trust, efficiency, and innovation in higher education credential management.

SHA-1 Algorithm

The SHA-1 (Secure Hash Algorithm 1) is a cryptographic hash function that produces a fixed-size hash value (160 bits) from input data of arbitrary size. It is designed to be a one-way function, meaning it is computationally infeasible to reverse the hash value back to the original input data. SHA-1 is commonly used in various security applications, such as digital signatures, message authentication codes, and checksums, to ensure data integrity and authenticity.

DOI: 10.5281/zenodo.11061377

In the SHA-1 algorithm, the input data is processed in blocks of 512 bits. The algorithm performs a series of logical operations, including bitwise operations such as AND, OR, and XOR, as well as rotations and additions modulo 2^32 [3]. These operations are applied to the input data in multiple rounds to generate the final hash value.

The algorithm also includes a series of constant values and functions that are used in each round to introduce non-linearity and ensure the security of the hash function. One of the key benefits of the SHA-1 algorithm is its cryptographic strength, which means it is highly resistant to collision attacks. A collision occurs when two different inputs produce the same hash value. While SHA-1 has been deprecated due to vulnerabilities discovered in its collision resistance, it is still widely used in legacy systems and applications. However, for new applications, it is recommended to use more secure hash functions, such as SHA-256 or SHA-3, which offer higher levels of security and resistance to collision attacks.

Steps of SHA-1 Algorithm

1. **Padding:**
   Append padding bits to the message so that its length is congruent to 448 modulo 512. The padding starts with a single 1-bit, followed by zeros, and ends with a 64-bit representation of the original message length.

2. **Dividing into Blocks:**
   Divide the padded message into blocks of 512 bits (64 bytes).

3. **Initialization:**
   Initialize the SHA-1 hash buffer (5 32-bit words, often represented as A, B, C, D, E) with the hash values from the SHA-1 standard.

4. **Processing Blocks:**
   For each block, extend the 512-bit block into an 80-word array of 32-bit words. For words 16 to 79, apply a function to mix the words.

5. **Initialize Variables:**
   Initialize variables for this chunk: a = A, b = B, c = C, d = D, e = E.

6. **Main Loop:**
   Perform 80 iterations of a compression function. In each iteration, update the variables a, b, c, d, and e using bitwise operations and logical functions.

7. **Update Hash Buffer:**
   After processing each block, update the hash buffer by adding the current hash values to the computed values of a, b, c, d, and e.

DOI: 10.5281/zenodo.11061377

8. **Output:**
   The final hash value is the concatenation of the five 32-bit words in the hash buffer, typically represented as a 160-bit hexadecimal number.

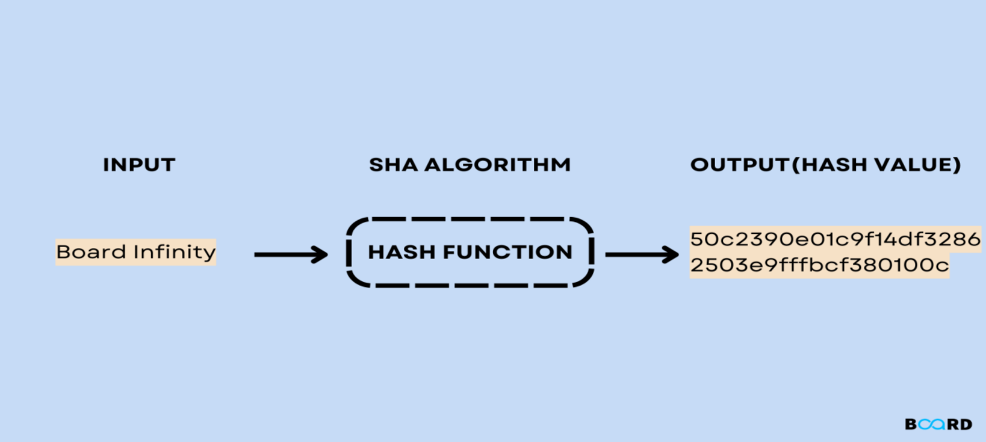
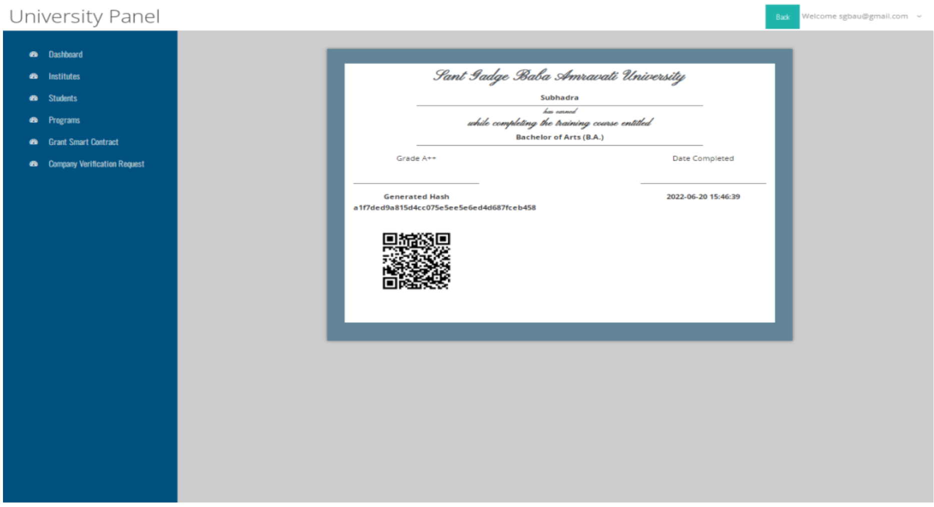


Figure 2: Application of Data Mining

V. RESULT

The integration of blockchain technology into higher education for the creation of a blockchain-based credit platform presents a promising solution to the challenges associated with traditional credential management and credit transfer processes. By leveraging blockchain's decentralized, immutable, and transparent nature, this platform offers a secure and efficient system for issuing, storing, and verifying digital credentials. Through smart contracts and cryptographic techniques, academic institutions can streamline credential verification and facilitate seamless credit transfer between institutions. The platform promotes trust, transparency, and interoperability, thereby addressing the shortcomings of traditional systems.

Blockchain Powered Certificate



Sant Gadge Baba Amravati University

Subhadra

has earned

while completing the training course entitled

Bachelor of Arts (B.A.)

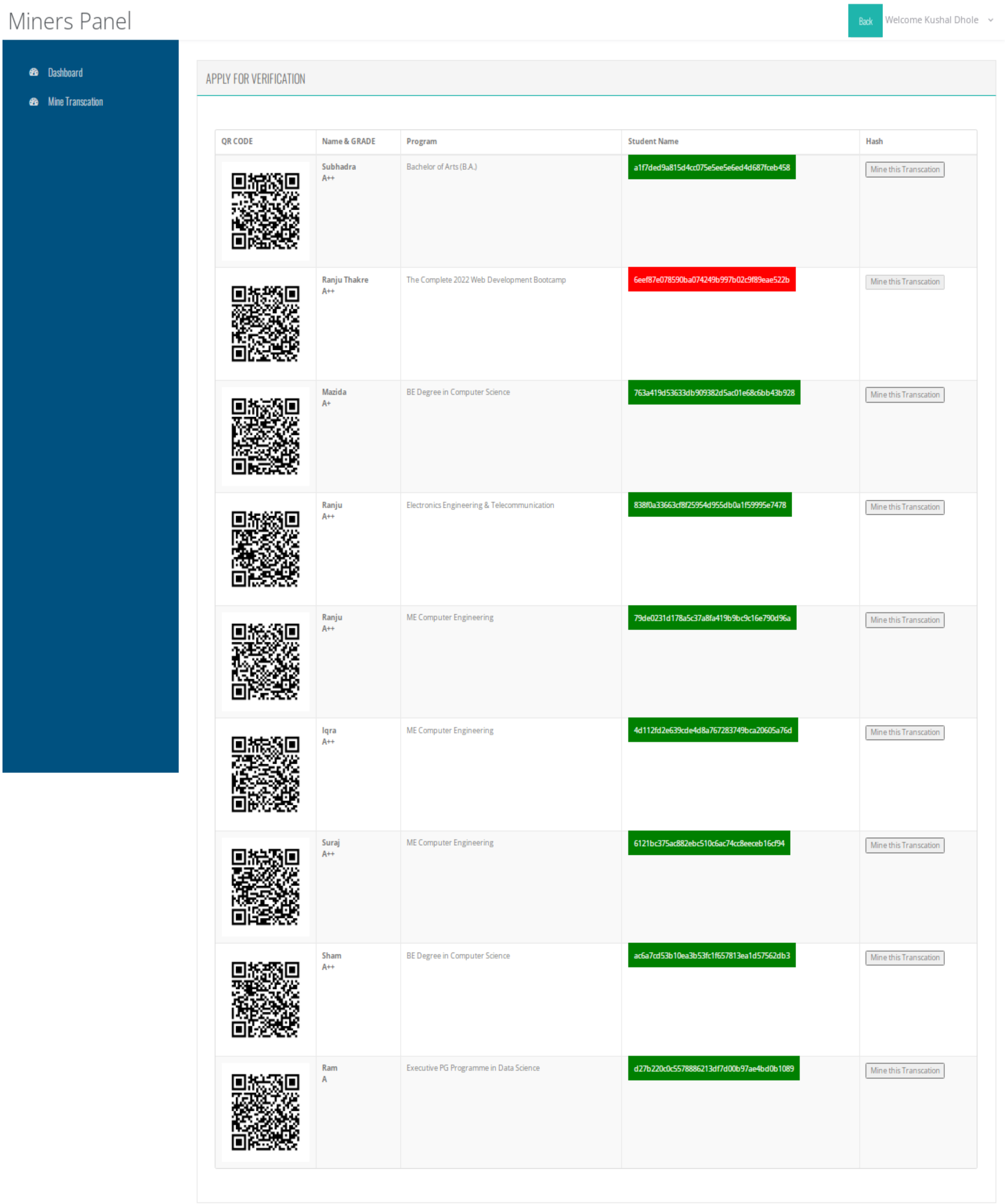
Grade A++

Date Completed

Generated Hash
a1f7ded9a815d4cc075e5ee5e6ed4d687fceb458

2022-06-20 15:46:39

Miners Panel



APPLY FOR VERIFICATION

QR CODE	Name & GRADE	Program	Student Name	Hash
	Subhadra A++	Bachelor of Arts (B.A.)	a1f7ded9a815d4cc075e5ee5e6ed4d687fceb458	Mine this Transcation
	Ranju Thakre A++	The Complete 2022 Web Development Bootcamp	6eef87e078590ba074249b997b02c9f89eae522b	Mine this Transcation
	Mazida A+	BE Degree in Computer Science	763a419d53633db909382d5ac01e68c6bb43b928	Mine this Transcation
	Ranju A++	Electronics Engineering & Telecommunication	838f0a33663cf8f25954d955db0a1f59995e7478	Mine this Transcation
	Ranju A++	ME Computer Engineering	79de0231d178a5c37a8fa419b9bc9c16e790d96a	Mine this Transcation
	Iqra A++	ME Computer Engineering	4d112fd2e639cde4d8a767283749bca20605a76d	Mine this Transcation
	Suraj A++	ME Computer Engineering	6121bc375ac882ebc510c6ac74cc8eeceb16cf94	Mine this Transcation
	Sham A++	BE Degree in Computer Science	ac6a7cd53b10ea3b53fc1f657813ea1d57562db3	Mine this Transcation
	Ram A	Executive PG Programme in Data Science	d27b220c0c5578886213df7d00b97ae4bd0b1089	Mine this Transcation

DOI: 10.5281/zenodo.11061377

ISSN (Online): 2583-648X

IJIRID

International Journal of Ingenious Research, Invention and Development

An International, High Impact Factor, Double-Blind Peer-Reviewed, Open-Access, Multidisciplinary Online Journal

Volume 3 | Issue 2 | April 2024

www.ijirid.in

Database Table Structure

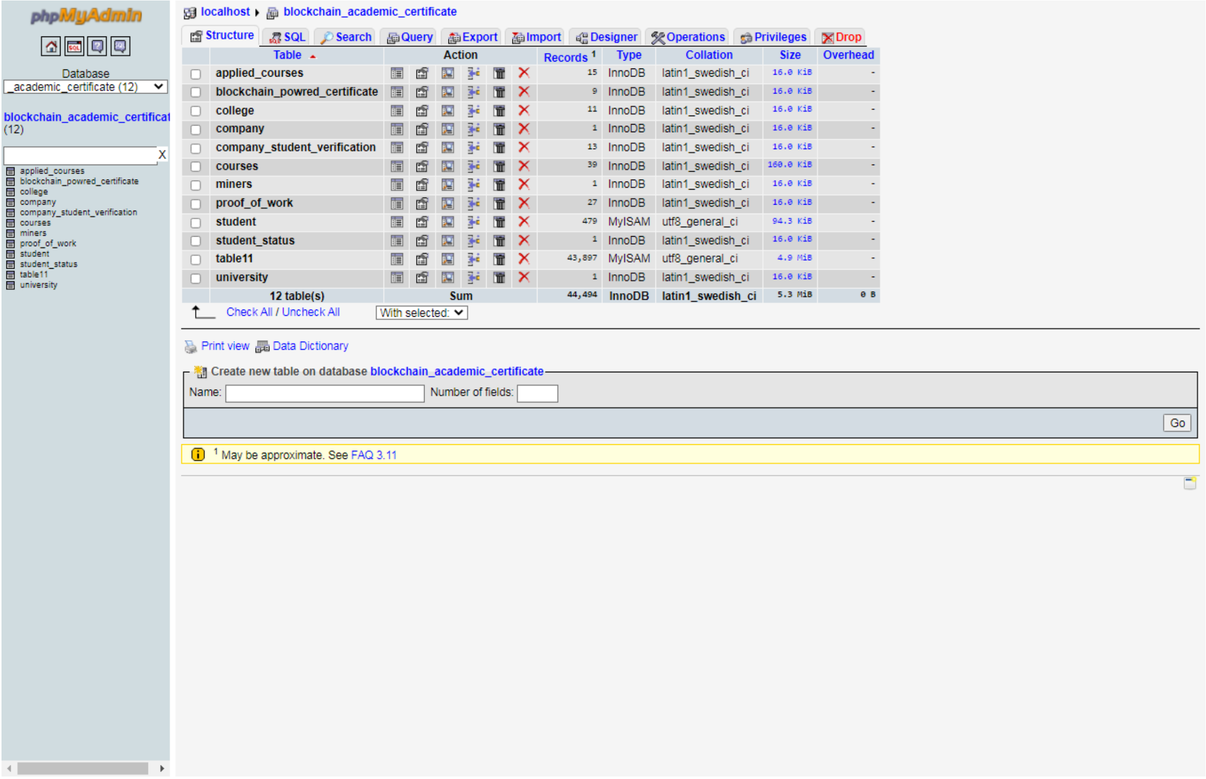


	Table	Action	Records [1]	Type	Collation	Size	Overhead
□	applied_courses		15	InnoDB	latin1_swedish_ci	16.0 KiB	-
□	blockchain_powred_certificate		9	InnoDB	latin1_swedish_ci	16.0 KiB	-
□	college		11	InnoDB	latin1_swedish_ci	16.0 KiB	-
□	company		1	InnoDB	latin1_swedish_ci	16.0 KiB	-
□	company_student_verification		13	InnoDB	latin1_swedish_ci	16.0 KiB	-
□	courses		39	InnoDB	latin1_swedish_ci	160.0 KiB	-
□	miners		1	InnoDB	latin1_swedish_ci	16.0 KiB	-
□	proof_of_work		27	InnoDB	latin1_swedish_ci	16.0 KiB	-
□	student		479	MyISAM	utf8_general_ci	94.3 KiB	-
□	student_status		1	InnoDB	latin1_swedish_ci	16.0 KiB	-
□	table11		43,897	MyISAM	utf8_general_ci	4.9 MiB	-
□	university		1	InnoDB	latin1_swedish_ci	16.0 KiB	-
	12 table(s)	Sum	44,494	InnoDB	latin1_swedish_ci	5.3 MiB	0 B

Create new table on database blockchain_academic_certificate

Name: ______ Number of fields: ______

[1] May be approximate. See FAQ 3.11

VI. CONCLUSION

The implementation of a blockchain-based higher education credit platform holds immense potential to transform the landscape of credential management and credit transfer in the higher education sector. By embracing blockchain technology, institutions can enhance the security, efficiency, and transparency of credential verification processes, ultimately benefiting students, academic institutions, and employers alike. While challenges such as regulatory compliance and scalability may need to be addressed, the future of blockchain in higher education appears promising. Continued research and collaboration will be crucial in realizing the full potential of blockchain technology in revolutionizing higher education credentialing.

REFERENCES

[1] N. Zhumabekuly Aitzhan and D. Svetinovic, “Security and Privacy in Decentralized Energy Trading through Multi-signatures, Blockchain and Anonymous Messaging Streams,” IEEE Transactions on Dependable and Secure Computing, pp. 1–1, 2016. [Online]. Available: http://ieeexplore.ieee.org/document/7589035/

[2] E. Mengelkamp, B. Notheisen, C. Beer, D. Dauer, and C. Weinhardt, “A blockchain-based smart grid: towards sustainable local energy markets,” Computer Science - Research and Development, pp. 1–8, 8 2017. [Online]. Available: http://link.springer.com/10.1007/s00450- 017-0360-9

[3] Muhamed Turkanovic, Marko H olbl, Kristjan Ko si c, Marjan Heri cko and Aida Kami sali c,” EduCTX: A blockchain-based higher education credit platform”, IEEE ACCESS, VOL. X, NO. Y, Z,2018.

DOI: 10.5281/zenodo.11061377

[4] G. Coulouris, J. Dollimore, T. Kindberg, and G. Blair, Distributed Systems: Concepts and Design (5th Edition). Addison-Wesley, 2011.

[5] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, “Where Is Current Research on Blockchain Technology? A Systematic Review,” PLOS ONE, vol. 11, no. 10, p. e0163477, 10 2016. [Online]. Available: https://doi.org/10.1371/journal.pone.0163477

[6] R. Alex, C. A. Costa, and R. R. Righi, “OmniPHR: A distributed architecture model to integrate personal health records,” Journal of Biomedical Informatics, vol. 71, pp. 70–81, 7 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1532046417301089

[7] O. S. Kemkar and P. Kalode, “Formulation of Distributed Electronic Patient Record (DEPR) System Using Opener Concept,” International Journal of Engineering Innovations and Research IJEIR, vol. 4, pp. 85–89, 2012. [Online]. Available: http://www.ijeir.org/index.php/issue?view=publication&task=show&id=418

[8] C. He, X. Fan, and Y. Li, “Toward Ubiquitous Healthcare Services With a Novel Efficient Cloud Platform,” IEEE Transactions on Biomedical Engineering, vol. 60, no. 1, pp. 230–234, 1 2013. [Online]. Available: http://ieeexplore.ieee.org/document/6324392/

[9] Z. Shae and J. J. Tsai, “On the Design of a Blockchain Platform for Clinical Trial and Precision Medicine,” in Proceedings - International Conference on Distributed Computing Systems. IEEE, 6 2017, pp. 1972–1980. [Online]. Available: http://ieeexplore.ieee.org/document/7980138/

[10] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, “MeDShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via Blockchain,” A Blockchain-Based Higher Education Credit Platform, Page 55 IEEE Access, Vol. 5, 2017. [Online]. Available: http://ieeexplore.ieee.org/document/7990130/

[11] M. Mettler, “Blockchain technology in healthcare: The revolution starts here,” in 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom). IEEE, 9 2016, pp. 1-3. [Online]. Available: http://ieeexplore.ieee.org/document/7749510/

[12] Azaria, A. Ekblaw, T. Vieira, and A. Lippman, “MedRec: Using blockchain for medical data access and permission management,” in Proceedings - 2016 2nd International Conference on Open and Big Data, OBD 2016. IEEE, 8 2016, pp. 25– 30. [Online]. Available: http://ieeexplore.ieee.org/document/7573685/

DOI: 10.5281/zenodo.11061377