Online Certificate Generation & Verification using Blockchain Framework

Prasad Jadhav[1], Aseem Godambe[2], Rutwik Gaikwad[3], and Kiran Deshpande[4]

[1] A.P. Shah Institute of Technology, University of Mumbai, Mumbai-400615, India,
prasadjadhav@apsit.edu.in
[2] aseemgodambe@apsit.edu.in
[3] gaikwadrutwik@apsit.edu.in
[4] kbdeshpande@apsit.edu.in

Abstract. There are many cases reported of certificate forgery every day and many of them go undetected. The purpose of this study is to develop a system that would authenticate certificates to their real owners and could verify the same on a specific portal. To achieve this, in this paper we focus on Ethereum Blockchain as it is immutable, transparent, scalable, and also cost-effective. Universities would be able to generate their own certificates on the web portal itself by uploading their certificate template in Scalable Vector Graphics(SVG) format and the student data in Comma-separated Values(CSV) format. Each generated certificate would be allotted to the respective student within the system. Each certificate would be given a unique hash code so that it could be verified easily and there would be no scope of duplication. The authentication and verification would be done on the same web portal. To sum up, this method would save time and efforts that are required to verify a certificate manually and would result in an effective, secure way to generate certificates.

Keywords: Blockchain, Ethereum, Distributed system, Security, Encryption, Hashing, Scalable Vector Graphics(SVG), Comma-separated Values(CSV), Digital certificate, Authentication, Verification.

1 INTRODUCTION

Everyone has a particular talent or excels in a field and certificates are a great way to reflect the achievements. It proves that an individual has acquired knowledge of a particular skill. Companies need skilled employees and certificates prove to be a valid solution to depict once capabilities. Displaying a certificate of a particular skill verifies that the certificate holder is competent in that skill and helps the company in the hiring process. Also due to the current pandemic situation, online learning and certifications through online courses has drastically increased. People have started to adapt to online learning and hence the certificates hold a greater value to validate the progress of an individual and also it adds a great value to their profiles.

As certificates hold such higher values people tend to misuse it and generate a fake copy of the certificate of the skill which they have not acquired. The companies or the organisation where an individual is applying offers an advantage to the person having the necessary certificates. It's difficult for the organisation to check individual certificates as they may have to contact the issuer and it takes a lot of time and effort. The fake certificates can be easily generated using any online website or normal photo editing software. As a result it makes it more difficult for the deserving candidate to have all the genuine certificates.A survey conducted by UK's national qualifications agency UK NARIC conducted across 17 countries in different universities found the common problem of difficulty in verifying documents. According to the survey, it has been found that 62% of them verify the documents by contacting the institutes awarding them while 14% of them didn't even bother to check the originality of the certificate. It stated that around 75% of the certificates submitted were fraud [1]. Similar research and investigation conducted by the BBC Radio 4's File on Four programme found out about thousands of fake degree certificates in the UK from "Diploma Mill" in Pakistan. This deteriorates the standard of employees being hired and unfair against the students who are hardworking and achieving the results [2].

The motive of this research is to create a system which is secure, easy to access and verify certificates. The organisation hiring an individual could verify the certificate online without the need to contact the issuer. Blockchain technology along with different hashing methods is used to maintain a secure record of the information. An SVG(Scalable Vector Graphics) format certificate template is used specifically to reduce the cost of storing multiple images on the blockchain network. This creates a scalable and economical system for an organisation to implement.

2 PRELIMINARY CONCEPT

2.1 Blockchain

The first idea of collecting various certificates and documents in one block was led out by Stuart Haber and W. Scott Stornetta back in 1991 [3]. Their basic idea was to create a system in which the documents and certificates cannot be tampered by anyone. They decided to implement it using a cryptographically secured chain of blocks. This further led to the concept of blockchain which was introduced in 2008 by Satoshi Nakamto (or group of people). At the initial stage, blockchain was focused on crypto-currency. But later on, blockchain extended in various other fields. Blockchain could also be considered as an online ledger that provides decentralized and transparency in data sharing.

The concept of blockchain was to store data in a block along with a timestamp. Once the data is entered into the block and it is verified then it becomes immutable and open in public to provide transparency. The block is provided with a hash value of the current block and also the hash value of the previous block in the chain. This ensures the trackability of the block from the chain.

2.2 Ethereum

The advancement in the field introduced Ethereum into the blockchain. Ethereum focused on another usage of blockchain. This led to the division as Bitcoin was for payment network Ethereum started its use in computing. The other advantage of Ethereum is that it is an open-source project.

Ethereum introduced EVM (Ethereum Virtual Machine). These are programmable blockchain. It works on a high-level language developed for this purpose like Solidity. It also offers smart contracts. Smart contracts basically streamline multiple complex tasks or processes involved in completing an objective. Smart Contracts basically work on a simple statement "if/when.... then....". It's just the coding done to perform tasks automatically if one situation occurs then what would be its countermeasure. Smart contracts not only have the same time but also provide reliable security [4]. The various aspects of smart contracts are self-verifying and self-executing. It is also tampering resistant, involves fewer intermediaries, and also has low transaction cost.

2.3 SVG - Scalar Vector Graphics

SVG is an Extensible Markup Language-based vector image format for two-dimensional graphics [5]. It has additional features and supports interactivity and animation. SVG was developed by the World Wide Web Consortium as an open standard. It allows us to define vector-based graphics in XML format on the web. It is recommended by W3C (World Wide Web Consortium) and is also integrated with DOM and XSL.

SVG provides multiple advantages over other image formats such as it can be created in a text editor and also provides an option to edit it later on. As its written in XML format it offers options to compress, index, search and script the images. They do not lose quality when zoomed and therefore can have high resolution when printing. As SVG provides the ability to edit the image we can use it to store the template of the certificate separately and print multiple certificates of the same template without actually saving the whole certificate.

3 LITERATURE SURVEY

3.1 Shanmuga Priya R,Swetha N 'Online Certificate Validation Using Blockchain.' [6]

This document summarizes the problems of forged certificates and how blockchain can solve the issue. Netbeans IDE and Android Studio are used to develop the server communication and the application to scan the QR codes. EthereumJS is used for faster Ethereum applications. The application involves the user uploading his/her certificate like 10th-grade mark sheet, college certificates, government certificates, and so on to the portal. After uploading the certificate, the data is then sent to the issuer for validation. The issuer (example: School which is responsible for validation of 10th grade Marksheet) has to validate the

data received by the application for verification. Once verification is successful, the data will be stored on the server else it would be discarded. On the mobile application, a QR code will be generated based on the certificate number. The QR code can then be shared with anyone else for verification in case of necessity. When the QR code is scanned, an OTP (One Time Password) will be sent to the registered mobile number for verification. After proper authentication, the user can view the certificate. If the number of scans goes beyond the permitted limit, the location of the scanner will be sent to the authorized user with a permission link. From that link, the authorized user can either allow or deny the person. The major drawback of this system is that verification can be delayed by the issuer as the certificate has to reach the organization for verification and the data is sent to blockchain only after verification. The OTP system can get tedious. This system can get costly as well.

3.2 Nitin Kumavat, Swapnil Mengade, Dishant Desai, JesalVarolia 'Certificate Verification System using Blockchain' [7]

This document summarizes that during the course of education the students achieve many certificates. Students produce these certificates while applying for jobs in public or private sectors, where all these certificates are needed to be verified manually. There can be incidents where students may produce fake certificates and it is difficult to identify them. The solution proposed in this system uses Ethereum and IPFS (Interplanetary File System). IPFS is a peer to peer, content address system. It is very similar to BitTorrent and MerkleDag. Unlike HTTP which restricts or provides low latency on transfer of large amounts over the network which uses IP addressing, IPFS uses content addressing. As a result it creates a distributed system of different nodes across the network. It returns us a hash value and it uses this value to retrieve the data. They propose to add the data with the certificate on the IPFS network to generate the hash for it and later on add the data to the blockchain network with the help of EVM. This topology includes two distributed networks to provide additional security to the model. While retrieving the certificate they would compare the hash and pull the entire certificate which has been stored on the IPFS network. The advantage of this system was it is more secure, provides reliability. With two distributed networks, it's almost impossible to tamper the data. On the other hand, the disadvantage of the system is that IPFS is a tedious process to set-up as well as storing the certificate image on any distributed blockchain platform costs a lot of money and hinders the scalability of the system.

4 PROPOSED SYSTEM ARCHITECTURE

4.1 Methodology

This proposed system revolves around creating a secure and fast method to generate and verify the certificates using the features of SVG and blockchain.

The certificate's data is hashed and stored on a blockchain network to provide security and immutability to the data. On the blockchain network, this data is stored on blocks. The block contains the hashed data, timestamp, and the id of the next block. Then the block is added to the network. The template of the certificate which is in SVG format is stored on a database server that is not a blockchain-based network as the certificate template won't be modified. The data which is hashed includes the name of the certificate holder, their email, issuing date, expiry date for the certificate, and information regarding other fields of the certificate. This data can only be submitted by the certificate issuer and thus ensuring the right data is provided. Anyone can check certificates of the students using the unique id provided to each student for their certificates or from a student's profile.

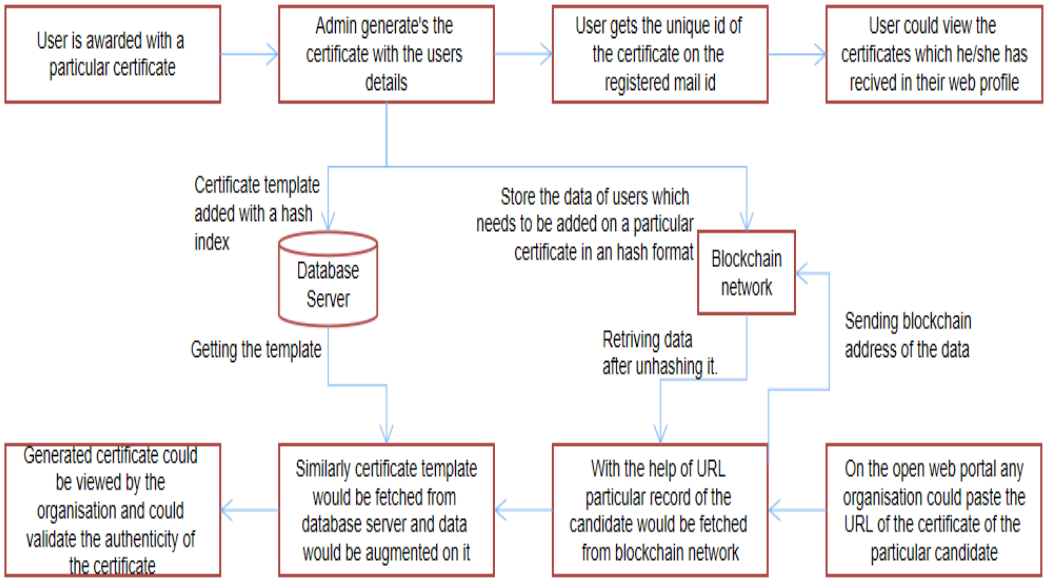

Fig. 1. Architecture of proposed system.

4.2 Certificate Generation

Certificates can be generated only by the organizations registered on the website. They need to upload the template of the certificate in the SVG format. The SVG template should have a proper id for a particular field like the space for the name of the receiver should have a well-defined id, for example, 's_name'. Once the SVG template is uploaded the organization needs to upload a CSV file that has the record of the students who have won the certificates. The CSV needs to have

the first row as the ids of the fields marked on the SVG template, along with it the CSV needs to have a compulsory email column that would contain the email of the receiver. Other columns of the CSV would be the remaining values that needed to be filled on the template like the receiver's name, issuing date and expiry date of the certificate, etc. The only condition is that the id of the field written on the SVG template should be the column header of the CSV file. This method is done to ensure that the blanks on the template could be filled by the right data in the CSV file. Once the upload action of the template and CSV file is done the certificates would be auto-generated for all the students receiving the certificates and would be available in their profile on the website. This would be done with the help of email ids associated with each student present in the CSV file.

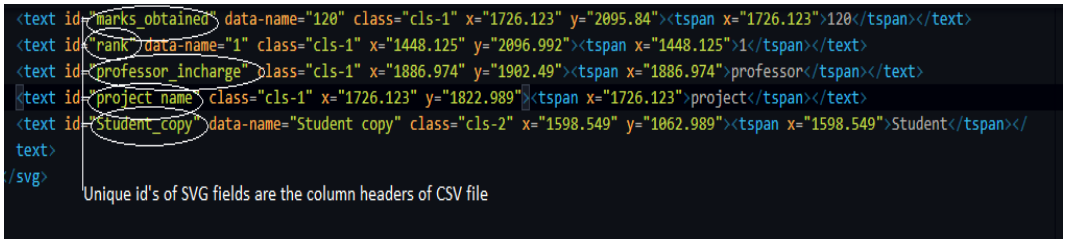

Fig. 2. Example of a certificate template in an SVG format indicating the ID's of the fields of the certificate.

cert_id	email	Student_copy	marks_obtained	rank	professor_incharge	project_name
1	abc1@gmail.com	Rahul Sharma	70	2	Prof. Gopal Yadav	Water sanitisation
2	abc2@gmail.com	Vishal Pande	79	1	Prof. Gopal Yadav	Soil quality analysis

Fig. 3. CVS file with the data of students winning the certificate for the above given SVG template.

4.3 Certificate Validation

In this process, the certificates are validated. As the data is stored on the blockchain network there is no way to edit the data once it's appended into the blocks on the network. The process works as when the certificate data is uploaded by the organization in CSV format the data is extracted from the CSV and uploaded on the blockchain network. Once the data is uploaded on the network, students who have won those certificates are informed through an

email that they can view their certificates now in their profile and are provided a unique key or URL for the certificate. Students could use or provide this key, URL to anyone to authenticate the certificates. When a particular key is used the data of that candidate is retrieved from the blockchain and the corresponding template is fetched from the database server. The data from the blockchain is mapped on the SVG templates as the fields of the template are pre-recorded and thus generates a certificate in front of the user which is not tampered with by any means. Thus an entity could verify that the certificate is genuine and possessed by the actual owner of the certificate.

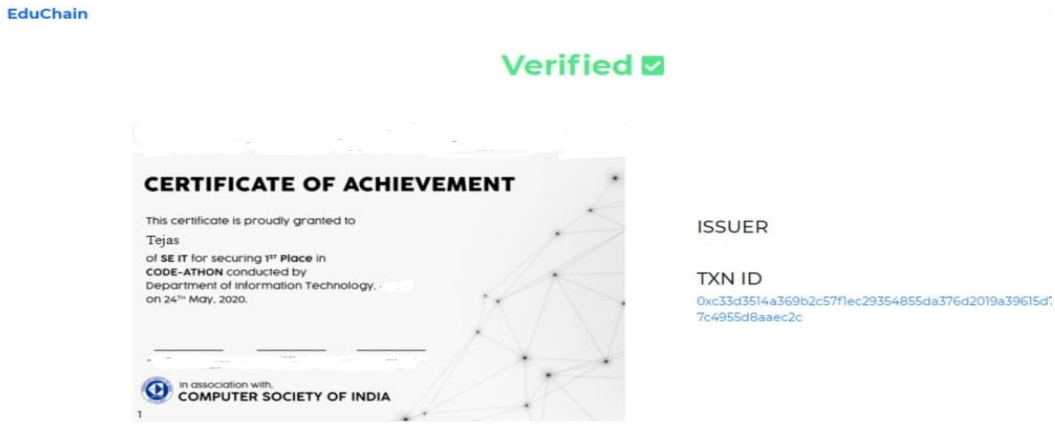

Fig. 4. Certificate uploaded on the web portal which is verified and genuine certificate.

4.4 Working of Application

In our application on the landing page any individual could see a certificate by just entering its unique id on the search bar. There is an admin login, once logged in the admin one could add certificate and CSV file to generate certificates. Once the data is uploaded by the admin it would be stored temporarily in a database and would be uploaded on the blockchain network periodically using a CRON script every day at midnight. This is done to ensure every certificate's data is uploaded on the blockchain network because if we fail to upload any data we cannot rewrite the blocks on the network. Once the data is uploaded students are informed that their certificate is uploaded. When logged in as students they could see the certificates achieved by them in their profile and would see a green tick indicating that the certificate is validated. Students can share their certificate links with anyone to view their certificates.

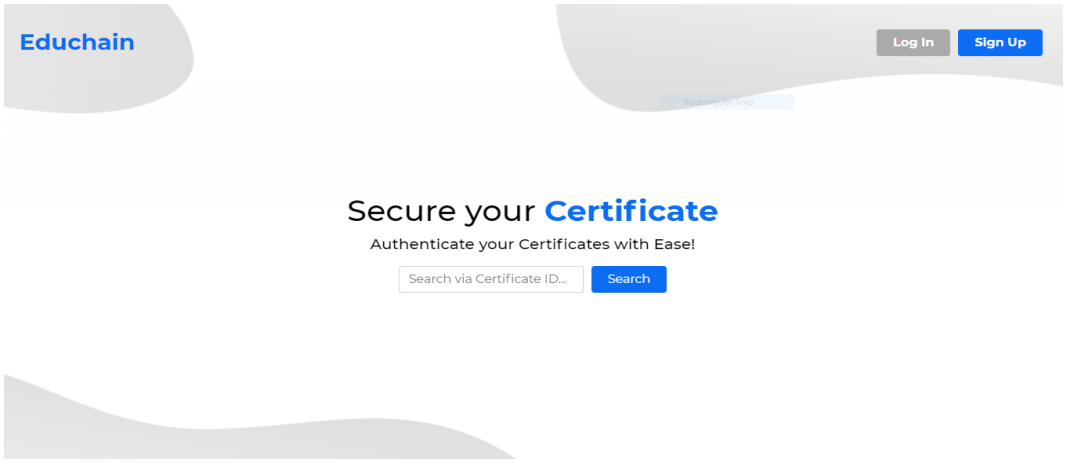

Fig. 5. Homepage of the web portal where anyone could search for any certificate to verify it's authenticity.

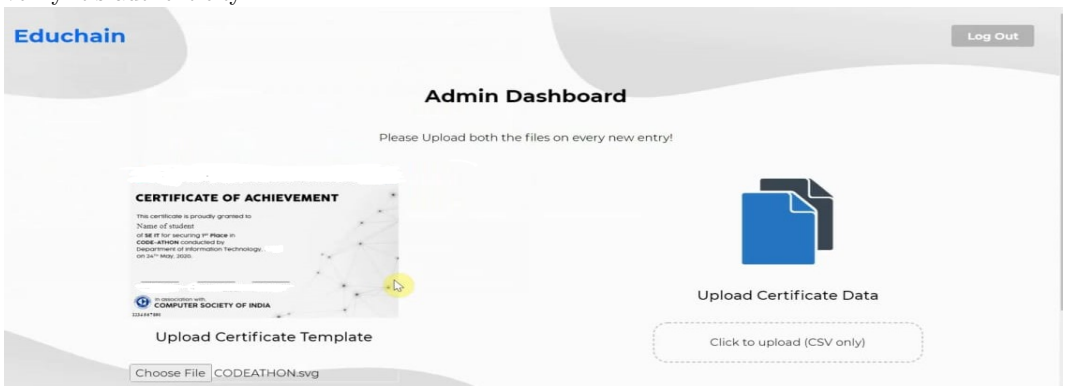

Fig. 6. Admin dashboard to upload SVG and CSV file

5 CONCLUSION

In this paper, we have successfully proposed a system where blockchain technology can be used to store and retrieve certificate data. The project will help companies issue certificates securely through Blockchain and can be verified by anyone with the unique link/code to each certificate. The system uses the concept of SVG templates for the certificates which would be stored on a local server and to store data over the blockchain for secure and reliable storage. This will minimize the cost of storing the entire certificate on the blockchain network. Storing only the data of the certificate will minimize cost and thereby turn out to be cost-efficient. The only drawback of this system is that the template of the certificate needs to be properly created with the SVG's text area ID to match

with the header of the CSV file. Only a properly crafted SVG and CSV pair will result in proper certificate generation through Blockchain.

6 ACKNOWLEDGMENT

The authors would like to sincerely thank A. P. Shah Institute of Technology for supporting this research by proving necessary resources and guidance.

References

1. UK: NARIC Survey: universities and education fraud – 75% cannot spot a fake certificate - Feb 2020, https://uknaric.org/2020/02/26/survey-universities-and-education-fraud-75-cannot-spot-a-fake-certificate/
2. BBC File on 4 exposes a multi-million pound global trade in fake diplomas - Jan 2018, https://www.bbc.co.uk/programmes/b09ly731
3. Blockchain, https://en.wikipedia.org/wiki/Blockchain.
4. Smart Contracts, https://www.ibm.com/blogs/blockchain/2018/07/what-are-smart-contracts-on-blockchain/
5. Scalable Vector Graphics, https://en.wikipedia.org/wiki/Scalable_Vector_Graphics
6. Shanmuga Priya R, Swetha N. Online Certificate Validation Using Blockchain. Published in Int. Jnl. Of Advanced Networking Applications (IJANA)
7. Nitin Kumavat, Swapnil Mengade, Dishant Desai, JesalVarolia (2019). Certificate Verification System using Blockchain. International Journal for Research in Applied Science Engineering Technology (IJRASET).
8. Oliver Miquel, Moreno Joan,Prieto Gerson, Ben tez David (2018). Using blockchain as a tool for tracking and verification of official degrees: business model 29th European Regional Conference of the International Telecommunications Society (ITS): "Towards a Digital Future: Turning Technology into Markets?", Trento, Italy, 1st - 4th August 2018.
9. K. Kuvshinov, I. Nikiforov, J. Mostovoy, and D. Mukhutdinov, "Disciplina: Blockchain for Education," pp. 1–17, 2018.
10. D.T.T. Anh, M. Zhang, B.C. Ooi, and G. Chen, "Untangling Blockchain: A Data Processing View of Blockchain Systems," IEEE Trans. Knowl. Data Eng., vol. 4347, no. c, pp. 1–20, 2018.
11. Kumar, NM Saravana. quot;Implementation of artificial intelligence in imparting education and evaluating student performance." Journal of Artificial Intelligence 1, no. 01 (2019): 1-9.
12. Smys, S., Joy Iong Zong Chen, and Subarna Shakya. quot;Survey on Neural Network Architectures with Deep Learning." Journal of Soft Computing Paradigm (JSCP) 2, no. 03 (2020): 186-194