EURASIP Journal on
Information Security

RESEARCH Open Access

Proposing a reliable method of securing and verifying the credentials of graduates through blockchain

T. Rama Reddy[1*], P. V. G. D. Prasad Reddy[2], Rayudu Srinivas[1], Ch. V. Raghavendran[3], R. V. S. Lalitha[3] and B. Annapurna[4]

Abstract

Education acts as a soul in the overall societal development, in one way or the other. Aspirants, who gain their degrees genuinely, will help society with their knowledge and skills. But, on the other side of the coin, the problem of fake certificates is alarming and worrying. It has been prevalent in different forms from paper-based dummy certificates to replicas backed with database tampering and has increased to astronomic levels in this digital era. In this regard, an overlay mechanism using blockchain technology is proposed to store the genuine certificates in digital form and verify them firmly whenever needed without delay. The proposed system makes sure that the certificates, once verified, can be present online in an immutable form for further reference and provides a tamper-proof concealment to the existing certification system. To confirm the credibility of the proposed method, a prototype of blockchain-based credential securing and verification system is developed in ethereum test network. The implementation and test results show that it is a secure and feasible solution to online credential management system.

Keywords: Tamper-proof digital certificates, DAPPs, Credential verification, Etherium, Blockchain

1 Introduction

As technology is advancing, the creation of fake certificates becomes easier. The forged certificates range from fake universities issuing certificates to forged certificates of existing reputed universities. Due to centralization and digitalization, this fake credentials problem became pain in the neck for both the universities and recruiting organizations, and it needs to be addressed with a sharp solution. According to CareerBuilder (https://resources.careerbuilder.com/recruiting-solutions/how-much-is-that-bad-hire-costing-your-business), a company can lose 15,000 dollars on average, for a wrong hire or for hiring someone with a fake qualification. The loss is not just financial but may also cost the lives of innocent people because of the constructions designed by fake engineers and treatment given by fake doctors. Validating the certificates properly before taking someone into an organization is the key to solve this hitch. The primary cause of this problem is that credential verification is not as easy as it is seems. It takes a lot of resources, time, and money as well.

Blockchain technology helps us in building a decentralized application that keeps all the data secure and tamper-free. In this application, the data is stored in text format to ease the implementation and testing, but once the transaction is done, the data is converted into hash values and stored in the block within the entire network. This provides security since a single bit of modification in a block should tamper all the data in the entire chain which is not possible because multiple copies are distributed in the peer network. So the integrity of the data is maintained. The proposed method is implemented and tested using ethereum test net. Whenever some data is

* Correspondence: ramatreddy@gmail.com
[1]Aditya Engineering College, Surampalem, India
Full list of author information is available at the end of the article

about to be stored in the block of an ethereum blockchain, some gas value is reduced from the admin account and distributed in the network and it acts as the reward for the miners whose system acts as the data carrier of the block. This gas is filled by spending some ether from their accounts. The etherium network limits gas availability in order to control infinite loops in the coding.

2 Related work

Research has been in progress to identify the fake documents and certificates, both paper and digital form. The following are some of the methods proposed to curtail fake documents. MV Ramana Murthy [1] presented a method to detect fake paper-based documents with ECC based digital signatures and cryptography. Xiaojing Gu [2] designed an attribute dependency-based detection method, called SSLight, in which some attribute dependencies are observed that are rarely present in legitimate samples. Dr. A. M. Kahonge [3] proposed a mechanism that uses the web and database programming, XML data sharing along with message passing via a very simple web service to share academic records between employers and the educational institutions. Zheng Dong [4] presented a scheme for detecting forged certificates from trusted CAs developed from a large and timely collection of certificates. In this method, classification is done automatically by building machine-learning models using deep neural networks (DNN). Kajal P. Chavan [5] proposed a system where the digital data, which is encrypted in the marks memo as a QR code, can only be retrieved back and decrypted by authorized users only using their web-application, which is hosted in their website. But all these are centralized applications and can be easily tampered. The following are various applications proposed based on blockchain technology. Ming L [6] proposed a blockchain-based decentralized framework for crowdsourcing named CrowdBC, in which a requester's task can be solved by a group of workers without depending on any intermediate third party, users' privacy can be guaranteed and also the required transaction fee is low. Haibo Yi [7] proposed an e-voting scheme, which is blockchain-based and meets the essential requirements of the e-voting procedure. All votes are linked using hash values in a blockchain. Yi Chen [8] designed a storage scheme to store and manage personal medical data using blockchain and cloud storage. Ali Dorr [9] proposed a blockchain-based framework to protect the privacy of users and to improve the security of the vehicular ecosystem. Xiao Yue [10] proposed an application, healthcare data gateway, whose architecture is based on blockchain to enable patient to control and share their medical reports seamlessly and securely without violating the privacy, which also provides a new way to improve the efficacy of healthcare systems while keeping patient data private. Daniel Kraft [11] stated mining as a Poisson process with time-dependent intensity and used this model to derive predictions about block times for various hash-rate scenarios. Tomaso Aste [12] published a paper that provides basic concepts of blockchain and also presented the challenges, the future opportunities, and the foreseeable impact of blockchain and distributed ledger technologies in the industry and society.

In this digital era, there is no proper method to curtail fake degrees by securing the marks memos on a tamper-proof platform and verifying them digitally using unique ID. In this paper, a method is proposed to store, secure, and verify the credentials of graduates through blockchain technology.

3 Existing method

In the presently existing system marks memos are issued directly to the students as a hard copy. There is no digitalized way to verify the certificate. Once the certificate is distributed among the students, there will be no connection between students, university, and the certificate. There is no platform to store the certificate safely and verify them when required. Therefore fake graduation degree certificates are created to get backdoor jobs. In industries, once an employee is hired, they require a background check of the educational details of the employee, and this verification is done just manually by their HR team or by some third party. There may be a delay in the process and a chance to manage the concerned section personnel of the university or college who receive the verification calls. It is even difficult to distinguish the fake and original degrees if the master register has already been tampered. Some universities store certificates in digital form but are also in a centralized network where there is a chance of tampering the certificate. Therefore, this may increase the cases of fraud since there is no means of security and integrity of the data both in manual and in digital form. The main reasons behind this problem are the lack of timestamp facility and method of storing data at a central storage.

Figure 1 explains the existing method from the admission stage of a student to the verification of the credentials of a graduate by the employers. The various stages are mentioned as follows:

1. Join/admit: students admitted to a university/affiliated college/autonomous college.
2. Results: after the semester/year-end examinations results are stored in a register/server.
3. Degree: issue of marks statements/original degree in paper form.
4. Transformed: now the students are transformed to graduates with a degree in hand.

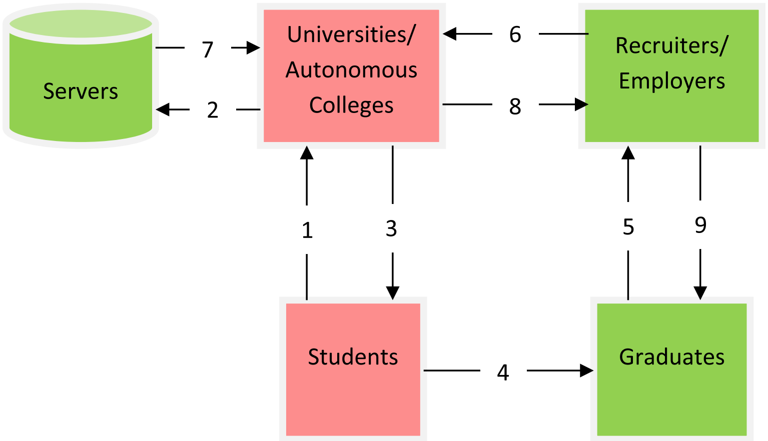


Fig. 1 Existing method from the admission stage of a student to the verification of the credentials of a graduate by the employers

5. Recruited: graduates are given a suitable job by employers/recruiters.
6. Verification request: employers request universities to verify the credentials of the employee.
7. Retrieve: universities retrieve data from the master register or a central server for verification.
8. Validate: compare the given data with the retrieved one to validate it and report it to the employer.
9. Confirm/reject: based on the report received, confirm/cancel the appointment of the graduate.

4 Proposed system

Since certificate storage and its security is a matter of concern to the university, students, and employers, the proposed system provides a platform to store and verify the student credentials using blockchain technology. Whenever a certificate is added into a block, it will return a unique certificate ID along with student Aadhar card number as a primary key. With the help of the unique certificate ID, student can verify the certificate and also the company can verify whether the certificate provided by the student is authorized or not. Apart from that, there will be an Aadhar card number of each student, by using which verifier can see all the certificates listed in the name of the same person and will be easy to verify individually. In the process to add the certificate, the certificate authority has to pay some ethereum gas value which will be reduced from the certificate authority account. This is needed for the miners which will later help to add the blocks in the blockchain in return for which they are awarded these ethereum coins. As the blockchain is distributed in nature and is popularly known as a distributed ledger, it is not easy to tamper the data stored in a block. Though not impossible, it becomes harder and harder to insert new data or modify the existing data as the length of the chain increases. It also acts as a bridge between institutions and industries. The institutions can store the candidates' academic credentials on this safe platform. And on the other hand, the industries can verify them by using the transaction id and unique candidate id like the Aadhar card number.

The advantages of this application are:

1. No one can tamper or create any fake degrees: the threat of altering the student marks, already entered in the central database of a university server is always there in existing system, which can easily be countered with the immutable and distributed nature of already created blocks of data in the proposed credentials blockchain.
2. Employer verification becomes easy and seamless: during the credential verification phase in the existing system, there is always a chance of influencing the concerned section personnel to manage the verification process. Also, the process is time-consuming as well. To counter these disadvantages, the proposed digital verification thru different sources is possible with in no time.

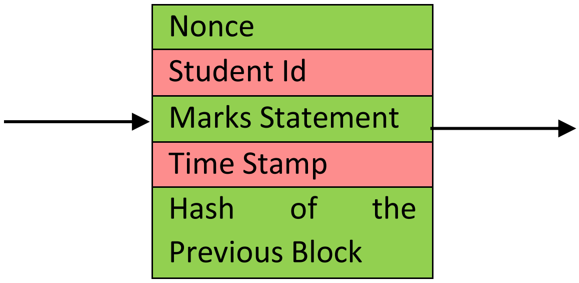


Fig. 2 The structure of the proposed block

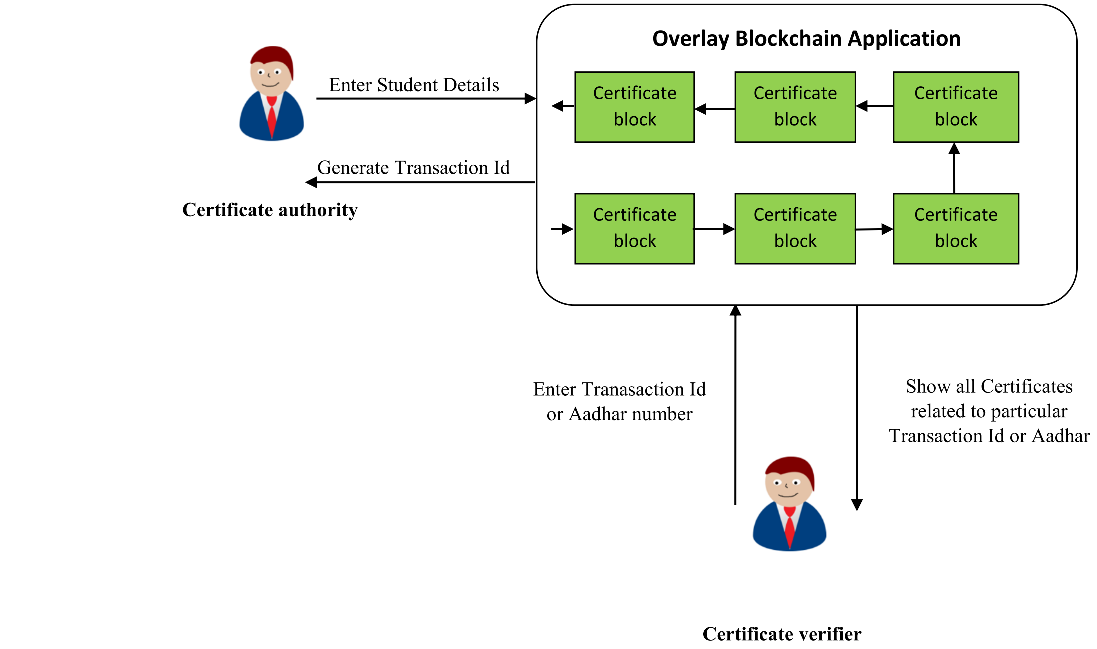


Fig. 3 Overlay blockchain application

4.1 A block and a blockchain

In the proposed system, every block contains the information shown in Fig. 2. The fields are selected to include the necessary information and may vary depending upon the requirements.

1. Nonce: a random value added by the miner to solve the hash puzzle
2. Student ID: Aadhar ID.
3. Marks statement: the details like roll no., name, class, subjects, and marks are entered in text format.
4. Time stamp: date and time of creation of the block
5. Hash value: the cryptographic hash value, which is calculated using SHA-256, of the previous block to link this new block to the existing chain

This system will maintain the integrity and security of the certificates and helps to avoid fake certificate generation. If all the companies and universities start using this portal, there will be no way to create a fake certificate and deceive the recruiter company or any further verifier. Even the timestamp will show the exact time of the certificate generated that will cover an extra layer in the security to the university certificate generation process. The proposed system acts as an overlay to the existing method of issuing physical or digital certificates by the universities and autonomous colleges.

As shown in Fig. 3, the blocks are created and attached to the chain by the certificate authorities (universities/ autonomous colleges) and the copies of the blockchain are distributed among the peer nodes of the corresponding universities and autonomous colleges. While adding the credentials to the blockchain, every entry will get a unique transaction ID (address) which can be further quoted whenever required to retrieve or verify the data along with his Aadhar ID. Through the application designed, the verifiers (recruiting companies) can access the blockchain and complete the process within no time, reliably, and also can get the details of that particular employee ID.

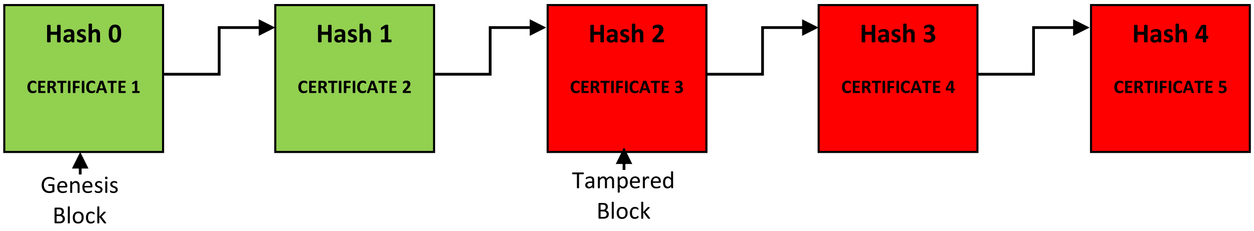


Fig. 4 Effect tampered Blocks in a particular node

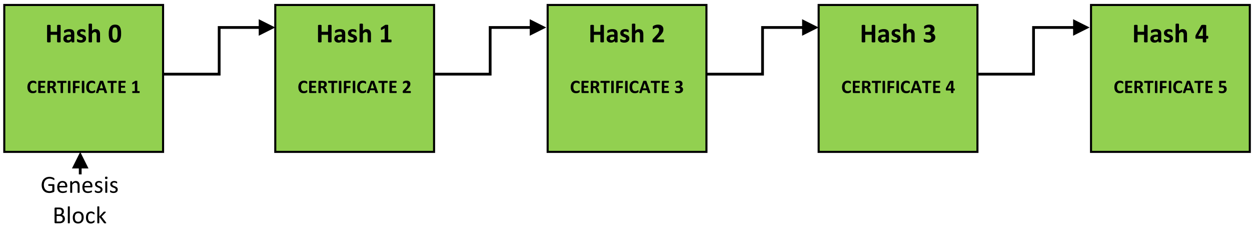


Fig. 5 Untampered blocks in other Distributed network of nodes

Suppose a blockchain is created with some certificates as blocks of data over a period of time and the copies are distributed in the network as explained in Section 4.1. If an intruder wants to alter the marks in a particular block, then its hash value will be different and will reflect the change in the next blocks of the blockchain. Even if he succeeded to change the next blocks in a particular node as shown in Fig. 4, it cannot be propagated onto the other nodes as it is a distributed network of nodes as shown in Fig. 5 and hence the change made can easily be identified during the consensus process. The same is the case with the insertion of a new block of certificate.

4.2 Data intervening proposed

In this paper, a method of data uploading, called data intervening, is proposed to facilitate the uploading of alumni data. The concept of data intervening is explained with a simple example as shown in Fig. 6. In this case, the institute needs to upload data from the year of inception, say 2016–2017, then it is proposed to initiate the blockchain from a reference academic year, say 2018–2019, upload the data of 1 year forward and 1 year backward as shown in Fig. 6. After reaching the year of inception, data uploading can be streamlined and continue in a normal way. This method helps even very old universities to include their alumni data in a hassle free manner.

4.3 Why blockchain?

One has to check some parameters before applying the blockchain technology to solve any existing problem. They are the following:

1. Are multiple parties involved in the data exchange?
2. Do different parties update data?
3. Is it required to verify the data stored?
4. Do the process of verification take significant time and money?
5. Is the time stamp of the data has any significance?
6. Do the transactions of various parties depend on one another?

If at least 4 of the 6 above questions got the answer ‘yes,’ then it is apt to go with blockchain implementation. In this credentials securing and verification system, almost all questions get the answer ‘yes.’ Hence, it clearly shows that the problem of fake certificates and delays in the verification process can be solved using blockchain technology.

5 Implementation and results

The proposed system is implemented and tested by using the following softwares: JavaScript, Truffle, Solidity, Ganache, Ethereum, and Chrome extension Metamask. Ganache is part of the Truffle ecosystem. Ganache is used for the development of DAPP (distributed application, a blockchain) and once it is developed and tested on ganache, it can be deployed on ethereum client like geth or parity. Truffle helps to develop, test, and deploy the DAPP. Metamask is one of the digital currency wallets to store and transact on ethereum using ethereum based tokens.

5.1 Features of the implemented prototype

- This application provides a tamper-proof platform to universities and autonomous colleges to publish the results and also to verify the marks memos submitted by the students to the employers.
- In this prototype, the marks are stored in text format, for simplicity. They can also be stored as an

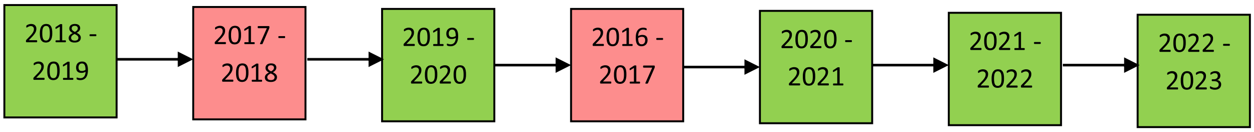
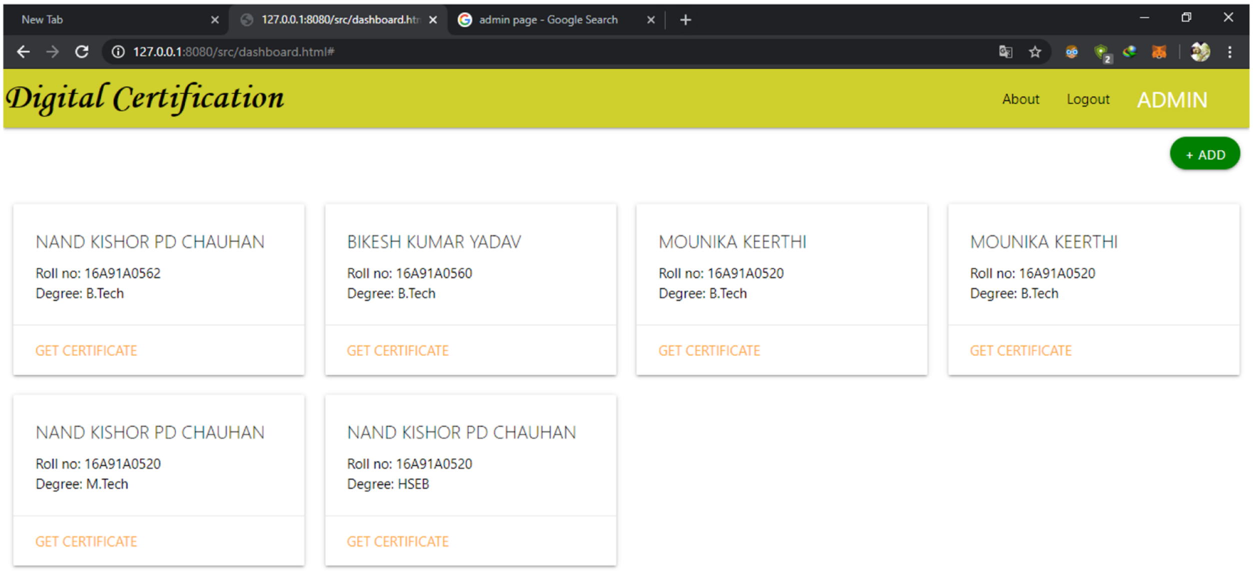


Fig. 6 Data intervening proposed to upload the alumni data


New Tab
127.0.0.1:8080/src/dashboard.htr
admin page - Google Search
127.0.0.1:8080/src/dashboard.html#
Digital Certification
About
Logout
ADMIN
+ ADD

NAND KISHOR PD CHAUHAN
Roll no: 16A91A0562
Degree: B.Tech
GET CERTIFICATE

BIKESH KUMAR YADAV
Roll no: 16A91A0560
Degree: B.Tech
GET CERTIFICATE

MOUNIKA KEERTHI
Roll no: 16A91A0520
Degree: B.Tech
GET CERTIFICATE

MOUNIKA KEERTHI
Roll no: 16A91A0520
Degree: B.Tech
GET CERTIFICATE

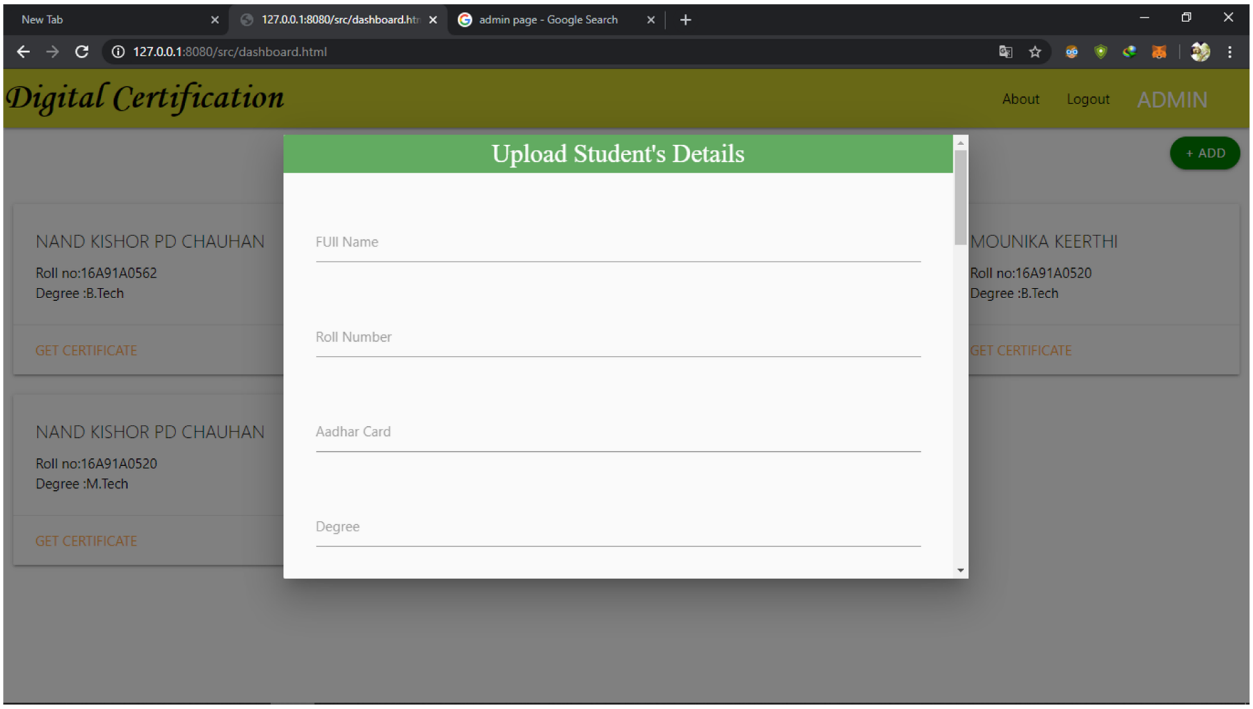
NAND KISHOR PD CHAUHAN
Roll no: 16A91A0520
Degree: M.Tech
GET CERTIFICATE

NAND KISHOR PD CHAUHAN
Roll no: 16A91A0520
Degree: HSEB
GET CERTIFICATE

Fig. 7 Application home page

image, if required. A consortium of colleges and universities manages this blockchain.

- Students who want to store their academic details on this authorized platform should approach the consortium.
- This distributed ledger (blockchain) keeps track of every academic detail of the student from X class to graduation/post-graduation.
- Only the authorized users can add marks into the blockchain.


New Tab
127.0.0.1:8080/src/dashboard.htr
admin page - Google Search
127.0.0.1:8080/src/dashboard.html
Digital Certification
About
Logout
ADMIN
+ ADD

Upload Student's Details

FUll Name

Roll Number

Aadhar Card

Degree

NAND KISHOR PD CHAUHAN
Roll no:16A91A0562
Degree :B.Tech
GET CERTIFICATE

MOUNIKA KEERTHI
Roll no:16A91A0520
Degree :B.Tech
GET CERTIFICATE

NAND KISHOR PD CHAUHAN
Roll no:16A91A0520
Degree :M.Tech
GET CERTIFICATE

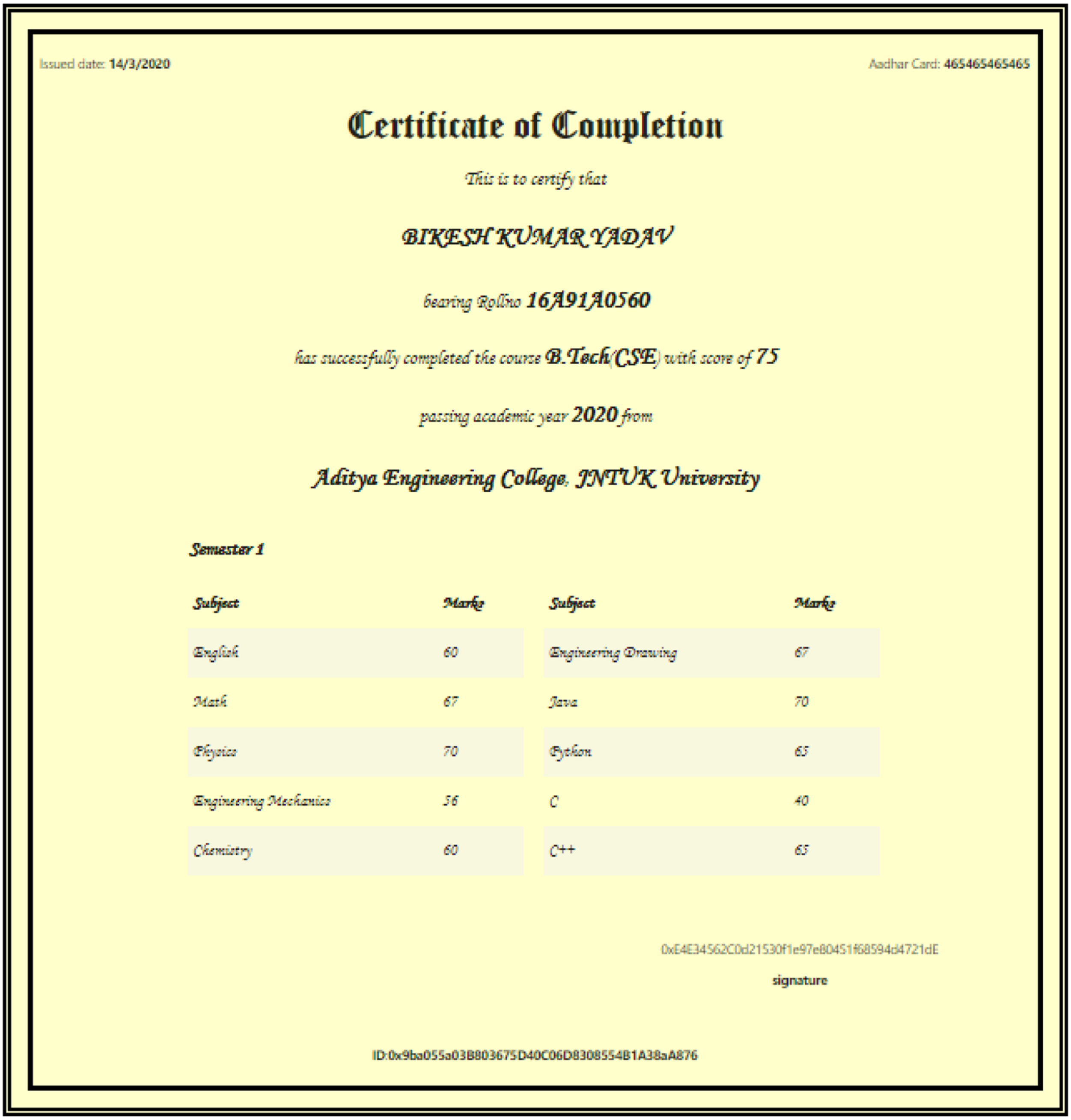
Fig. 8 Data entry form

- The credentials of the students are added along with roll number, name, marks, and unique ID like Aadhar number.
- All the generated certificates are attached with an individual certificate ID and this certificate ID is the unique ID used for verification.
- If anyone wants to check how many certificates are generated on a particular Aadhar number, then by entering Aadhar number, a report will show all the certificates generated on the particular name and Aadhar number

5.2 Glossary

Certificate authority: the person who is permitted to generate the marks memo.

Certificate verifier: the person who verifies the certificates and gets the list of certificates with respect to the Aadhar card number.



Issued date: **14/3/2020**

Aadhar Card: **465465465465**

Certificate of Completion

This is to certify that

BIKESH KUMAR YADAV

bearing Rollno ***16A91A0560***

has successfully completed the course ***B.Tech(CSE)*** *with score of* ***75***

passing academic year ***2020*** *from*

Aditya Engineering College, JNTUK University

Semester 1

Subject	Marks	Subject	Marks
English	60	Engineering Drawing	67
Math	67	Java	70
Physics	70	Python	65
Engineering Mechanics	56	C	40
Chemistry	60	C++	65

0xE4E34562C0d21530f1e97e80451f68594d4721dE

signature

ID:0x9ba055a03B803675D40C06D8308554B1A38aA876

Fig. 9 The generated certificate

Web user interface: an application that can be accessed by the user using any standard web browser and Internet connection.

Transaction ID: a unique hash ID generated when a marks memo is uploaded. This is displayed on the digital marks memo which is generated.

Gas value: gas refers to the charge required to successfully execute an instruction or a transaction on the ethereum blockchain platform to avoid infinite execution.

Wallet: to trade with ether, the wallet is a location to store and spend it in the crypto-currency world. It is nothing but a piece of code that allows to store the funds, perform transactions, and check the balance whenever needed.

5.3 Results and testing

The student data is entered into the blockchain when the add button is pressed by the certificate authority from the home page shown in Fig. 7. The data entry form shown in Fig. 8 receives complete details of the student and generates a certificate with a unique ID. The certificate is generated as shown in Fig. 9. The certificate can be verified by the recruiters using the unique ID on the certificate, whenever required. The blockchain is created by storing the data in text format to simplify the testing process. There are other methods of blockchain creation, as well. They are (1) by including hash values of the marks statements, (2) by including the root of the Merkle tree which represents an entire batch of student marks statements. The pros and cons of these methods can be discussed later and are not covered in this paper.

6 Conclusion and future work

The proposed system is a consortium blockchain among universities, their affiliated colleges, autonomous colleges, and the companies. Typically, universities first add the students' certificates and subsequently the companies or any other verifier can verify the credentials by using student's Aadhar number or transaction ID of the certificate. The data stored in a blockchain will be protected as no one can tamper it or add new transactions to it with a back date. The generated unique ID for each transaction is later used to verify the certificates. This system can be used by all the universities and colleges, in order to provide extra security to the certificates and the students' data. The problem of fake certificates can be eradicated and there will be no question of its validation. In the future, this can be extended to provide integrity to any type of documents not only to the education sector but also to government sectors where a digital document time stamp is required. Not only to store the student marks information but also to store their employment and experience data, and can also be tracked by using this proposed system. The pros and cons of creating blockchain using hash values of image or pdf format of the marks statements and also the merkle tree method can be discussed. The application of CryptCloud+ [13] can also be considered for securing the data stored in a public cloud platform.

Abbreviations

CA: Certificate authority; CrowdBC: Crowd blockchain; DAPP: Distributed application; DNN: Deep neural network; ECC: Elliptic curve cryptography; SHA: Secure Hash Algorithm

Acknowledgements

The authors would like to acknowledge the efforts of K.V. Mounika, Bikesh Kumar Yadav, and Nand Kishore Pd Chauhan, from IV B.Tech (CSE), Aditya Engineering College-Surampalem, in implementing the prototype for verification of the results and efficacy of the proposed method.

Authors' contributions

RR proposed the basic idea of applying blockchain technology to secure and verify the credentials. PR contributed in preparing the final revised draft. RS and RCh have driven the implementation of prototype to verify the efficacy of the model. LR and BA have tested the functionality of the prototype. All the authors reviewed the draft. They all read and approved the final manuscript.

Funding

Not applicable.

Availability of data and materials

The data used to test the prototype is taken randomly. The documentation and source code are available with corresponding author upon reasonable request.

Declarations

Competing interests

The authors declare that they have no competing interests.

Author details

[1]Aditya Engineering College, Surampalem, India. [2]Andhra University College of Engineering, Visakhapatnam, India. [3]Aditya College of Engineering & Technology, Surampalem, India. [4]Aditya College of Engineering, Surampalem, India.

Received: 23 July 2020 Accepted: 12 June 2021
Published online: 26 June 2021

References

1. S.G.K. Murthy, M.V.R. Murthy, A.C. Sarma, *Elliptic curve based signature method to control fake paper based certificates;* Proceedings of the World Congress on Engineering and Computer Science 2011 Vol I WCECS 2011, October 19-21, 2011, San Francisco, USA, ISBN: 978-988-18210-9-6 ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)
2. X. Gu, X. Gu, On the detection of fake certificates via attribute correlation. Entropy **17**, 3806–3837 (2015). https://doi.org/10.3390/e17063806
3. J.M. Muthoni, A.M. Kahonge, *E-verification – a case of academic testimonials (2015) UoN Digital Repository Home (http://erepository.uonbi.ac.ke)*
4. K.P. Chavan, R.R. Kamble, P.P. Meshram, K.K. Doke, QR code based digitized marksheet system. Int. J. Eng. Res. Adv. Technol. ISSN **02**(03), 24546135 (2016)
5. D. Zheng, K. Kane, L.J. Camp, Detection of rogue certificates from trusted certificate authorities using deep neural networks, ACM Transactions on Privacy and Security, **19**(2), 1–31 (2016) https://doi.org/10.1145/2975591
6. M. Li et al. CrowdBC: A Blockchain-Based Decentralized Framework for Crowdsourcing. IEEE Trans Parall Distrib Syst, **30**(6), 1251-1266 (2019) https://doi.org/10.1109/TPDS.2018.2881735.

7. Yi, H. *Securing e-voting based on blockchain in P2P network.* J Wireless Com Network **2019**, 137 (2019). https://doi.org/10.1186/s13638-019-1473-6
8. Chen, Y., Ding, S., Xu, Z. et al. *Blockchain-Based Medical Records Secure Storage and Medical Service Framework*. J Med Syst, **43**, 5 (2019). https://doi.org/10.1007/s10916-018-1121-4
9. A. Dorri, M. Steger, S. S. Kanhere and R. Jurdak. *BlockChain: A Distributed Solution to Automotive Security and Privacy.* IEEE Communications Magazine, **55**(12) :119-125 (2017). https://doi.org/10.1109/MCOM.2017.1700879
10. X. Yue, H. Wang, D. Jin, M. Li, W. Jiang, Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. J. Med. Syst. **40**, 218 (2016). https://doi.org/10.1007/s10916-016-0574-6
11. D. Kraft, Difficulty control for blockchain-based consensus systems. Peer-to-Peer Netw. Appl.. https://doi.org/10.1007/s12083-015-0347-x
12. T. Aste, P. Tasca, T. Di Matteo. Blockchain Technologies: The Foreseeable Impact on Society and Industry. Computer, **50**(9), 18-28 (2017). https://doi.org/10.1109/MC.2017.3571064
13. J. Ning, Z. Cao, X. Dong, K. Liang, L. Wei, K.-K.R. Choo, CryptCloud$^+$+: secure and expressive data access control for cloud storage. IEEE Trans. Serv. Comput. **14**(1), 111–124 (2021). https://doi.org/10.1109/TSC.2018.2791538

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.