Blockchain based Certificate Validation

Rachna Jain[*1], Geetika Dhand[2], Kavita Sheoran[2], Shaily Malik[2], Nishtha Jatana[2]

[1] JSS Academy of technical education, Noida, India
[2] Maharaja Surajmal Institute of Technology, New Delhi, India
Emails: rachnajain@jssaten.ac.in; geetika.dhand@gmil.com; kavita.sheoran@gmail.com; shaily.malik33@gmail.com; nishtha.jatana@gmail.com

Abstract

Certificate management is a tedious task for any university or any other organization. These schemes impose problems in Public Key Infrastructure (PKI). Checking the validity and preserving the security of these documents is of utmost importance. In this work, we have devised a blockchain-based solution for preventing malfunctioning in certificate validation which is an important step for any university. Each certificate is uploaded in its hash format and is stored using blockchain. The hashes are stored in unique transactions in nodes, which are deployed on a private network. Using the SHA-256 hashing algorithm, the certificates are uploaded into the system and can be viewed by anyone with the right credentials. Due to the usage of blockchain technology, the certificates are stored in a decentralized manner, which ensures there is no central point of failure. Any changes in the uploaded document need to be validated by other nodes. This paper also improvises that when certificate uploading is required new nodes are added, instead of modifying the past blocks. This work provides a very user-friendly app where any user with the right credentials can upload documents. In this work, digitized documents are stored using Inter Planetary File System (IPFS) which is distributed method of storage. Our theoretical analysis proves that it is a user-friendly application with the security of blockchain technology in partnership with IPFS. Only the issuer can upload documents and others can only view them. Using our proposed solution, problem of malicious certificates can be tackled with E-certification. The proposed method solves all the issues of storing, validating, and sharing documents. Chaotic Map technique is used in hash generation which is quite simple to implement. The proposed approach Chaotic Key based Certificate validation (CK-Cert) provides a hassle-free solution for certificate managements since it better manages the block size as compared to previously proposed techniques (PBCert and CertChain) as discussed with the help of graphs.

Keywords: Blockchain; Smart City; Intelligent Systems; Certificate validation; Hashing

1. Introduction

The world's population is rapidly urbanizing, which creates several economic, environmental, and social issues that have a substantial impact on many people's lifestyles [1]. Given the high population density in metropolitan areas, the idea of a "smart city" presents an opportunity for various segments of society. The idea of sustainable smart cities is to spread knowledge on and promote the best ways to use green energy sparingly. Sixty-six per cent of the world's population, as predicted by the UN (United Nations, 2015), will soon reside in large cities, posing enormous problems for social sustainability. Additionally, the consistently expanding progression of data sharing is convincing an ever-increasing number of organizations and individual clients towards the utilization of digitized reports. If an individual wants to join an organization; the certificates need to be verified and validated. This task is a cumbersome and time-consuming process.

This issue might have a remedy thanks to blockchain technology [2–5]. There are numerous other situations in which a person's presence must be determined using the issued certificates. It takes a lot of time and effort to

Doi: https://doi.org/10.54216/FPA.120204
Received: January 12, 2023 Revised: April 18, 2023 Accepted: June 14, 2023

present the original certificates every time for verification before putting back safely. The certificate must not suffer any loss or damage throughout the verification process. It is known that a person's life is literally defined by their certificates. It takes a while to find a certificate again if it is accidentally lost [6–10]. 90% of the institutions deal with these problems and offer superior intelligent services that improve quality of life. Additionally, the disorganized and tiresome approval exchanges of traditional actual archives add to inspiring individuals to utilize current methods of allowing and approving significant documents. However computerized archives are without a doubt advantageous to utilize, and demonstrating the genuineness of these records is frequently an issue of concern. The certificate verification process is an ever-occurring and tedious process [11-15]. If a person wants admission to a university, he/she needs to verify their certificates. In India, be it universities or schools; hold the student's certificates until the student leaves that institution.

At present, the record verification manner consists of human interventions and third-party observations. Since it is a tedious task and additionally, there is constantly a risk of errors and dishonesty. This approach of verification does not appear dependable and efficient. Several styles of studies stated, there are various faux files and certificates that surround the worldwide industry [16-18]. Blockchain generation can remove those problems and enhance protection by preserving complete integrity [19, 20]. Instead of producing the certificates every time in any institution, a mechanism is proposed wherein the certificates may be saved in a hashed format.

There are many problems that may arise during the certificate verification and validation process. This has led to the question of where the certificates can be stored safely without any intrusion or failure [21- 24]. Also, there is a possibility that the certificates may perish, or any other harm may affect them during the verification process. As we all know, certificates literally define our life. Thus, the online storage of certification is proposed, where any organization with the right credential can check and verify certificates, just ensuring that the certificates are valid the first time. This way, the authenticity of the certificate does not need to be verified every time.

The rest of the paper is organized as follows: Section 2 presents the related work. Section 3 presents the motivation of the work done. Section 3 explains why blockchain can be used as a validator. Section 4 gives the software requirements. Section 5 presents the proposed methodology. Section 6 presents the conclusion and limitations.

2. Related Work

The way people live engage, and conduct business has changed significantly since the advent of the Internet. The World Wide Web is now a crucial component of our everyday activities and environment, and it handles enormous volumes of data transport every day. For consumers 'privacy, much of the transmitted data should be protected because it is sensitive. In addition, authorization is necessary to accept or access a few communications and requested services. Many strategies were suggested to meet these security needs, but the Public Key Infrastructure is the most popular one (PKI). In fact, the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols, when used in conjunction with a Public Key Infrastructure, offer encryption for private communication and certificate chains for authentication.

Yao et al. [25] have discussed that in recent years, real-world assaults, like the single point of failure of the certificate authority or the disclosure of clients' private information; have shown the vulnerabilities of conventional public key infrastructure. One strategy to address the first issue involves the introduction of numerous entities to help with certificate procedures such as registration, update, and revocation. But its computation efficiency is poor. Another kind involves using log servers to make the certificate information available to the general public. However, network latency could result from log servers synchronizing their data. The suggested blockchain-based public key infrastructure plans are based on the second strategy. All certificate operations are recorded in the blockchain for public audit using this type of method. To address these two problems, the authors have developed the PBCert status validation system. The control and storage plans for revoked certificates are first separated. It leverages external data storage for the complete information about all revoked certificates and only stores the minimal control information (certificate hashes and relevant operation block height) on the bblockchain . Second, in order to protect client privacy, a cryptic response to their certificate status question is devised.

Wang et al. [26] have proposed a novel technique using the role of both web servers and Certification Authorities (CAs). In the proposed scheme, SSL/TLS web servers form a mutually reliant community that actively restrains the unrestricted power of Certification Authorities (CAs)in conventional Public Key Infrastructure (PKIs). First, a CA as well as a specific number of interdependent web servers certify the publishing key of a web server. Therefore, CAs cannot publish a certificate in the blockchain without the community of web servers' approval.

Doi: https://doi.org/10.54216/FPA.120204
Received: January 12, 2023 Revised: April 18, 2023 Accepted: June 14, 2023

Second, each web server's validated publishing key is also documented on the blockchain. It implies that a certificate's publishing is also subject to public scrutiny. In other words, the public certificate blockchain is kept up-to-date with append-only logs to track the performance of web servers and CAs.

In the proposed work, Nginx and Firefox were used to put the prototype system into action. Sending its certificate transactions to the Nginx server SSL/TLS extensions are available for browsers, and the browser used the certificate blockchain to verify the received certificates. The proposed system introduced suitable overheads in terms of storage, certificate validation delay, communication, transaction verification cost, and incentive cost, according to a study based on real-world data and experimental results.

The advantage of the scheme is that in SSL/TLS conversations, browsers use the certificate blockchain to verify the certificates. A false certificate signed by compromised CAs but not published in the blockchain will be denied. A server certificate is only accepted if it is published in an unexpired transaction. The certificate blockchain is incrementally downloaded by a browser from the P2P storage network of web servers. There is no need for SSL/TLS negotiation to complete this download.

According to the paper [27], the foundational technology for enabling secure information exchange over the Internet is public-key infrastructure (PKI). However, PKI is vulnerable to dangers because Certificate Authorities (CAs) could fail and issue end users with fake certificates as a result. The security of the relevant end-users will be in danger if a CA is compromised, as seen by numerous recent hacks. Blockchain technology, a new alternative, may be able to address some of the issues with conventional PKI systems, including the elimination of a single point of failure and quick response to CA flaws.

Imam et al. [28] described a decentralized web application for computerized record validation utilizing Ethereum blockchain-based environment in a P2P distributed storage to upgrade the confirmation process by making it more open, straightforward, and auditable. The proposed model incorporated a few strategies like public/private key cryptography, online capacity security, computerized marks, hash, distributed organizations, and confirmation of work which had made the check of any transferred records for any association easier. The hash values generated are likewise related to every person's archive. The proposed model effectively put together all the rules for an advanced record check framework by mitigating the holes and troubles in the conventional strategies in the report confirmation. In this work, the hash of the data is stored in the block, and it forms a long chain of nodes. However, if any tampering is done then its hash will change, and a mismatch with the hash value stored in the former block will occur, thereby helping us to know about the tampering of data.

Padmavati E Gadgetry et al. [29] described a model for certificate validation that focused on solving the issue of certificate counterfeiting using blockchain technology. An incontestable benefit of Blockchain has been that it will make the stage decentralized. The model has been planned to store the certificates in the block and create a hash on the solicitation of the user. When the certificates are placed in the block; then it becomes difficult to fix or alter by anyone. Placing the data in the block will likewise eliminate uncertainty about the information on the worker. The model secure cert proposed a stage which has been intended to beat issues like fake declarations by utilizing cryptographic arrangements. The block utilized cryptography strategies to guarantee security and mostly to have validation.

A. Gayathiri et al. [30] demonstrated a model for HSC, SSLC, and other academic certificates wherein the digitized certificates are produced by the institutions and provided to the students. In the first place, the paper declarations have been changed to computerized certificates. The chaotic algorithm is utilized to produce the hash code as an incentive for the digital certificates. Then, at that point, the certificates are stored in the blockchain. Further, these testaments are approved by utilizing the mobile application.

Belurgikar et al. [31] described a model for individuals who need to make, share, and send certificates containing private data, like scholastic records or advanced identifications, which should be stored with an additional layer of safety. The proposed framework is centred on the confirmation of individual portfolios utilizing the moving blockchain innovation. This is a decentralized framework that can be extended to any expert space where your personal credits and authentications are compulsory. The research work intends to make a cross-country intelligible, straightforward, and all-inclusive air to give a normalized stage to the personality of the executives in an extremely durable, straightforward, and secure way.

Masoomeh Bahrami et al. [32] discussed a model that focuses majorly on solving issues created by the forgery of academic certificates. The model provides a reliable and sealed authentication check framework. Decentralization

Doi: https://doi.org/10.54216/FPA.120204
Received: January 12, 2023 Revised: April 18, 2023 Accepted: June 14, 2023

enhances the security and power elements of the framework by staying away from weak links and eliminating the need to put trust in any single party. The proposed plan influences bblockchain based cryptographically safeguarded savvy contracts to robotize the check cycle and give straightforwardness. Furthermore, security is expected for building a quick, reliable, and cost-effective check framework [33]. Table 1 summarizes the comparative analysis of different techniques.

Table 1: Related work on various approaches of certificate management

References	Objective of the work	Advantages	Disadvantages	Conclusion
Garba,A., Chen,Z., Guan, Z. and Srivastava, G., 2021[34]	Authors have proposed domain certificate validation methodology: Lightledger	Less storage and low bandwidth requirement, hence suitable for IoT devices.	Trusted Certificate authorities can validate any domain name.	Trusted CA associated with authenticated domain name is recorded.
Y.Zhang, C.Xu, X. Lin and X.Shen, 2021[35]	Authors have proposed Certificate less public verification against procrastinating auditors (CPVPA)	Verification is time stamped on the bblockchain network	Heavy cost in local storage	Cevapi's certificate-less So does not suffer from management issues.
Y.Xu, C.Zhang, G.Wang, Z.Qinand Q.Zeng, 2021[36]	Data integrity maintain educing both bblockchain and bilinear cryptography	Bilinear cryptographic techniques removed deduplication.	This technique records both entities data outsourcing and auditors resulting in heavy cost.	Client wise de-duplication policies helps to decrease the burden of service providers.
R. Zhou, M. He and Z. Chen[37]	To preserve data privacy against Third Party	Integrity of data is efficient	Identity based schemes suffer	Remote Data Integrity checking

3. Motivation of the work

The primary objective of this research work is to build a web application that is easy to use for the end-user and at the same time provides a secure platform where certificates can be uploaded, stored, and verified by the concerned authorities. The certificate validation application focuses on scrutinizing the authenticity and integrity of the certificates that have been issued to avoid document forgery. This work focuses on implementing a system that is feasible, stable, and secure. The system is using blockchain as it is immutable and provides better security.

The proposed work provides a digital and preferred method for certificate validation rather than traditional methods. This work develops a certificate validation system that aims to store the certificates in their hash format. Another objective is to make sure that the certificates are always accessible and do not vanish due to some server

Doi: https://doi.org/10.54216/FPA.120204
Received: January 12, 2023 Revised: April 18, 2023 Accepted: June 14, 2023

failure. To ensure the safety of the certificates, the SHA-256 algorithm is implemented through blockchain technology. Adopting the immutable characteristics of blockchain, the proposed framework provides better security. Transparency is achieved since every transaction is viewable to all the other members of the network.

4. Blockchain as a Validator

In today's digital age, everything is digitalized, including academic certificates like the SSLC and HSC that are given to students in educational institutions. It is challenging for students to hold onto their degree diplomas. Verification and validation of certifications are time-consuming and difficult for the organization and institution. This work will contribute to the secure storage of the certificate in the blockchain system. The paper certificates are first transformed into digital form and then hash code value for the certificate is created using the chaotic algorithm as shown in Figure 1. However, Equation 1 shows the generation of Certificates using chaotic algorithm.

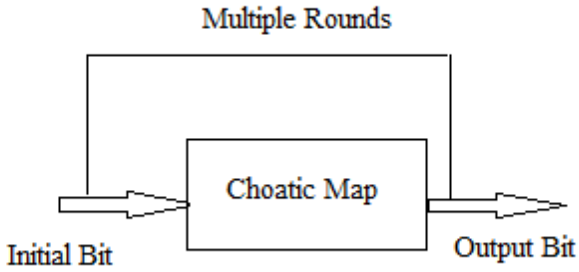

Figure 1: Hash Code value for generation of Certificates using Chaotic Map

$$x_{n+1} = \mathrm{r}_1 x_n(1 - \mathrm{x}_n) \quad (1)$$

$$x_{n+1} = \frac{r_2}{4}\sin(\pi \mathrm{x}_n) \quad (2)$$

$$x_{n+1} = \begin{cases} \frac{r_3}{2}\mathrm{x}_n if \mathrm{x}_n < 0.5 \\ \frac{r_3}{2}(1 - \mathrm{x}_n) \quad \text{if } \mathrm{x}_n \geq 0.5 \end{cases} \quad (3)$$

Where, x0 is the initial condition, r1, r2, r3 € [0, 4] are the control parameters, n is the number of iterations, and xn € [0, 1] denotes the system variable or chaotic point.

The certifications are then kept on the blockchain and the mobile application is used to validate these certificates. It can deliver a more effective and safe digital certificate validation using blockchain technology. It can obtain diplomas and achievement certificates at every stage of our professional development. As technology has developed recently, there are cases of persons impersonating and copying certificates in order to cheat. By faking their names on legitimate certificates, we see people making copies of certificates. Most institutions have already digitalized paper certificates, therefore, by including this technology at the issuing and receiving parties, the entire process may be made secure and dependable. This paper suggests a mechanism where the certificate's issuing party can utilize it to prevent certificates from being duplicated and the receiving party can verify that the certificate is valid and undamaged.

5. Software Requirements

Blockchain: A blockchain is a distributed database that is shared among the nodes of a computer network. As a database, a blockchain stores information electronically in a digital format. The innovation of a blockchain is that it guarantees the fidelity and security of a record of data and generates trust without the need for a trusted third party.

Doi: https://doi.org/10.54216/FPA.120204
Received: January 12, 2023 Revised: April 18, 2023 Accepted: June 14, 2023

Ethereum: Ethereum is a decentralized open-source Blockchain featuring smart contract functionality. At its core, Ethereum is a decentralized global software platform powered by blockchain technology. It has a token designed for use in the blockchain network, but it can also be used by participants as a method to pay for work done on the blockchain. Ethereum is designed to be scalable, programmable, secure, and decentralized.

Smart Contract: Smart contracts are a piece of code that runs on a Blockchain when a user performs some action. Smart contracts are simply programs stored on a blockchain that run when predetermined conditions are met. They typically are used to automate the execution of an agreement so that all participants can be immediately certain of the outcome, without any intermediary's involvement or time loss.

Solidity: Solidity is an object-oriented programming language for writing smart contracts. It is used for implementing smart contracts on various Blockchain platforms, most notably, Ethereum. Solidity is the primary language for blockchains running platforms. Solidity can be used to create contracts like voting, blind auctions, crowdfunding, multi-signature wallets, and many more.

Ethash: Ethash is the proof-of-work function in Ethereum-based Blockchain currencies.

IPFS: The Inter Planetary File System is a peer-to-peer network for storing and sharing data in a distributed file system. IPFS uses content-addressing to uniquely identify each file in a global namespace connecting all computing devices.

Metamask: MetaMask is an extension for accessing Ethereum-enabled distributed applications or Dapps in your browser. MetaMask allows users to store and manage account keys, broadcast transactions, and send and receive.

Ganache: Ganache is used for testing Solidity contracts on a personal Ethereum Blockchain. It by default provides an easy setup for spinning up a network with around ten users with each having100 eths on their account.

Truffle: Truffle provides easy compilation, linking, deployment, and binary management of smart contracts written in solidity language.

React: React (also known as React.js or ReactJS) is a free and open-source front-end JavaScript library for building user interfaces based on UI components.

6. Proposed Methodology

A web application has been implemented that will upload and store certificates using the blockchain's Ethereum framework. The system will help the user in verifying the certificates authenticity by comparing it with the uploaded hash and will provide the provision of uploading the hash of the certificate.

Blockchain is basically a publicly available ledger where participants enter data and certify their acceptance of the transaction via an elliptic curve digital signature algorithm (ECDSA). An elliptic curve is an equation such as

$$y^2 = x^3 + Ax + B \quad (4)$$

In equation 4, A & B are the constants. Also, A, B, x, y are usually elements of some field. Each certificate is uploaded in its hash format and is stored using blockchain. The hashes are stored as unique transactions in nodes, which are deployed on a private network. Each node maintains a copy of the transactions along with the hashes, thus making it available at any time. The certificates are hashed using the SHA-256 algorithm, and, the transaction ids are obtained using the same. Figure 2 shows an example of hash code generation.

Doi: https://doi.org/10.54216/FPA.120204
Received: January 12, 2023 Revised: April 18, 2023 Accepted: June 14, 2023

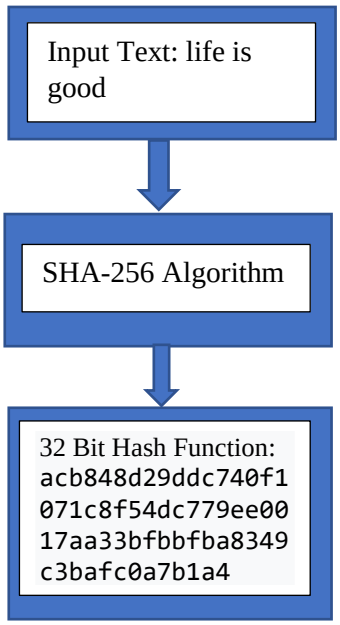

Figure 2: An Example of Hash code generation by SHA-256 Algorithm

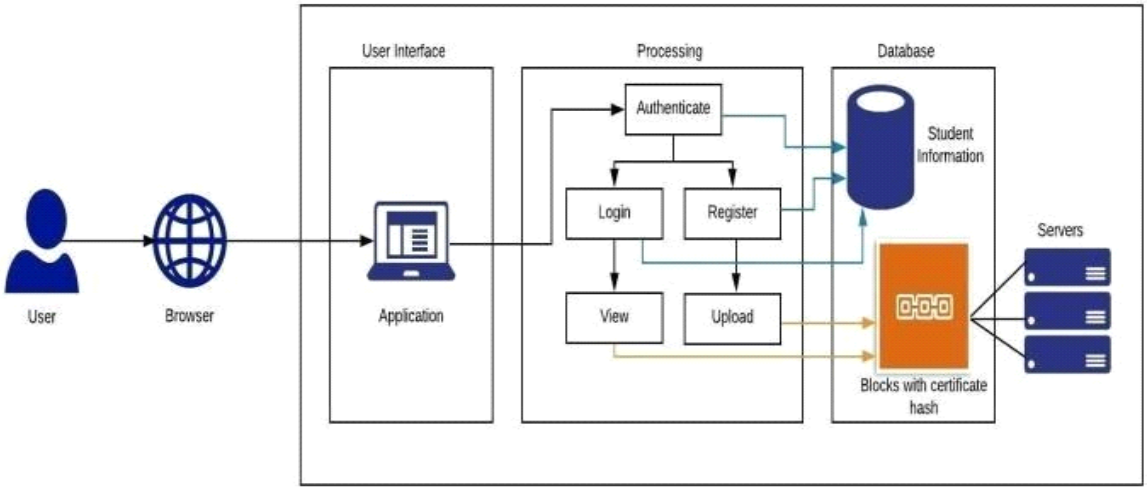

Figure 3: Proposed Framework

The proposed system consists of a platform that will help the students to upload and store their certificates in a safe and secure manner. The system is a web application, which provides decentralized storage of the certificates, and security of the certificates, through the usage of blockchain technology. The users of the system are initially verified if they are valid users. Figure 3 displays the proposed framework.

Doi: https://doi.org/10.54216/FPA.120204
Received: January 12, 2023 Revised: April 18, 2023 Accepted: June 14, 2023

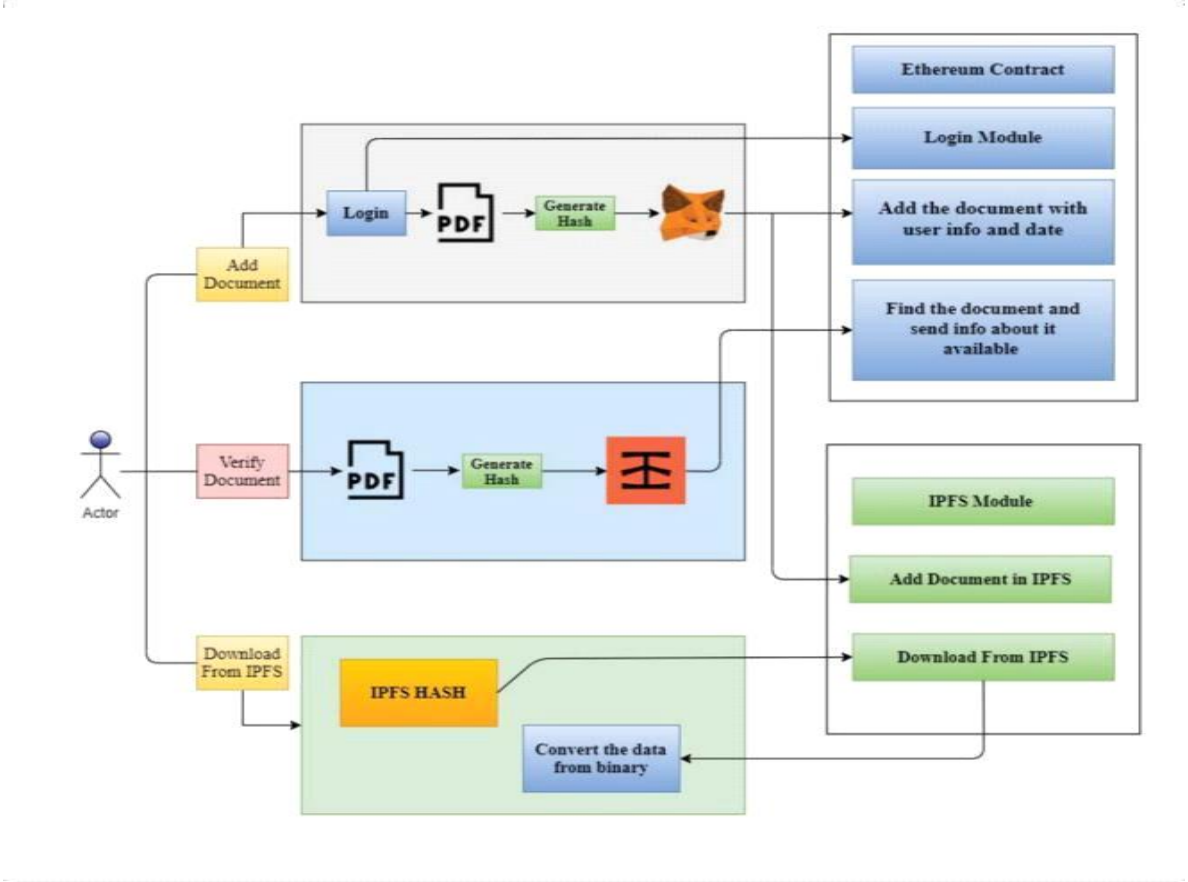

Figure 4: Uploading, verification and storage of the documents

The proposed framework in figure 4 will ask the students for their 10th-grade registration number, and for the organizations, it will ask for the institution code or company code. If the registration number or the code matches with the ones available in the database, then only the user is allowed to enter the system. After the above step of verification, the person may register if they are a new user, or login into the system if they are existing users. The student users are the only users who have the option to either view the uploaded certificates or upload a new certificate. Once the student login into the system, they can see their information on the web page and view two options to either upload the certificate or view the existing certificates. With this objective, a D-App Blockchain-based certificate validation system is proposed for an educational institution. The certificates can be uploaded by the student and validated by the institution. Only the user with the correct credentials can access the certificates which makes it a safe way of verifying the certificates without the hassle of hours to get the validation done.

The student and institute modules are as shown in the resultant system. The student module contains all the data related to a student and the institute module contains the data of all students. An institute module can store all the data of students with their certificates. The student form contains information that needs to be uploaded by the student for his/her certificate verification from the institute. It includes basic information like the parent's name, DOB, etc. along with the respective academic details like the student roll along with the institute code and other relevant information. To signup/register a new student, a transaction is run on MetaMask for the creation of a record in the block.

Once the student is registered, he/she can now upload documents for verification. The student dashboard displays his/her details and my documents section contains all the uploaded documents. To upload a document for verification, a transaction is run for storing the documents. Whenever a student requests verification of a document, the institute can view the request on its dashboard. The documents are sorted using document status and document type. The institute holds the right to either verify or reject the document after viewing the document uploaded by the student.

The digitized document is now stored on IPFS. The college can verify the document using the hash stored on the blockchain. The data contain the sender's address, the receiver's address, and the hash function. One can verify

Doi: https://doi.org/10.54216/FPA.120204
Received: January 12, 2023 Revised: April 18, 2023 Accepted: June 14, 2023

the data using the Ganache software. All the data is stored on the local blockchain network. Thus, it can be concluded that the certificate that is stored on the blockchain safely can now be safely considered as tamper-proof.

8. Results and Discussion

The proposed model Chaotic Key based Certificate validation (CK-Cert) is compared with PBCert and CertChain with setting size of half million certificates under varying rate of revoked certificates. Figure 6 depicts that the proposed algorithm performs better since only Chaotic points are stored on IPFS server, whereas in PBcert techniques complete root address is saved on OCSP server and CertChain performs the worst since complete address is stored directly on bloom filters.

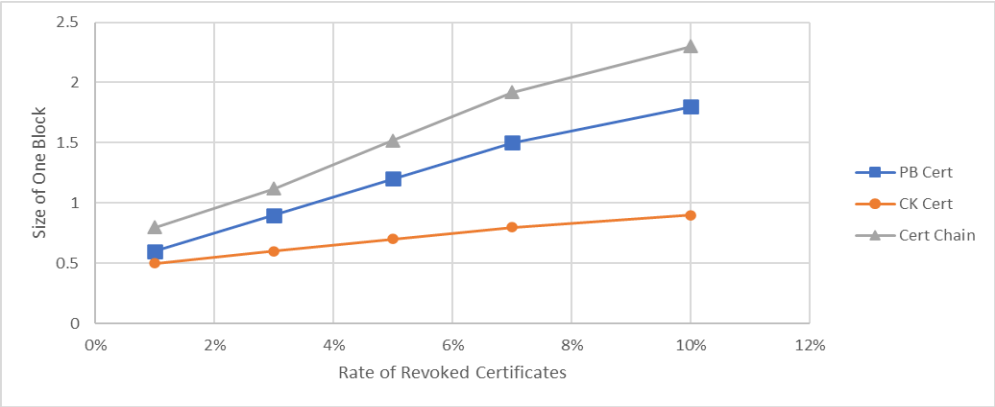

Figure 6: Blocksize comparison between Proposed model (CK-Cert), PB Cert and CertChain

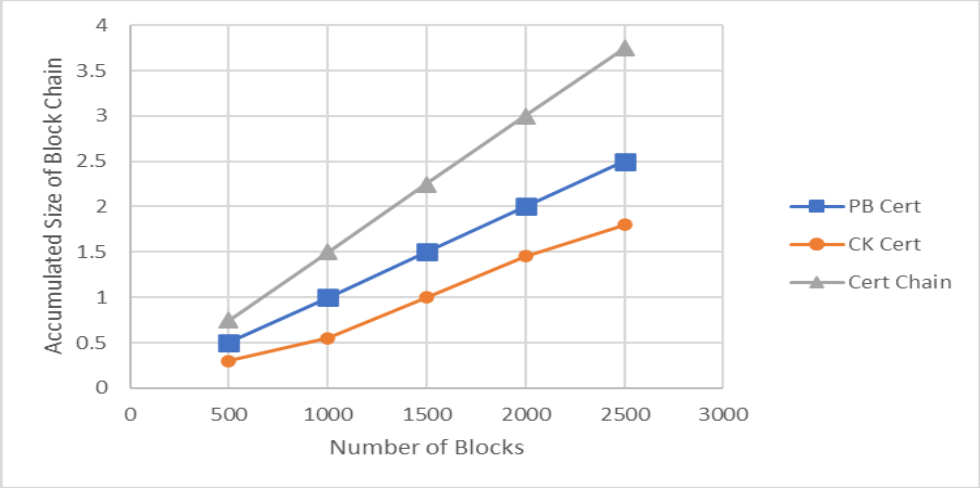

Figure 7: Number of blocks Vs. Accumulated size of Blockchain for CK-Cert,PB Cert and CertChain

Figure 7 compares the number of blocks versus the accumulated size of blockchain in GB for proposed algo (CK-Cert), PBCert and CertChain. Results indicate that the proposed algorithm better manages the block size, since Chaotic points show periodic behavior and in CertChain complete bloom filter rebuilds even if one certificate status changes. Hence proposed algorithm shows better results in case of certificate revocation and provides a better solution as accumulated size is also lesser due to simplicity of chaotic algorithm.

6. Conclusion

There are numerous cases of certificate fraud these days in the digital age society. There is a need fora robust mechanism which can help to keep away from forged documents. Therefore, a user-friendly secure web app to resolve this international hassle. The predominant cause of the proposed structures is to create a platform to save

Doi: https://doi.org/10.54216/FPA.120204
Received: January 12, 2023 Revised: April 18, 2023 Accepted: June 14, 2023

and affirm any essential files like certificates, land/assets/asset records, clinical records, etc. The counselled fashions are carried out with the complete usage of the Ethereum blockchain network. The collaboration of a few famous capabilities like cryptographic hash and decentralization makes the blockchain era immutable. As a result, there is no critical server to very own the facts instead all the facts concerning any transactions is shipped to the complete network. The verification result is constantly correct and verified. The usage of our proposed system reduces document forgery. Any company, organization, or group can use this proposed web app. In conclusion, our proposed approach guarantees integrity and protection for each use case. However, this growing era of blockchain has a few minor complexities. But still, the blockchain era outperforms any other technology where the protection and security of data is of utmost importance. With the immutable assets of blockchain, will benefit mankind to control their virtual certificates. Limitations of the proposed work is that there is a dearth of people with expertise in the technology. Although immutability helps in maintaining the integrity of the documents, but it has a drawback that any modification in the document is not possible.

Funding: "This research received no external funding"

Conflicts of Interest: "The authors declare no conflict of interest."

References

[1] S., Sharma, P.K., Yoon, B., Shojafar, M., Cho, G.H. and Ra, I.H., 2020. Convergence of blockchain and artificial intelligence in IoT network for the sustainable smart city. Sustainable Cities and Society, 63, p.102364.

[2] Xie, J., Tang, H., Huang, T., Yu, F.R., Xie, R., Liu, J. and Liu, Y., 2019. A survey of blockchain technology applied to smart cities: Research issues and challenges. IEEE Communications Surveys & Tutorials, 21(3), pp.2794-2830.

[3] Khan, Z., Abbasi, A.G. and Pervez, Z., 2020. Blockchain and edge computing–based architecture for participatory smart city applications. Concurrency and Computation: Practice and Experience, 32(12), p.e5566.

[4] Qian, Z., 2021. The Integration of Blockchain and Artificial Intelligence for a SmartCity. Academic Journal of Computing & Information Science, 4(8).

[5] Zheng, Z., Xie, S., Dai, H.N., Chen, X. and Wang, H., 2018. Blockchain challenges and opportunities: A survey. International journal of web and grid services, 14(4), pp.352-375.

[6] Aamir, M., Qureshi, R., Khan, F.A. and Huzaifa, M., 2020. Blockchain based academic records verification in smart cities. Wireless Personal Communications, 113(3), pp.1397-1406.

[7] Monrat, A.A., Schelén, O. and Andersson, K., 2019. A survey of blockchain from the perspectives of applications, challenges, and opportunities. IEEE Access, 7, pp.117134-117151.

[8] Bhutta, M.N.M., Khwaja, A.A., Nadeem, A., Ahmad, H.F., Khan, M.K., Hanif, M.A., Song,H., Alshamari, M. and Cao, Y., 2021. A survey on blockchain technology: evolution, architecture and security. IEEE Access, 9, pp.61048-61073.

[9] Alsunaidi, S.J. and Alhaidari, F.A., 2019, April. A survey of consensus algorithms for blockchain technology. In 2019 International Conference on Computer and Information Sciences (ICCIS) (pp. 1-6). IEEE.

[10] Shrimali, B. and Patel, H.B., 2021. Blockchain state-of-the-art: architecture, use cases, consensus, challenges and opportunities. Journal of King Saud University-Computer and Information Sciences.

[11] Johar, S., Ahmad, N., Asher, W., Cruickshank, H. and Durrani, A., 2021. Research and applied perspective to blockchain technology: A comprehensive survey. Applied 395 Sciences, 11(14), p.6252.

[12] Kaur, A., Nayyar, A. and Singh, P., 2020. Blockchain: A path to the future. Cryptocurrencies and Blockchain technology applications, pp.25-42.

[13] Dharmalingam, R., Ugail, H., Shivasankarappa, A.N. and Dharmalingam, V., 2022.Framework for Digitally Managing Academic Records Using Blockchain Technology. In Mobile Computing and Sustainable Informatics (pp. 633-645). Springer, Singapore.

Doi: https://doi.org/10.54216/FPA.120204
Received: January 12, 2023 Revised: April 18, 2023 Accepted: June 14, 2023

[14] Han, M., Li, Z., He, J., Wu, D., Xie, Y. and Baba, A., 2018, September. A novel blockchain-based education records verification solution. In Proceedings of the 19th annual SIG conference on information technology education (pp. 178-183).

[15] Badr, A., Rafferty, L., Mahmoud, Q.H., Elgazzar, K. and Hung, P.C., 2019, June. A permissioned blockchain-based system for verification of academic records. In 2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS) (pp. 1-5). IEEE.

[16] Bhagwat, M., Shah, J.C., Bilimoria, A., Parkar, P. and Patel, D., 2020, July. Blockchain to improve Academic Governance. In 2020 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT) (pp. 1-5). IEEE.

[17] Bhumichitr, K. and Channarukul, S., 2020, July. Acachain: Academic credential attestation system using blockchain. In Proceedings of the 11th International Conference on Advances in Information Technology (pp. 1-8).

[18] Rasool, S., Saleem, A., Iqbal, M., Dagiuklas, T., Mumtaz, S. and ulQayyum, Z., 2020. Docschain: Blockchain-based IoT solution for verification of degree documents. IEEE Transactions on Computational Social Systems, 7(3), pp.827-837.

[19] Awaji, B., Solaiman, E. and Marshall, L., 2020, July. Blockchain-based trusted achievement record system design. In Proceedings of the 5th International Conference on Information and Education Innovations (pp. 46-51).

[20] Ghaffar, A. and Hussain, M., 2019, July. BCEAP-A blockchain embedded academic paradigm to augment legacy education through application. In Proceedings of the 3rdInternational Conference on Future Networks and Distributed Systems (pp. 1-11).

[21] Jha, A., Bhattacharjee, R.K., Nandi, M. and Barbhuiya, F.A., 2019, July. A framework for maintaining citizenship record on blockchain. In Proceedings of the 2019 ACM international symposium on blockchain and secure critical infrastructure (pp. 29-38).

[22] Patel, K. and Das, M.L., 2020, January. Transcript management using blockchain enabled smart contracts. In InternationalConferenceonDistributedComputingandInternetTechnology (pp. 392-407). Springer, Cham.

[23] Curmi, A. and Inguanez, F., 2018, July. Blockchain based certificate verification platform. In International Conference on Business Information Systems (pp. 211-216). Springer, Cham.

[24] Shariar, A., Imran, M.A., Paul, P. and Rahman, A., 2020, January. A decentralized computational system built on blockchain for educational institutions. In Proceedings of the International Conference on Computing Advancements (pp. 1-6).

[25] Yao, S., Chen, J., He, K., Du, R., Zhu, T. and Chen, X., 2018. PBCert: Privacy-preserving blockchain-based certificate status validation toward mass storage management. IEEE Access, 7, 435, pp.6117-6128.

[26] Wang, Z., Lin, J., Cai, Q., Wang, Q., Zha, D. and Jing, J., 2020. Blockchain-based certificate transparency and revocation transparency. IEEE Transactions on Dependable and Secure Computing.

[27] Yakubov, A., Shbair, W., Wallbom, A. and Sanda, D., 2018. A blockchain-based PKI management framework. In The First IEEE/IFIP International Workshop on Managing and Managed by Blockchain (Man2Block) colocated with IEEE/IFIP NOMS 2018, Tapei, Tawain3-27 April 2018.

[28] Imam, I.T., Arafat, Y., Alam, K.S. and Shahriyar, S.A., 2021, February. DOC-BLOCK: A Blockchain Based Authentication System for Digital Documents. In 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks 446 (ICICV) (pp. 1262-1267). IEEE.

[29] Gundgurti, P.E., Alluri, K., Gundgurti, P.E. and Vaishnavi, G., 2020, July. Smart and Secure Certificate Validation System through Blockchain. In 2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA) (pp. 862-868). IEEE.

[30] Gayathiri, A., Jayachitra, J. and Matilda, S., 2020, July. Certificate validation using blockchain. In 2020 7th International Conference on Smart Structures and Systems (ICSSS) (pp. 1-4). IEEE.

Doi: https://doi.org/10.54216/FPA.120204
Received: January 12, 2023 Revised: April 18, 2023 Accepted: June 14, 2023

[31] Belurgikar, D.A., Kshirsagar, J.K., Dhananjaya, K.K. and Vineeth, N., 2019, March. Identity solutions for verification using blockchain technology. In 2019 1st International Conference on Advanced Technologies in Intelligent Control, Environment, Computing &Communication Engineering (ICATIECE) (pp. 121-126). IEEE.

[32] Bahrami, M., Movahedian, A. and Deldari, A., 2020, October. A Comprehensive Blockchain-based solution For Academic Certificates Management Using Smart Contracts. In 2020 10th International Conference on Computer and Knowledge Engineering (ICCKE) (pp. 573-578). IEEE.

[33] Li, X., Jiang, P., Chen, T., Luo, X. and Wen, Q., 2020. A survey on the security of blockchain systems. Future Generation Computer Systems, 107, pp.841-853.

[34] Garba, A., Chen, Z., Guan, Z. and Srivastava, G., 2021. LightLedger: A novel blockchain-based domain certificate authentication and validation scheme. IEEE Transactions on Network Science and Engineering, 8(2), pp.1698-1710.

[35]Y. Zhang, C. Xu, X. Lin and X. Shen, "Blockchain-Based Public Integrity Verification for Cloud Storage against Procrastinating Auditors," in IEEE Transactions on Cloud Computing, vol. 9, no. 3, pp. 923-937, 1 July-Sept. 2021, doi:10.1109/TCC.2019.2908400.

[36] Y. Xu, C. Zhang, G. Wang, Z. Qin and Q. Zeng, "A Blockchain-Enabled Deduplicatable Data Auditing Mechanism for Network Storage Services," in IEEE Transactions on Emerging Topics in Computing, vol.9, no. 3, pp.1421-1432, July-Sept. 2021, doi:10.1109/TETC.2020.3005610.

[37] R. Zhou, M. He and Z. Chen, "Certificateless Public Auditing Scheme with Data Privacy Preserving for Cloud Storage," 2021 IEEE 6th International Conference on Cloud Computing and Big Data Analytics (ICCCBDA),2021, pp. 675-682, doi:10.1109/ICCCBDA51879.2021.9442586.

Doi: https://doi.org/10.54216/FPA.120204
Received: January 12, 2023 Revised: April 18, 2023 Accepted: June 14, 2023