Journal of Sensors, IoT & Health Sciences
ISSN: 2584-2560
Vol.02(01), Mar 2024, pp.17-27.

Research Article

A Secure Blockchain Based Student Certificate Generation and Sharing System

S. Venkatramulu[1,*], K. Vinay Kumar[2], Md. Sharfuddin Waseem[3], Sabahath Mahveen[4], Vaishnavi Vaidya[5], Tulasi Ram Reddy[6] and Sai Teja Devarakonda[7]

[1,2] Associate Professor, Department of Computer Science and Engineering, KITSW (Affiliated to Kakatiya University), Warangal, Telangana,506015, India.

[3] Assistant Professor, Department of Computer Science and Engineering, KITSW (Affiliated to Kakatiya University), Warangal, Telangana,506015, India.

[4,5,6,7]Students, Department of Computer Science and Engineering, KITSW (Affiliated to Kakatiya University), Warangal, India – 506015.

[*]Corresponding Author: S. Venkatramulu. Email: svr.cse@kitsw.ac.in

Received: 24/02/2024; Accepted:22/03/2024.

Abstract: In order to handle and validate academic credentials in a distributed, secure manner, block-chain technology is employed for generation of student academic certificates. This paper addresses the three important aspects of the application i.e. need for generation of student academic certificate, sharing it over the secure digital platform i.e. dapp which stores and exchange academic credentials with third parties for verification i.e. selective disclosure of certificates. Additionally, it discusses the necessity of authenticating certificates through blockchain technology by which management and ownership of the certifications is done securely. The users of the application include the universities, students and verifiers. The dapp consists of two profiles i.e. universities who issue the academic certificates by filling out the student details; students who receive them, view and manage the certificates over the student's dashboard and can also share them with third party. The suggested method offers controlled exchange of student information and upholds information privacy through blockchain in addition to minimizing paper-based tasks. Issuing, sharing and verifying academic certificates while improving privacy and saving the time are the important aspects of the application.

Keywords: Data sharing; distributed systems; computer network; certificate blockchain; ethereum.

1 Introduction

Educational credentials have a high level of credibility since they serve as auxiliary indicators of the human capital of those who possess them. The skills, knowledge, information, and aptitudes acquired via education are referred to as human capital. Educational credentials are extremely important in the workplace since they serve as a proof of the holders' abilities, responsibility, and dedication, in addition to their knowledge, experience, and skills. When a university is authorized to grant such certificates, it is acknowledged that educational credentials are regarded as legitimate whenever they are provided by the institution as being genuine. People frequently fabricate fake certificates to conceal their academic credentials since they are so valuable [1-4]. When used to certificate verification processes through a rigid architecture, block-chain technology ensures authenticity and significantly cuts down on time when compared to colleges employing centralized systems to oversee the entire procedure, which takes days to complete.

The programme also makes use of blockchain technology's low transaction latency, average speed at which certificates are issued, and low latency for sharing and checking electronic certifications [5]. Data that are stored and managed centrally are more susceptible to theft, exploitation, and destruction. Blockchain technology's decentralization, immutability, scalability, trust lessness, and managed privacy are seen as potential solutions for issues with data sharing [6]. Additionally, by minimizing the consumption of paper, the digital transformation of certificate issuance and verification participation greatly aids in mitigating adverse climate impacts.

The major objective is to provide a user-friendly system that combines blockchain technology to certificate verification processes in a way that ensures authenticity and significantly reduces time [7-9]. It aims to study the applicability of decentralized application for digital certificate verification of students [10]. The application offers two primary services: issuing electronic certificates and distributing them, which is certificate verification.

2 Literature Survey

Numerous academics have recognized the potential of blockchain technology for exchange of information in field of education. Decentralization, simplicity, and permanence are the three main characteristics of the blockchain that make it suited for educational applications [11]. Blockchain technology allows for decentralized transactions by serving as an immutable record. Many new industries are finding uses for blockchain technology. Some of these include financial services, reputation systems, and the IoT [13].

These qualities, for instance, can guarantee that the system of higher education won't ever be corrupted and enable the public verification of student data. Users can put out intellectual work and ensure reputational rewards by sharing and protecting the data at the same time [14]. In order to illustrate how blockchain technology is being applied in education, Li and Han presented their research in 2019[15]. The blockchain was utilized to store student records with the aim of ensuring data dependability and security [16]. Smart contracts were also used to transfer data.

Evaluation of work focused on proving economics and safety of suggested technology [17]. The authors suggested that future works incorporate elements that make it easier to certify academic records for use by foreign organizations or employers and to recall academic records [18]. Using blockchain technology, According to Turkanovi et al. developed a platform for higher education credits that is widely trusted [19]. Oliver et al. created a blockchain-based solution with a user-friendly interface for automatically verifying university degrees [20].

The proposed plan calls for the graduate to be responsible for safeguarding a key that controls certification sharing. Economic effectiveness and sustainability are the main objectives of the suggested approach [21]. In 2016, Sharples and Domingue proposed a blockchain-based system to maintain an immutable distributed ledger of scholarly work and creative output. They maintained student data on a personal blockchain. They stored academic data in their study on a distributed ledger to prevent certificate forgery [22].

3 Proposed System

The proposed system will make it easy for students to access the information they need. The Blockchain Network securely stores certificates. The ideal candidate will be given the ideal job opportunity. The use of fake certificates will not cause problems. Students must attest their certificates for verification each time. This could be prevented. Access to certificates is simple. After being placed on the Blockchain Network, the certificates become immutable. Therefore,

Certificate Data won't be changed. The certificate's manual verification requires more time.

This problem will be resolved using a digital certificate verification system that verifies certificates quickly. Distributed database is present in blockchain. Therefore, security is greater in comparison to other technologies. The background checks will take less time thanks to online document authentication. The idea of online academic document verification will benefit many students, institutions, and employers as the world becomes more digital. According to this approach, the admin or university will be in charge of utilizing a DApp to upload the student's academic information into the blockchain, after which a special Certificate Id will be issued and given to the relevant student's email. If the business is seeking to hire a candidate.

The student or applicant must give the recruiter their special Certificate Id, which they use to view and confirm the legitimacy of a certificate. Since the Certificates are stored on the blockchain, Data Security and Immutability are strictly upheld. Overall, In the near future, there will be a significant impact on the development of a Decentralized application that is universally available for students/employers to examine and verify academic certificates without any third-party involvement that is very user-friendly, as well as efficient.

The major uses of this system are losing the certificates such as misplaced certificates and damaged, this situation will make it difficult for them to apply for work or study, verify all certificates manually and it take long time especially for employer and organizations, the production of fake certifications will be resolved. Few issues in this system are strict limitation on the number of transactions that the network can process in any given second. Ethereum blockchain can process only 15 transaction per second, or 900 transactions per minute. Figure 1shows architecture for proposed system

A digital certificate is basically a JSON Object that has the fields our cert-issuer code needs in order to store it on the blockchain. which can be verified using a hash that can be produced for it. the blockchain storage technique the development of a system to store and maintain digital certificates makes use of Ethereum. React.js and Node.js, two cutting-edge web development tools, are used to create an interface that makes it easy for users to see, handle, and check documents online.

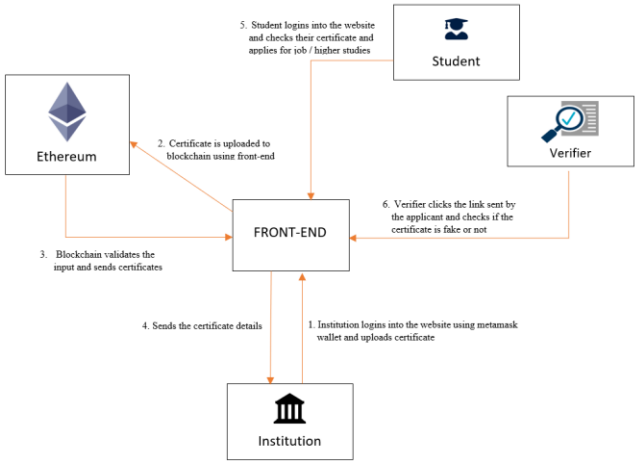

Figure 1: Architecture for Proposed System

4 Implementation

There are now several steps involved in issuing and sharing graduation certificates, the majority of which must be completed manually, and it is a time taking process. Examination

committee updates student records at completion of each course, and once all graduation requirements have been satisfied, the student's certification is prepared for distribution. When a student applies for a job opportunity or higher education overseas, the following steps must be taken before the graduation certificate can be issued and shared:

The graduation certificate is issued, distributed, and confirmed online in this proposal. The exam committee will transfer all the courses the student took, including with their grades, from system database to blockchain once they have successfully fulfilled the course prerequisites.

The university receives the student's request for issuance of certification when student submits it via the dapp application. After amending the student data and approving the procedure, the authorized body grants authorization to produce the certification. The learner then uses a decentralized application to receive the e-certificate, which may be exported as a pdf and shared with third party, in the following step. The issue of a certification is illustrated.

Any person wishing to validate an issued e-certificate may do so by using a dapp that has been designed for this purpose. The verifier could be a hiring department within a business, a different educational facility, or even the graduates themselves. A student may ask for a specific URL with an expiration date from the online application, which a third party can use to verify the e-certificate. Figure 2 shows homepage of DApp

The implementation modules of this system are, In the controller it contains the JavaScript files that handles the content sent by the users. In the model it contains all MongoDB Schema files written in JavaScript and use mongoose driver for interaction with MongoDB atlas. Scalable apps and highly accessible web applications are made using MongoDB, a document database. Agile development teams favor it because of its flexible schema approach.

In the routes Contains all files written in JavaScript with express framework for handling all routes. In the util it Contains all the feature related files. Example, Email (send grid). In the Client it Contains all the react files which make frontend of the project. JavaScript library and framework ReactJs were developed by Facebook. It is used to quickly and efficiently construct interactive user interfaces and web apps in comparison to utilizing vanilla JavaScript.

All of the Solidity-based smart contracts are housed in the Contracts section. When certain conditions are satisfied, these are the programs that will help to run the programs automatically. Commonly, they are used to automate the execution of contracts, allowing the parties to know the result instantly, without any middleman or delay.

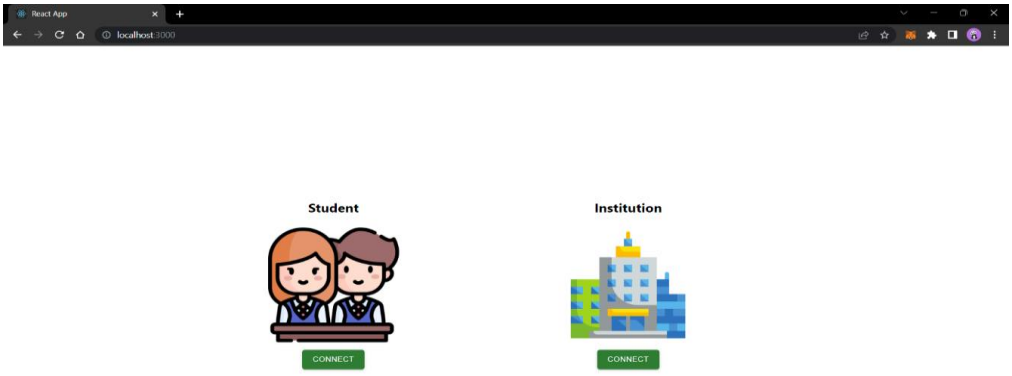

Figure 2: Homepage of DApp

Blockchain based Student Certificate Management System is a pure Decentralized App. One kind of application that utilizes a decentralized network and integrates a smart contract with a frontend user interface is called a decentralized application (dapp). The underlying code of a decentralized app executes on a decentralized peer-to-peer network. Figure 3 shows issuing certificate.

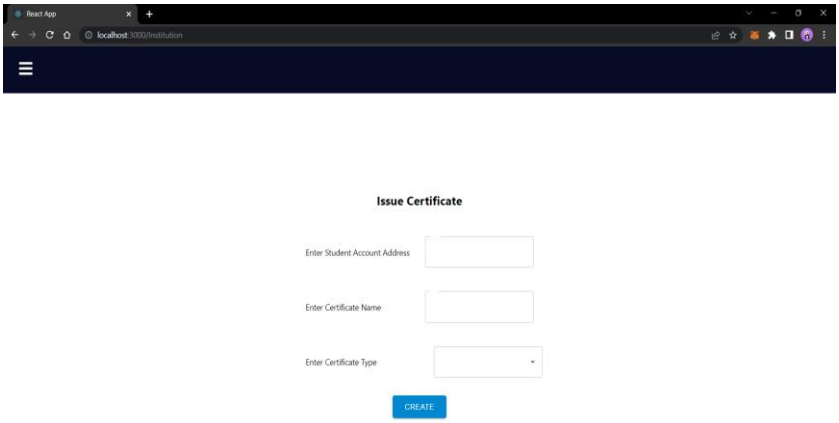

Figure 3: Issuing Certificate

Our application uses Ethereum network to run smart contract. Smart contract is deployed on goerli test net. Our frontend application is built by using react library. React is java script library for web and native user interface. Figure 4 shows transaction details.

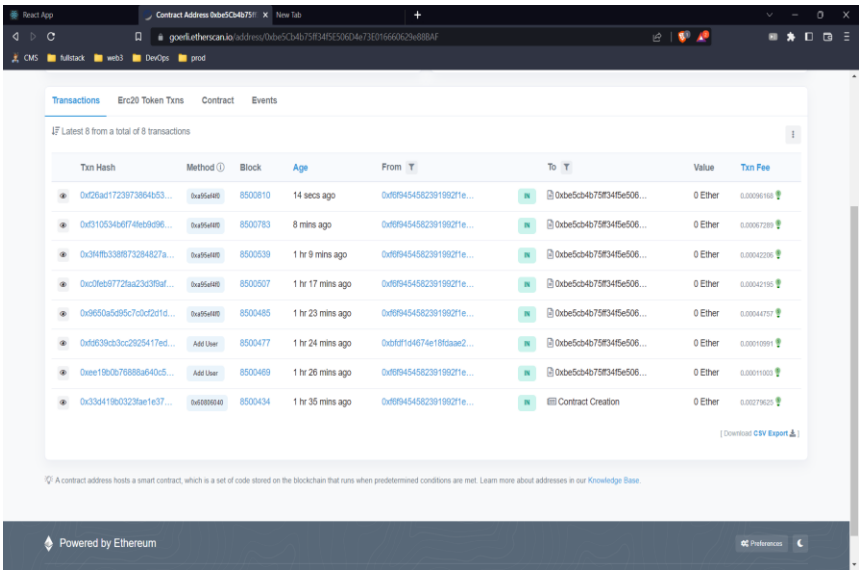

Figure 4: Transaction details

Our application has two 2 users. One is a student who gets the certificate and other is organization who issues the certificate. First the user has to create an account using meta mask

wallet. Meta mask is client-side software which used to perform the transactions. Figure 5 shows generated certificates.

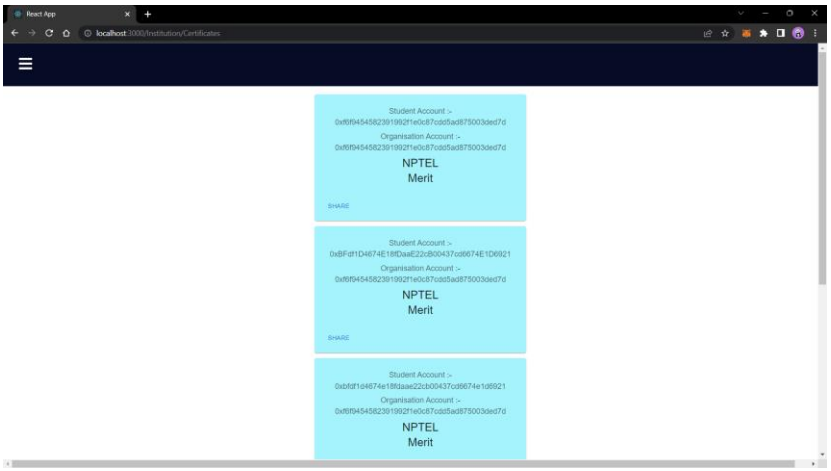

Figure 5: Generated Certificates

Organization admin logins with the meta mask wallet and create a certificate to the student. All the certificate created or issued for the user can be seen after student logging in to the website. From here student can share the certificate with the other users. Figure 6 shows students dashboard.

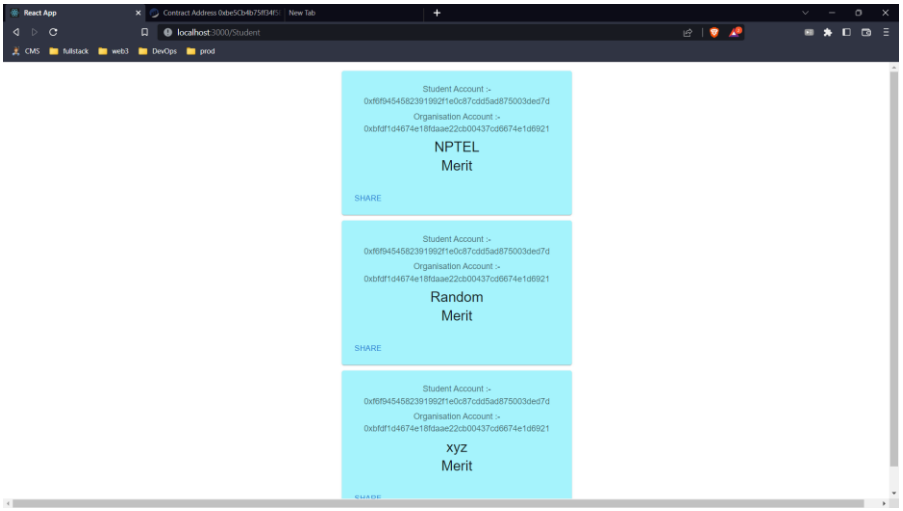

Figure 6: Students Dashboard

Packages used in front end: -

Moralis: - Moralis is 3rd party package used to connect to meta mask and to smart contract on test net.

React-moralis: - Package that provides react hooks that can be used to connect with meta mask and smart contract on test net.

React-router-dom: - Package that provides multi page application support to react.

Styled-Components: - This package makes a component at runtime that can be used as normal html tag.

Hard hat: - The Ethereum software development environment is called Hard Hat. Included in its many parts is an integrated development environment (IDE) for creating, editing, building, testing, and releasing decentralized applications (dApps) and smart contracts.

Meta mask: - MetaMask offers the safest and easiest method to connect to apps that run on the blockchain. When you use the new decentralized web, you're in charge at all times.

- ETHEREUM

Ethereum is a global, open-source platform that supports decentralized applications. On Ethereum, you can write code that controls the value of digital assets, runs flawlessly, and can be accessed from any location in the world. Using Ethereum, a decentralized blockchain technology, to construct a peer-to-peer network, it is possible to securely execute and certify application code for smart contracts.

To facilitate direct communication between parties, smart contracts do away with the need for a reliable central authority. Full ownership and visibility of transaction data is achieved by participants due to the immutability, verifiability, and safe transmission of records throughout the network.

Ethereum allows users to send and receive transactions through their accounts. The native currency of Ethereum, Ether, must be used to sign and pay for transactions before they can be finalized on the network. The Ethereum ecosystem is growing quickly as a result of the increasing demand for decentralized applications (dApps) in sectors such as technology, gaming, art and collectibles (NFTs), and finance (decentralized finance, or DeFi applications). Ethereum will also implement sharding at some point to make it more scalable.

- WEB3.JS

A collection of libraries known as Web3.js may allow you to interact with local or distant Ethereum nodes, use a protocol, or establish an IPC connection.

Web 3 is built on top of blockchain technology and cryptocurrencies. Although blockchain and virtual currencies are essential to the decentralized web, other technologies such as the internet of things, augmented and virtual reality, and virtual reality rely on them as well. The third version of the internet, known as Web3, will be built on blockchain technology.

- MONGODB ATLAS

The global cloud information service for modern applications is MongoDB Atlas. It offers accessibility, measurable results, and adherence to the most stringent information security and privacy requirements**.** You can rest easy when you use MongoDB Atlas to set up, manage, and fix your installations on any cloud provider (AWS, Azure, GCP, etc.). When it comes to cloud-based MongoDB administration, MongoDB Atlas is your best bet. Several cloud services use MongoDB Atlas, a developer data platform. Our fully managed cloud database for modern apps is at the heart of everything. The most effective approach to use MongoDB, the most popular non-relational database, is Atlas.

- TEST NETWORK FOR ETHEREUM

Test net for Ethereum (or test network). Developers typically use test networks to execute "tests" on their software systems or applications. Test net money has no value. A group of nodes used to test the Ethereum protocol is known as a test net. On the test nets, tests are carried out to make sure the protocol is operating as intended. In that they are meant to test the protocol in a regulated setting, test nets are similar to mocks. We create smart contracts and test them in a test net in the same way that we create tests in a unit test. Building tests and delivering them on the

test net is far less expensive than writing smart contracts and deploying them on the main net. This is due to the fact that we must pay gas fees which are actual financial costs before we can deploy our smart contracts on the main net.

- HARDHAT

It is an Ethereum development environment. Compile your contracts and run them on a development network. A development environment called Hardhat aids programmers in building, deploying, and troubleshooting DApps on the Ethereum network. Hardhat is the name of the Ethereum software development environment. Together, these components make up a complete development environment that may be used to deploy, edit, compile, and debug your smart contracts and dApps. The main thing you deal with when utilizing Hardhat Runner is Hardhat. It is an adaptable and scalable task manager that facilitates the organization and automation of ongoing processes necessary for creating smart contracts and decentralized apps (dApps).

- ETHERSCAN

Users can use Etherscan to look up and verify smart contracts; Use the Etherscan gas tracker to determine Ethereum gas fees. Look up a single transaction made from any Ethereum wallet, view cryptocurrency assets kept in or linked to a public wallet address, and observe live Ethereum blockchain transactions, and keep track of how many smart contracts they have authorized with their password (DApps).

An Ethereum blockchain block explorer goes by the name of Etherscan. Users can quickly view and look up transactions and blocks. Details like the date and hash of each block and transaction are also provided. Etherscan is like Google for Ethereum, you might say.

Etherscan is the name of a network explorer for the Ethereum blockchain. The website allows you to search through various types of on-chain information, including transactions, blocks, wallet addresses, smart contracts, and more. As far as free Ethereum blockchain viewers go, it's among the most popular. By utilizing Etherscan, you can gain a deeper comprehension of your interactions with blockchain, various wallets, and DApps.

Protecting yourself and spotting suspicious behavior are two additional uses for this data. To use Etherscan, paste a wallet address, transaction ID (TXID), contract address, or any identifier into the search field.

Depending on what you're looking at, you'll see different information, but for the most part, you'll see connected transactions, addresses, timestamps, and quantities.

- GANACHE

Ganache provides a private Ethereum blockchain environment that allows users to replicate the Ethereum blockchain and interact with smart contracts on their own custom blockchain. In order to build and test on a local network, Ganache can assist you in establishing your own Ethereum blockchain. You can use Ganache, a private Ethereum blockchain environment, to create a copy of the Ethereum blockchain and interact with smart contracts on your own private blockchain. Some of Ganache's best features are as follows: Ganache is a powerful mining control tool that shows results from the blockchain log. It includes an Ethereum blockchain environment, an integrated block explorer, a desktop program, and a command-line tool.

- EMAIL DELIVERY SERVICE SENDGRID

A cloud-based service called SendGrid offers help with email distribution for companies. The service handles a variety of emails, including newsletters, friend requests, sign- up confirmations, and shipping notifications.

Through the use of SendGrid, a cloud-based SMTP provider, you may send emails without worrying about maintaining email servers. The technical specifics are fully handled by SendGrid, including infrastructure scaling, ISP outreach, reputation monitoring, whitelist services, and real-time analytics. Table 1 shows comparative analysis of tools used.

Table 1: Comparative analysis of tools used

CRITERIA:	BLOCKCHAIN TYPE	READ PERMISSIONS	CONSENSUS	IMMUTABLE	IDENTITY	DISTRIBUTION
ETHEREUM	public blockchain	public	permissionless	no tampering	anonymous	high
WEB3JS	defi: decentralized blockchain	authorized permissions	permissionless	no tampering	pseudo anonymous	medium
MONGODB ATLAS	blockchain ledger	flexible	distributed no-sql database	yes	pseudo anonymous	high
ETHERSCAN	public data	public	permissioned	yes	fully anonymous	high
TESTNET	public/ private	public/ private	permissionless	-	anonymous	medium

5 Results

In this paper, the security, validity, and secrecy of certificates are increased with the deployment of the blockchain-based student certificate management system. The key benefit of the proposed system above the conventional approaches is high throughput of completed issued and confirmed certification. This digital certification will speed up the process of issuing and verifying e-Certifications.

Two crucial performance indicators regular the lag time, which is likewise measured in seconds, and the time it takes to issue a certificate, both in seconds were used to evaluate the acceptance of blockchain-based student certifications. The length of time it takes blockchain network to process a transaction is referred to as latency. Student certificates were issued utilizing the Ethereum-based electronic certification system that was trialed.

Through a smart contract, the proposed e-certificate system offers controlled data sharing. While the blockchain only has information related to e-certifications. On the other hand, access to confidential data is permitted with consent of blockchain-authorized user. The number of validators in the system determines how long it takes to verify each certificate.

Students can share their certificates generated by the university easily to the third parties using the same decentralized application developed within less time.

6 Conclusion

A framework for using blockchain to store and share graduate credentials was developed as a result of this effort. These certifications are made unchangeable, private, and decentralized by using blockchain to store them, which is certified by various bodies. In this study, we suggested and put into practice an electronic certificate distribution method. The blockchain was used to develop the system.

The blockchain can capture hundreds of transactions in a matter of seconds. A system based on smart contracts was suggested to secure and oversee the certifications' rollout.

The system's testing showed that distributing certificates with low latency might preserve anonymity. The main benefits of the proposed system over more established methods for issuing and verifying certification are its high throughput of successfully completed certifications. The traditional approach takes somewhere between a week and ten days, whereas the e-certification is provided and verified in under a minute. The suggested system can also regulate data sharing, maintaining client privacy. Additionally, this approach enables greater transparency in how colleges do their business. Last but not least, the digitalization of certification issuance and verification contributes significantly to reverse the harmful effects of climate change by consuming less paper.

7. Future Scope

Blockchain has wide range of applications with the feature of chain of blocks containing information. Some of the applications of block chain are Assets Management, Cross-Border payments, Healthcare, Cryptocurrency, Generation of birth and death certificate, Copy right and Royalties. In future, to the students after generation of certificate we can also include more secured two factor authentications.

Acknowledgement: Not Applicable.

Funding Statement: The author(s) received no specific funding for this study.

Conflicts of Interest: The authors declare no conflicts of interest to report regarding the present study.

References

[1] R. F. Ghani, A. A. Salman, A. B. Khudhair and Laith Aljobouri, "Blockchain-based student certificate management and system sharing using Hyperledger fabric platform," *Periodicals of Engineering and natural sciences*, vol. 10, 2022.

[2] Q.Liu, Q.Guan, X. Yang, H. Zhu, G. Green et al, (2018), "Education- Industry Cooperative System Based on Blockchain," *2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN)*, Shenzhen, China, pp. 207-211, 2018.

[3] Z.Zheng, S. Xie, H. Dai, X.Chen and Huaimin Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," *2017 IEEE 6th International Congress on Big Data*, Honolulu, HI, USA, pp. 557-564, 2017.

[4] T. T. Huynh, T. Tru Huynh, D. K. Pham and A. Khoa Ngo, "Issuing and Verifying Digital Certificates with Blockchain," *2018 International Conference on Advanced Technologies for Communications (ATC)*, Ho Chi Minh City, Vietnam, pp. 332-336, 2018.

[5] R. N. Nortey, L. Yue, P. R. Agdedanu and M. Adjeisah, "Privacy Module for Distributed Electronic Health Records (EHRs) Using the Blockchain," *2019 the 4th IEEE International Conference on Big Data Analytics*, Suzhou, China, pp. 369-374, 2019.

[6] M.J.M. Chowdhury, A. Colman, M. A. Kabir, J. Han and P.Sarda, "Blockchain as a Notarization Service for Data Sharing with Personal Data Store," *12th IEEE International Conference on Big Data Science and Engineering*, New York, NY, USA, pp. 1330-1335, 2018.

[7] A. Kamisalic, M.Turkanovic, S.Mrdovic and M. Hericko, “A Preliminary Review of Blockchain based solutions in Higher Education,” *Communications in Computer and Information Science*, vol 1011, 2019.
[8] S. Makridakis and K. Christodoulou, "Blockchain: Current challenges and future prospects/applications," *Future Internet*, vol. 11, no. 12, pp. 258, 2019.
[9] S.Omar Saleh, O. Ghazali and M. E. Rana, “Blockchain Based Framework for Educational Certificates Verification,” *Journal of critical reviews*, vol. 7, no.3, 2020.
[10] A. Gayathiri, J. Jayachitra and S. Matilda, “Certificate validation using blockchain,” *IEEE 7th International Conference on Smart Structures and Systems ICSSS 2020*, Chennai, India, pp.1-4, 2020.
[11] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized Business Review*, pp. 21260, 2008.
[12] Z. A. Kamal and R. Fareed, "A Proposed hash algorithm to use for blockchain base transaction flow system," *Periodicals of Engineering Natural Sciences*, vol. 9, no. 4, pp. 657-673, 2021.
[13] D. Macrinici, C. Cartofeanu, and S. Gao, "Smart contract applications within blockchain technology: A systematic mapping study," *Telematics Informatics*, vol. 35, no. 8, pp. 2337-2354, 2018.
[14] C. Fan, S. Ghaemi, H. Khazaei, and P. Musilek, "Performance evaluation of blockchain systems: A systematic survey," *IEEE Access*, vol. 8, pp. 126927- 126950, 2020.
[15] M. Oliver, J. Moreno, G. Prieto, and D. Benítez, "Using blockchain as a tool for tracking and verification of official degrees: business model," in 29th European Regional Conference of the International Telecommunications Society (ITS): Towards a digital future: Turning technology into markets, Trento, Italy, Trento, Italy, vol. 10, 2018.
[16] H. Li and D. Han, "EduRSS: A blockchain-based educational records secure storage and sharing scheme," *IEEE Access*, vol. 7, pp. 179273-179289, 2019.
[17] S. Jayalakshmi, "The Impact of the Blockchain on Academic Certificate Verification System-Review," *EAI Endorsed Transactions on Energy Web*, pp. e35, 2021.
[18] A. Alammary, S. Alhazmi, M. Almasri and S. Gillani, "Blockchain-based applications in education: A systematic review," *Applied Sciences*, vol. 9, no. 12, p. 2400, 2019.
[19] Z. A. Kamal and R. Fareed, "Data retrieval based on the smart contract within the blockchain," *Periodicals of Engineering Natural Sciences*, vol. 9, no. 4, pp. 491-507, 2021.
[20] H. Zhao, M. Zhang, S. Wang, E. Li, Z. Guo, and D. Sun, "Security risk and response analysis of typical application architecture of information and communication blockchain," *Neural Computing Applications*, vol. 33, no. 13, pp. 7661-7671, 2021.
[21] N. Ullah, W. Mugahed Al-Rahmi, A. I. Alzahrani, O. Alfarraj, and F. M. Alblehai, "Blockchain technology adoption in smart learning environments," *Sustainability*, vol. 13, no. 4, pp. 1801, 2021.
[22] R. Raimundo and A. Rosário, "Blockchain system in the higher education," *European Journal of Investigation in Health, Psychology Education*, vol. 11, no. 1, pp. 276-293, 2021.