Certificate Verification using Blockchain

Monika Sharma
Assistant Professor ABESEC,
Ghaziabad

Srishti Sharma
Scholar IPEC,
Ghaziabad

Yash Gupta
Scholar IPEC, Ghaziabad

ABSTRACT

Blockchain technology is arguably best known for its use in the digital currency Bitcoin, which is even more well-known than the Blockchain technology itself. Blocks in a distributed environment—one in which storage devices are not all linked to a single processor—that makes up the Blockchain are immutable. It is a collection of records/public ledger of every digital transaction that has taken place, and information is exchanged between involved parties. The system's participants all agree to verify each submission before it is made. Blockchain data cannot be deleted once it has been inputted. A secure and open method might be offered as a result. We still need to uphold confidence in certification, and proof of learning as education becomes more diverse, decentralized, and democratic. Nowadays, everyone is required to present their documents and credentials to anyone they meet for a job or other reason. A third party cannot verify the authenticity of the certificate after seeing it. Using blockchain technology, we can get confidence or find a solution to this issue. There is no requirement for a central authority to verify certificates when using this technology.

Keywords

Blockchain, Digital Certificates, Confidentiality, Integrity,Availability.

1. INTRODUCTION

In India, children's academic careers usually begin with attendance at kindergarten before changing schools for primary, secondary, and high school. After completing secondary school, students must apply for admission to colleges. In addition, there is a second school change for graduation. This is the basic learning year cycle for students. Some students choose to continue their formal education after this. The problem with this cycle is that a student must present all of their transcripts for validation at each step. In the process, the document may be lost or damaged. It is also very tedious for the examiner to validate each individual certificate. With such a large population, our country almost always has 26.3 million graduates per year. It is very difficult to record and verify such a large number of documents. As a result, tampering and the creation of fake or duplicate certificates become an undesirable situation. There are numerous covert organizations that operate this fraud behind the backs of everyone in our country. To date, technology has evolved significantly. Differentiating between a fake certificate and a real one requires a lot of attention, wasting valuable time. Blockchain is a system that has the potential to eliminate this disadvantage. Under practical circumstances, it is impossible to change the data in a blockchain. Even when data is altered, the notification of the change happens very quickly. In a blockchain, a node or data entity is only confirmed when several parties concur. The method would become trustworthy and authenticated as a result. The problem of hacking is now solved. Most certificates issuedin universities or schools are in paper form. Since companies must manually verify all certificates - a tedious process - there is a possibility that some applicants have presented certificates that are not legitimate and that go undetected by the verifier during the process, giving an opportunity to an ineligible applicant. In the past, there has been lot of cases of individuals being discovered selling cheap fake certificates from various organizations. We can use blockchain technology to tackle this problem and reduce the issuance of fake certificates. Blockchain is used to store certificate data that can be validated by anyone, anywhere.

Blockchain is a decentralized, shared, distributed database that virtually prevents data from being altered. It is a type ofdatabase that follows a set of rules and is not centralized. The decentralized certificate verification application on the blockchain is being developed as part of this research. Our choice of this technology is based on its encryption, tamper-resistance, and traceability. The encrypted hash value of each document is stored in the blockchain andmatched with the user document using a smart contract in the backend. The weaknesses of our current system areclosed by the proposed system, which also provides a viable, tangible solution.

2. LITERATURE SURVEY

2.1 BLOCKCHAIN BASEDCERTIFICATE VALIDATIONSYSTEM (2022) Mrs. R. Suganthalakshmi,Mrs. G. Chandra Praba, Mrs. K. Abhirami,Mrs. S. Puvaneswari

In this paper, they proposed a solution to document forgery. By integrating blockchain technology, we can eliminate the problem of forged and missing certificates. We can view our certificates at any time and from anywhere. The application provides accurate and reliable information about digital certificates.

2.2 Certificate Generation and VerificationUsing Blockchain Technology and Quick Response Code (2022)

Muhammad Umar Abdullahi, Dr. G. I.O. Aimufua, Adamu Aminu Muhammad

This research looked into how certificates are generated and verified, and it created a quick response code and blockchain-based certificate verification system that aims to fix the various flaws in the current system. The system was implemented in such a way that only the college (administrator) can create certificates and uploads them to the blockchain system, and once these certificates are created, no changes can be made. This feature helps us to create a system where the whole process is transparent and unchangeable. Our system automates the certificate creation process and reduces the manual labor required to verify the certificates. Moreover, the risk of losing the certificate is comparatively low for the students. By adding the QR code as an additional feature, the system reduces the percentage of data that can be manipulated and may be difficult and unreliable.

2.3 Smart Certificate using Blockchain (2022) Krishna Bihari Dubey and MuktaGoyal

According to certain surveys, millions of students graduate and continue their education. In this conception, it was found that a tamper-proof system is in use worldwide. As a result, smart certificates are developed to improve student security. In this recent study, the development of smart certificates for students was covered in detail. It made use ofdata from Firebase and the blockchain. As a result, a secure code, called a hash, is generated for each piece of data and stored securely in a database. It can be deduced that by creating a smart certificate in the blockchain, a certain level of security can be achieved for the certificates and any change can be detected. This blockchain can be useful in a variety of industries and could reach an important milestone in the future.

2.4 Proposing a trustworthy blockchain solution to secure and confirm graduate certificates (2021) T. Rama Reddy, P. V. G. D. Prasad Reddy, Rayudu Srinivas, Ch. V. Raghavendran, R. V. S. Lalitha, B. Annapurna

The suggested method is a consortium blockchain between the universities, the universities that are affiliated with them, the autonomous universities, and the businesses. Usually, colleges add students' credentials first, after which businesses or other auditors can confirm the credentials using the student's Aadhar number or transaction ID of the credential. The data stored in a blockchain is protected as no one can falsify it or add new transactions with a past date. In a nutshell, the transactional ID for each certificate is distinct. All colleges and universities are able to use this method to further protect student information and certificates.

2.5 Certificate Verification using Blockchain and Generation of Transcript (2021) Ravi Singh Lamkoti, Devdoot Maji, Hitesh Shetty, Bharati Gondhalekar

One of the most significant characteristics of the blockchain is the ability to create immutable ledgers. This behavior aids in the development of an immutable, transparent system. Our system automates the certificate creation process and reduces the manual work required to verify the certificates. Moreover, the risk of losing the certificate is comparatively low for students. By using an additional hash algorithm, we reduce the percentage of data manipulation. The Inter Planetary File System (IPFS) will house the original document, while the blockchain will keep the certificate's hash. This will help us preserve the data and provide transparency.

3. PROPOSED SYSTEM

3.1 Methodology

Academic transcripts will be converted to digital form according to the proposed method. Both the school and the students will be registered. The transcripts for each student will be uploaded. The hash values are generated using the consensus method. A hash value, a timestamp, and a prior hash value are all linked together to form each block on the blockchain. The user validates the certificates using the credentials created by the institution for the student and his password.

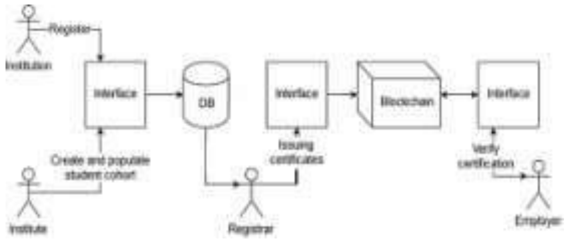


Fig 1: Proposed Model for Digital Certification

3.2 Creating Digital Certificates

The institution logs into our program using the admin login. The students are then registered by providing their name, email address and mobile number and are given a user ID and password. They enter the certificates and the corresponding information into the system.

3.3 Generating Hash Value

The hash number for the certificates is generated using the algorithm SHA -256. It takes input of different sizes and generates a hash value with a fixed size. The hash number is created during the upload of the certificate

3.4 Validating Certificates

The credentials are kept on the blockchain. With the help of the proof-of-work consensus method, they are verified. To select a mining block, this consensus method is used. The user should enter his login ID and password to access our program. By scanning the generated QR code, they can verifythe students' certificates. "The certificate is authentic" will be displayed if the certificate in question is genuine. If the certificate is not genuine, an error message will appear.

3.5 Workflow of Application

In this web-based portal, students and administrators (college/institution) have login access, and others than students and administrators can check the certificate. It consists of the following two main areas:

1. The student can select a course and receive a certificate on the blockchain after successful completion.
2. The administrator can manage the student and create acertificate on the blockchain.

3.6 Module Description

3.6.1 User Interface

For user interface design, we use NodeJs and React in this project. For database communication, we use IPFS storage. Using NodeJs and React, we are developing a web application to share and scan the QR code. The Ethereum client for testing and development, Testrpc, is built on Node.js. The use of Ethereum.js to emulate entire client behaviour speeds up the development of Ethereum apps significantly.

3.6.2 Validation

In this module, the user uploads the certificates, such as grade sheets, college certificates, state certificates, etc. Before uploading, these certificates are verified by the appropriate sector. When a college certificate is uploaded, the certificate number is compared with the associated college database server; if the certificate is verified, it is saved on the server; otherwise, it is discarded.

3.6.3 Creation of Block

A block is a container data structure. It indicates that a block is typically 1MB in size (source). Here, each certificate number is created as a block. A hash code is generated for each block for security.

3.6.4 Generating QR Code

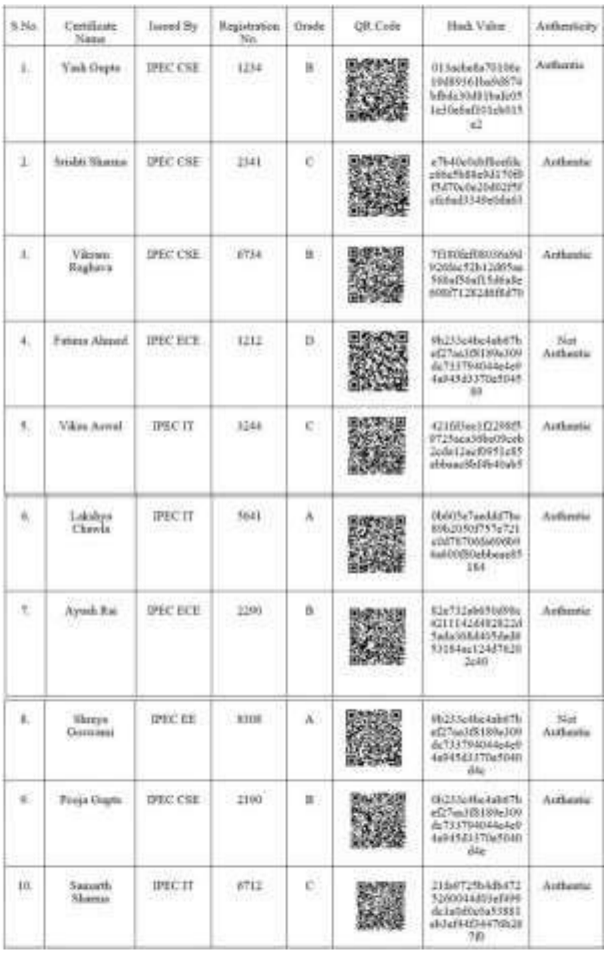
In this module, QR code is generated based on certificate numbers. The great advantage of this module is that the user can pass the QR code to another person if needed. When the user scans the QR code, the unique hash code is displayed which can be matched with the blockchain data for verification.

4. RESULT AND DISCUSSION

After adding 10 certificates from the admin side, some implementation outcomes are as follows:

- Table includes Name of the Certificate owner, Issuing authority, Registration number of the student, Grade achieved, QR Code Generated, Hash Value and the result whether the certificate is original or fake.
- We observed that 8 out of 10 certificates are valid / authentic and are issued by the authorized admin.
- We added two fake QR Codes to prove tampering of documents which showed "Not Authentic" by the system when verified.
- All QR Codes Generated and Hash Values provided are unique.

Table 1. QR codes and hash value generated for each certificate along with authentic/ unauthentic status.



S.No.	Certificate Name	Issued By	Registration No.	Grade	QR Code	Hash Value	Authenticity
1.	Yash Gupta	IPEC CSE	1234	B		013acbe8a70106e 10d89161ba0d874 bfbda30d81ba1e05 1e30e6af031cb015 a2	Authentic
2.	Srishti Sharma	IPEC CSE	2341	C		e7b40e0dbf8eefdc z86e5b84e9d170f0 f5d70e0e20d02f5f efcfad3348e0da61	Authentic
3.	Vikram Raghava	IPEC CSE	6734	B		7f1f00ef08036a9d 920dae52b12d05ae 56baf56af15d6a8e 6080712f2488f8d70	Authentic
4.	Fatima Ahmed	IPEC ECE	1212	D		9b233c4bc4ab67b ef27ae3f8189e309 dc733794044e4e9 4a945d3370a5045 80	Not Authentic
5.	Vikas Aswal	IPEC IT	3244	C		421f6f0ee1f2298f5 0725aca36be09ceb 2cda12acf0951c85 ebbaac8bf4b40ab5	Authentic
6.	Lakshya Chawla	IPEC IT	5641	A		0b605e7aeddd7be 89b2050f757e721 e0d78706da6096b9 6a600f80ebbeae85 184	Authentic
7.	Ayush Rai	IPEC ECE	2290	B		82e732ab650d98e 4211142d482822d 5ada368d455dad8 53184ac124d7828 2c40	Authentic
8.	Shreya Goswami	IPEC EE	8308	A		9b233c4bc4ab67b ef27ae3f8189e309 dc733794044e4e9 4a945d3370a5040 d4e	Not Authentic
9.	Pooja Gupta	IPEC CSE	2100	B		0b233c4bc4ab67b ef27ae3f8189e309 dc733794044e4e9 4a945d3370a5040 d4e	Authentic
10.	Saurabh Sharma	IPEC IT	6712	C		21da0725b4db472 52600448039ef498 dc1a0d0c0a53881 eb3af44f34470b28 7f0	Authentic

5. CONCLUSION

Currently, we exchange information over the Internet, a decentralized online medium. But when we move money, we do so through centralized, antiquated financial institutions like banks. We also use centralized systems to exchange information in other areas (such as education, where universities have complete control). Thank you to blockchain technology, this "middleman/central authority" can be eliminated. It accomplishes this by performing three critical functions: documenting transactions, establishing identity, and creating contracts. One of themost important aspects of blockchain is the protection of information. Rather than being used only to store cryptocurrencies, blockchain can also be used for any type of digital information, such as computer code.

Earlier work related to blockchain focused mainly on cryptocurrencies and their processing. Blockchain reached a peak in 2017. As investors look to ride the next wave, cryptocurrencies such as Bitcoin and Ethereum have attracted most of the interest. Currently, it is being used in various industries, including banking, education, and land registration. We can use blockchain technology as a foundation for true digitization of processes in banking and other industries. It will increase trust and give someone a faster way to validate and verify the originality of another person's documents. It will be "the first step to a corruption-free country" if we use blockchain technology in banking, land registry, education, and ID card verification.

6. ACKNOWLEDGEMENT

Efforts have been made in this area, but it would not have been possible without the generous support and help of many people and organizations. We would like to express our sincere gratitude to each and every one of them. We are very grateful to Prof. Monika Sharma for her guidance, constant monitoring, providing the necessary information about the project and helping us to carry the project to completion. We would like to thank Prof. (Dr.) Ajay Kumar, Principal of Inderprastha Engineering College, and Prof. (Dr.) Vijai Singh, Head of Computer Engineering Department, for their kind support and cooperation in carrying out this project. We would like to specifically thank each and every one of our collaborators for their time and diligence. Our thanks andappreciation also goes to our friends who helped us develop the initiative and those who volunteered their skills to assistus.

7. REFRENCES

[1] C. K. Wong and S, S. Lam "Digital signatures forflows and multicasts", WEEE/ACM Transactions on Networking, 7(4): 502- 513, 1999.

[2] A. M. Antonopoulos, Mastering Bitcoin: Unlocking Digital. Sebastopol, CA, USA: O'Reilly Media, 2015.

[3] Benyuan He, "An Empirical Study of Online Shopping Using Blockchain Technology", Department of Distribution Management, Takming University of Science and Technology, Taiwan, R.O.C., 2017.

[4] Chris Dannen, Introducing Ethereum and Solidity, https://www.apress.com/br/book/9781484225349

[5] J. Clark and P. C. van Oorschot, "SoK: SSL and HTTPS: Revisiting past challenges and evaluating certificate trust model enhancements," in proc. IEEES&P'13, May 2013, pp. 511–525.

[6] L. Zhang, D. Choffnes, D. Levin,et al., "Analysis of SSL certificate reissues and revocations in the wake of Heartbleed," in proc. ACMIMC'14, Nov 2014, pp. 489–502.

[7] M. Carvalho and R. Ford, "Moving-target defenses for computer networks," IEEE Security & Privacy, vol. 12, no. 2, pp. 73–76, Mar.- Apr.2014.

[8] Papazoglou, M., Service-Orientated Computing: Concepts, Characteristics and Directions, in International Conference on Web Information Systems Engineering. 2003, IEEE: Rome.

[9] D. Ferraiolo, R. Kuhn, and R. Sandhu, "Rbac standard rationale: Comments on "a critique of the ansi standard on role-based access control", "IEEE Security Privacy, vol. 5,no. 6, pp. 51–53, Nov 2007.

[10] A. Ouaddah, A. A. Elkalam, and A. A. Ouahman, "Towards a novel privacy- preserving access control model based on blockchain technology in IOT," in Europe and MENA Cooperation Advances in Information and Communication Technologies. Springer, 2017, pp. 523–533.

[11] L. Y. Chen and H. P. Reiser, "Distributed applications and interoperable systems, 17th ifip wg 6.1international conference, dais 2017, held as part of the 12th international federated conference on distributed computing

[12] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, "Medshare: Trust-less medical datasharing among cloud service providers via blockchain," IEEE Access, vol. 5, pp. 14 757–14 767, 2017.