Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 171 (2020) 790–799

Procedia Computer Science

www.elsevier.com/locate/procedia

Third International Conference on Computing and Network Communications (CoCoNet'19)

Smart Contract based Central Sector Scheme of Scholarship for College and University Students

Punam Bedi[a], Pushkar Gole[b,*], Shivani Dhiman[c,*], Neha Gupta[d]

[a,b,c,d] *Department of Computer Science, University of Delhi, Delhi, 110007, India*

Abstract

Education plays a vital role in human life. To encourage higher education, the Indian government has taken many initiatives. These include the disbursement of scholarships to financially help the students belonging to low-income families. Central Sector Scheme of Scholarship for College and University Students (CSS) is one such scheme that financially helps meritorious students in pursuing graduation and post-graduation. This scheme was introduced in 2008. Scholarships from CSS have been helping students to fund their educational expenses. But there have been some difficulties faced by the students in availing this scholarship. These include lack of traceability of application form, loss of application form in transit through Indian Postal Service, lack of transparency between students and their respective Education Boards, and lack of bank account verification. In this paper, we propose a Smart Contract for CSS Scheme that overcomes the above-mentioned drawbacks. It has four entities: Students, Education Boards, Colleges, and Banks. The Blockchain-based Smart Contract proposed in this paper, has been developed to provide a user-friendly environment to a student and maintain a transparent and constant connection between students and their respective Education Boards. Many applications have been developed on the Blockchain platform but to the best of our knowledge, there does not exists any government scholarship scheme on the Blockchain platform in India.

© 2020 The Authors. Published by Elsevier B.V.
This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/)
Peer-review under responsibility of the scientific committee of the Third International Conference on Computing and Network Communications (CoCoNet'19).

Keywords: Blockchain; Smart Contract; Central Sector Scheme of Scholarship for College and University Students

1. Introduction

The Department of Higher Education, Ministry of Human Resource Development (MHRD) manages the planning and policy making process for higher education in India. It also takes care of the disbursement of the various

1877-0509 © 2020 The Authors. Published by Elsevier B.V.
This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/)
Peer-review under responsibility of the scientific committee of the Third International Conference on Computing and Network Communications (CoCoNet'19).
10.1016/j.procs.2020.04.086

scholarships. National Scholarship which is provided by Indian government and External Scholarship which is offered by various other countries are two types of scholarship taken care by Department of Higher Education, MHRD. To promote higher education and financially help meritorious students belonging to low-income families, Indian government's Central Sector Scheme of Scholarship for College and University Students (CSS) plays an important role. This scheme has four entities: Students, Education Boards, Colleges and Banks. In the existing process of the CSS Scheme, the authentication of a student is done by his College and the Education Board. The task of student authentication is done manually by both entities and it is time consuming. Bank entity does not verify the student's bank information.

There are two amendments that have been done since 2008 in the CSS Scheme. In January 2013, CSS Scheme was included in the Direct Benefit Transfer (DBT) programme [1]. According to this programme, the scholarship will be sent directly to the student's bank account. In July 2015, under the Digital India Initiative [2] a web portal was introduced for scholarships named, National Scholarship Portal. CSS Scheme was shifted to this platform in 2015. There have been continuous efforts to improve the existing system, but there are still some areas where the improvement is required. To automate and improve the existing system, we propose Blockchain based Smart Contract for CSS Scheme. A Smart Contract runs on Blockchain technology which provides the decentralization and tamper-proof records. Smart Contract for CSS Scheme will automate the existing system and reduce the need for manual labor, hence reduce the time consumption.

This paper is organized into six sections. In section 2, different applications that have been developed on the Blockchain platform are described. Section 3 explains about the Central Sector Scheme of Scholarship for College and University Students, Blockchain, and Smart Contract. Section 4 explains the details of our proposed system. Section 5 explain the technologies used in the development of Smart Contract for CSS Scheme. Section 6 describes the conclusion and future scope.

2. Related Work

The term Blockchain was first coined by Satoshi Nakamoto in his white paper Bitcoin: A Peer to Peer Electronic Cash System [3]. Blockchain working and its various properties like privacy, anonymity, and security, are explained in [4]. Blockchain has numerous applications in both financial and non-financial fields. These applications are described in [5]. Ethereum is one of the most popular Blockchain platforms. Ethereum provides the platform for the development of Smart Contracts and Distributed Applications. The working of Ethereum is defined in [6]. Various real-life applications have switched to the Blockchain platform using Smart Contract [7]. Some of these applications are in the field of agriculture, health care, e-waste management, business applications, expert system, and trust-based systems [7], [8] .To the best of our knowledge, Smart Contract based scheme for scholarship distribution in India has not been proposed until now in any existing research work.

3. Background

This section of the paper describes CSS Scheme and the basic concepts of Blockchain and Smart Contract.

3.1 Central Sector Scheme of Scholarship for College and University Students

Central Sector Scholarship Scheme for Colleges and University Students (CSS) is one of the national scholarships offered by MHRD. It was introduced in the 11^{th} five-year plan in 2008. The aim of CSS Scheme is to help the meritorious students belonging to low-income families, in their educational expenses while pursuing their graduation, post-graduation, or some professional courses. The CSS Scholarship is awarded to 82,000 student and is equally distributed between boys 41,000 and girls 41,000 [1]. Total scholarship funds are distributed among Central Board of Secondary Education (CBSE), Indian Certificate of Secondary Education (ICSE), and various Education Boards and further every Education Board divides the scholarship among their students of different streams. The time period for the scholarship is 3 years for graduation and 2 years for post-graduation. The amount of scholarship is 10,000 INR annually at graduation level and 20,000 INR annually at post-graduation level.

- **Eligibility Criteria**: The meritorious students scoring at least 80th percentile in class 12th and belonging to non-creamy layer (i.e. not belonging to creamy layer defined by the Department of Personnel and Training) of the society are eligible to avail this scholarship [9]. To avail the benefits of Scheme, a student must pursue his/her higher studies from the institutions recognized by All India Council of Technical Education (AICTE), UGC Act, 1956, Medical Council of India, or Dental Council of India [10]. The students pursuing diploma courses, correspondence or distance mode of education are not eligible for the CSS Scheme. After successfully applying for the scholarship in the first year on the basis of marks obtained in class 12th, the student must keep securing at least 50% marks in the graduation and post-graduation examinations. The attendance of the student must be at least 75% in the classes and not indulged in any ragging activities.

- **Working of Existing CSS Scheme:** Application forms are released in the month of June-July every year, the student uses the National Scholarship portal www.scholarships.gov.in to apply for the scholarship. They fill the form, submit it, and take a print out of submitted form. Then the student goes to the administrative staff of the college or university in which they are pursuing their current course and gives the printed form to the staff for manual verification, updating the attendance in the form and attestation by the head of institution to ensure the authenticity of the application form. The student will get the form verified by the college and post the verified form with necessary documents to the office of his respective Education Board. Mark sheet of last examination, bank passbook, and income certificate (only for first time, no need in renewal process) are to be posted with the attested form [10]. These documents should reach at office of Education Board before the last date of submission. This process is repeated every year for the renewal till the student have complete their graduation or post-graduation.

There are some challenges faced by the students in availing the scholarship. The verification and attesting of application form in colleges is done manually and hence it is time consuming. The active or inactive status of the bank account is not checked by authorities, if inactive then the scholarship funds will be returned back to the Education Board. The application form is to be posted to the Education Board office by the Indian Postal Service. During transportation, application may get lost and Education Board will not be able to authenticate the student information.

3.2 Blockchain

Blockchain is the core technology used in Bitcoin- the first digital cryptocurrency. It was developed by a person or group of persons named Satoshi Nakamoto whose identity is not revealed until now [3]. Earlier all monetary transactions required a trusted intermediary. After the development of Bitcoin, the end-users can transfer the funds without the trusted intermediaries.

Table 1. Fields in Block

Fields in the Block	Size of the Field in Bytes	Description of the Field
Block Size	4	2
Block Header	80	4
Transactions	1-9	6

The Blockchain is a data structure, like a linked list which is connected with the help of cryptographic hash (SHA-256) [11] of the previous block. The Blockchain stores the data in the form of blocks. Each block contains various fields like block header, transaction counter, transactions, and block size. These fields are described in Table 1 [12]. A block is uniquely identified using the block header. Block header contains various fields like previous hash, Merkle root, timestamp, difficulty target, and nonce. These fields are described in Table 2 [12].

Table 2. Fields in Block Header.

Field	Size of Field in Bytes	Description of the Field
Version	4	Various versions of blocks
Previous Hash	32	Reference to previous block
Merkel Root	32	The root of Merkel tree
Timestamp	4	Block's creation time
Difficulty target	4	Used in Block mining
Nonce	4	Counter used in Block mining

Each block contains a set of transactions. These transactions are similar to entries in the book-keeping records that have double-entry in them. Each transaction has one or more input, which act as debits for a user and one or more outputs, which are credits added to a user's account. It is not necessary that all input and output sum up to the same amount, but output can sum up to slightly less than input. This difference is referred as the transaction fees that is a little amount charged, by the miner to include a transaction in a block, and eventually in Blockchain [12].

To perform a transaction user needs to download a cryptocurrency wallet which contains a pair of keys- public key and private key. A transaction is formed by selecting necessary inputs and outputs, according to sender's specification. Sender only needs to specify the receiver and amount to be transferred. All internal working details are hidden from the sender. Once a transaction is formed it is digitally signed using Elliptic Curve Digital Signature Algorithm (ECDSA) [13] by the private key of the sender. After this transaction is propagated to the nearby nodes of Blockchain network. These nodes then verify the integrity of the transaction by verifying the digital signature using sender's public key. It is also verified that input specified in the transaction are unspent or not. If the transaction get successfully verified then it is stored in Transaction pool. A Transaction pool is a storage which contains those transactions that are not included in any block till now.

Transaction is propagated over the network of Bitcoin, but until now it is not included in the Blockchain. Mining is a process to include a transaction in a block after verifying it. Verification by computation is the basis of the Bitcoin system. Transactions are grouped into blocks, which require a lot of computation. Miner collects the transactions from transaction pool and builds a Merkle tree [12] to summarize all transactions in 32 bytes. Miner also constructs the block header of the new block according to the format defined in Table 2. Then the miner can validate the newly created block, using Proof-of-Work algorithm [12]. After mining, miners broadcast the newly created block over the Blockchain network. The other nodes and miners then verify the block. This block is then appended to the Blockchain if it gets a consensus about the correctness on the Blockchain network.

3.3 Smart Contracts

A Smart Contract is a self-operating computer program that automatically executes when certain conditions are met. Smart Contracts were invented by an American computer scientist, Nick Szabo in 1994 [14]. Smart Contracts allow selling and purchasing of goods, real estates, securities, etc. Once the required conditions are met, the Smart Contract executes the required operation. There are following advantages of Smart Contracts:

- **Speed:** Manual scanning and processing document takes a lot of time which leads to delays in the completion of the process. A Smart Contract is an automatic process and it does not require human involvement which saves precious time.
- **Independence:** Smart contracts remove the requirement of third-party.

- **Reliability:** Data in a Blockchain cannot be destroyed or altered.
- **Less error:** Since there is no human interference so there is less chance of human errors.
- **Savings:** Smart contracts provide a significant amount of savings due to the elimination of expenses for third-party.

Smart Contracts also have following disadvantages [15] :

- **Lack of regulation:** As of now, there are few laws for Blockchain, Smart Contracts, and cryptocurrencies in the International legal field.
- **Difficult implementation:** It takes a lot of time to map the smart contracts terms to the real world entities.
- **Impossibility of changing a Smart Contract:** Ironically, one of the major advantages of the smart contract can become a disadvantage. It is not possible for a party to alter the existing condition in the Smart contract.

Ethereum is a platform for building and executing decentralized applications in the form of Smart Contracts. Ethereum was introduced by Vitalik Buterin in 2013 [16]. Ethereum runs on Blockchain platform which makes it decentralized. Users can gain Ethers by mining and transfers from other users. Since decentralized applications run on Ethereum Blockchain some of the following implicit properties of Blockchain are inherited automatically [17].

- **Immutability:** No one can change the previous record.
- **Corruption and temper proof:** Since Blockchain follows consensus algorithm, so applications also inherit this property.
- **Secure:** There is no single point of failure. Blockchain is secured by cryptography so applications are protected against hacking and fraudulent attacks.
- **Zero downtime:** Applications never get switched off.

4. Proposed System for Central Sector Scheme of Scholarship for College and University Students

The CSS Scheme depends on four individual entities. These entities are Education Boards, Students, Colleges, and Banks. These entities are explained in the following subsections in detail. Fig. 1 shows the process flow and the interaction between these four entities diagrammatically.

- **Education Boards**: The Education Boards are responsible for selecting the meritorious students based on their percentage of marks in class 12th. The students who applied for the scholarship will be authenticated by this authority with the documents provided by the students. In the proposed system, the entity corresponding to Education Boards has been automated with the help of Smart Contract. Smart Contract contains all the conditions along with the functions to execute when those conditions met. The first step of the process will be the deployment of the Smart Contract. According to the guidelines of CSS Scheme, top 82,000 students should be selected that can apply for the scholarship. Every board has been assigned certain number of students like Central Board of Secondary Education (CBSE) board has been assigned with 5413. From CBSE database top 5413 students will be selected to avail the scholarship. When a CBSE student applies for the scholarship, certain checks will be performed by the system, like if the student belongs to top 5413 students, if not then the student is not eligible for the scholarship and will not be able to get the application form. If the student is authenticated successfully, then the student can access the form, fill the details, and upload an income certificate to prove that the student belongs to non-creamy layer. Bank and College also need to verify the students. After verification by bank and college entities, the students will be added to Blockchain for 3 years for graduation and this period can be extended to 2 more years if students pursue their post-graduation course. The students have to be successfully authenticated by the Smart Contract and then on a specified date student will receive the scholarship in their respective bank accounts. Further every year the process is repeated for the student who have completed their class 12th and the students who apply for renewal. When the duration of the pursuing course gets finished, Smart

Contract removes the students from Blockchain. Smart Contract for CSS Scheme uses web interface for the inputs of the application form and confirm the details of students from the Education Board's database itself. The manual work that was needed to perform the document authentication is not needed anymore, since the authentication is being done digitally, the challenge of lost application form during transportation has been resolved.

- **Student:** In the existing procedure of CSS Scheme, a student can register to avail the scheme, and he/she can track the status of their application. This registration is done by filling an online form on the National Scholarship Portal. This form captures the personal, academic, and bank details of the student. In the Smart Contract of CSS Scheme, the already registered student first has to log in using their roll number, certificate number, year of passing, and percentage of marks obtained in class 12th. If the above details are successfully authenticated on the server of CBSE, then the student is redirected to fill the CSS Scheme form. After successfully filling all the details of the CSS Scheme form, the student is redirected to the success page. A student can also track the status of their application using the roll number of class 12th. In the implementation of student entity, a check point is introduced after every step of process to keep the track of application form. Fig. 2 shows the login portal for students.

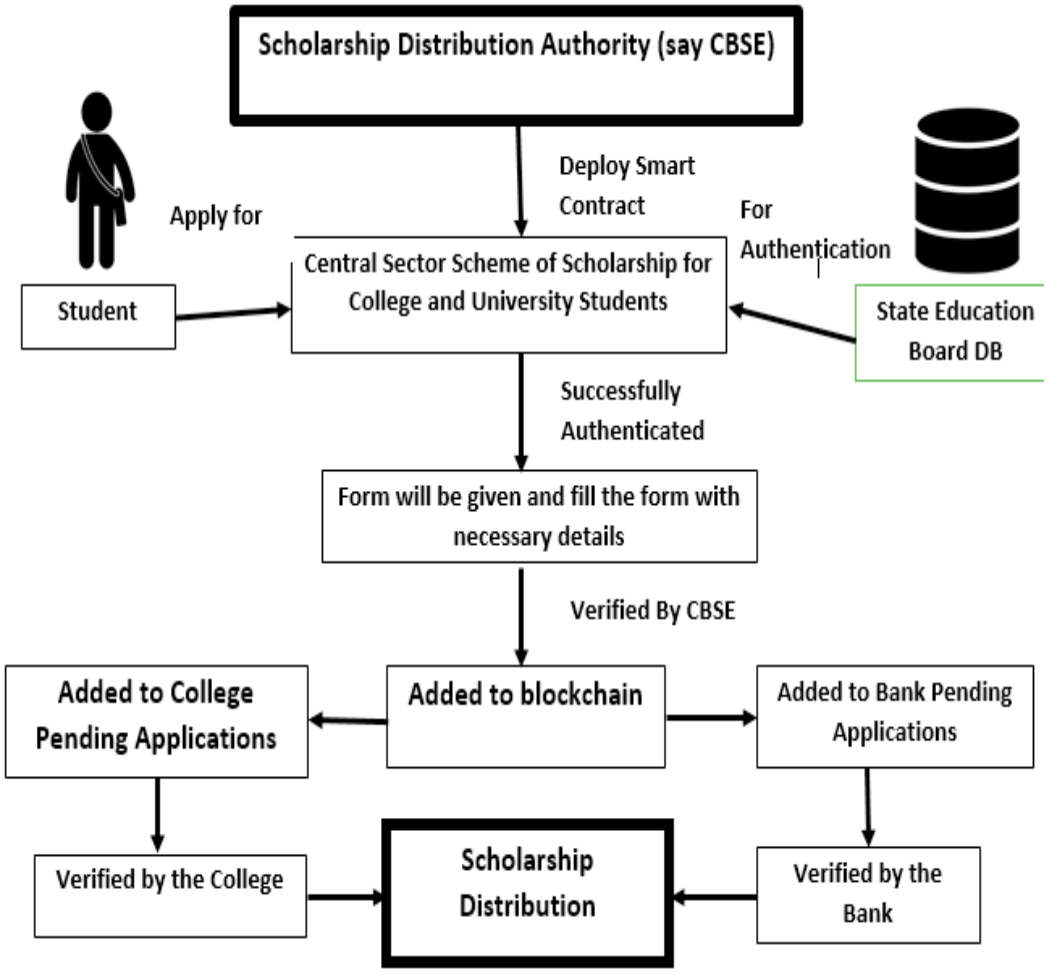


Fig. 1. Interaction between Education Board, Students, Colleges, and Banks

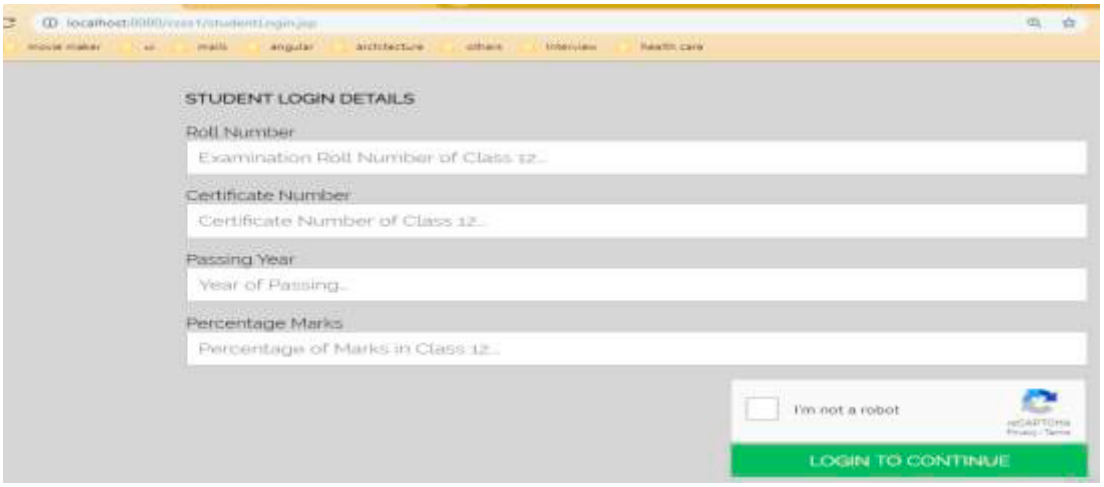


Fig. 2 Login portal for the students

- **College:** The role of college entity in CSS Scheme is to verify that a particular student is registered in their college or not. It also updates the percentage of marks and attendance of the student in the course that is being pursued by him. Using these details, CBSE entity can verify that a particular student is eligible for the scheme. In the proposed system, whenever a student fills the CSS Scheme form successfully, a pending application for college is created. This step is shown in Fig. 3. Authorized college staff can update the necessary details of pending applications after logging in with their credentials. These details are the percentage of marks and attendance of the pursuing course.

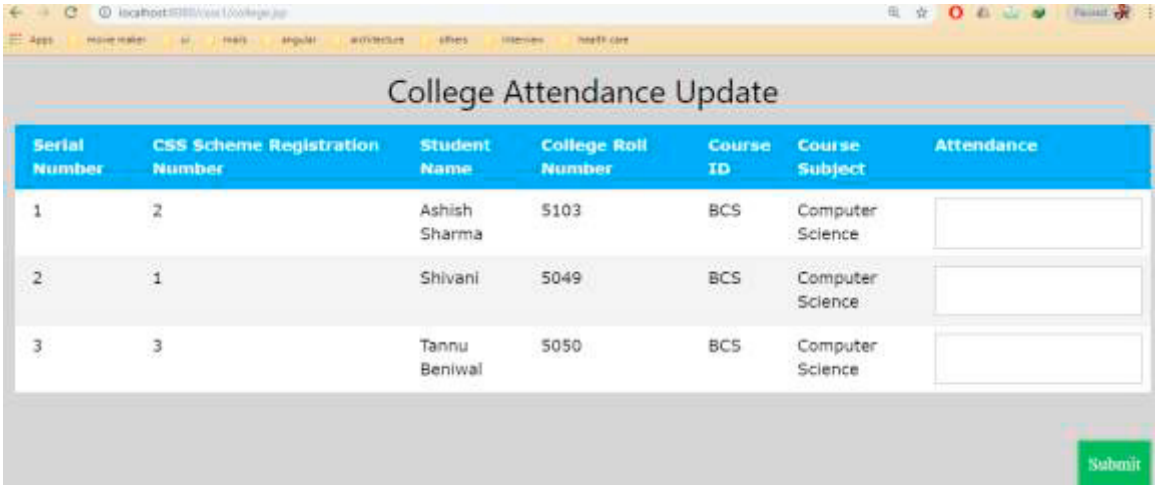


Fig 3. Interface of College to Update and Verify Student Details in the Smart Contract for CSS Scheme

- **Bank:** The bank plays an important role in CSS Scheme. Under the DBT programme, the scholarship funds are directly transferred to the student's bank account. This step was taken to ensure the scholarship reached directly to the student and it also helps in tracking the scholarship funds. A web portal has been developed for the bank associates to access the data regarding student bank account. Only an authorized person will have credentials to access the web portal. In Smart Contract of CSS Scheme, whenever a student successfully submit the application form, a row of student's bank account information with an additional field to confirm the active or non-active status is created in the Bank Pending Applications. This step is shown in Fig. 4.The authorized person will

confirm the active or inactive status of a student's bank account. It helps to maintain a tamper-proof record of scholarship distribution and provides a detailed record of monetary transactions to the Indian government. It is a necessary step to take because if the status of student's bank account is not active, a notification can be generated to remind the student to active his/her bank account status which is not present in the existed system.

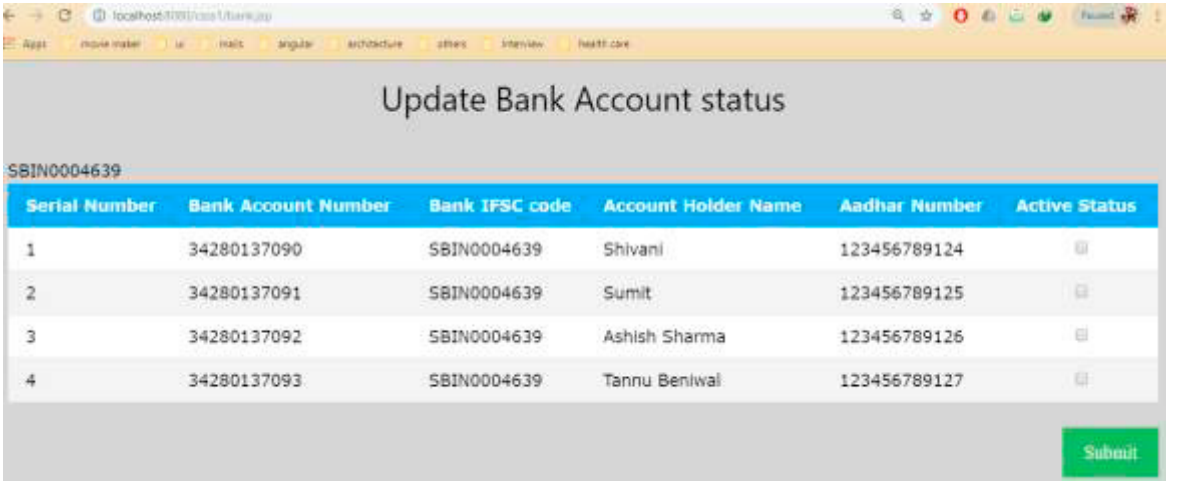


Fig 4. Interface of bank to update student bank account status in the Smart Contract for CSS Scheme

5. Experimental Study

A Smart Contract has been developed to test the proper functioning of the proposed system. The entities defined in section four were implemented in Solidity and Java Server Pages (JSP) using NetBeans IDE 8.2, Remix Ethereum IDE, and Web3j. NetBeans is an integrated development environment for JSP. Remix is an integrated development environment written in JavaScript. It is an open source tool and it can be accessed directly from https://remix.ethereum.org. It is used for writing, debugging, and testing the Solidity Smart Contracts.

Web3j is a lightweight and highly modular Java and Android Application Programming Interface (API) for working with Smart Contracts. Truffle provide a framework named Ganache which is used to test the functioning of Smart Contract using Web3j. It is available as a Desktop application as well as a command line tool.

The web interface of Smart Contract tested against various attacks. These attacks are executed using the Kali Linux 2019.1a. The application was successfully handling the attacks mentioned in Table 1.

The Smart Contract for CSS Scheme is tested by performing different attacks. We perform time jacking on our application by changing the time of a system but it was successfully prevented by continuously synchronizing the time of server with Indian Standard Time (IST) using NTP protocol. Next attack is phishing attack. We perform it with the tool named Weeman. The phishing attack was not able to compromise our application because of the Google Recaptcha within our application. Next attack we perform is the bot based brute force attack on passwords that was implemented by java script and successfully prevented with the help of Google Recaptcha within the application. Overflow and underflow is prevented by updating the value of variable under a range.

Our application is also secured against the Sybil attack, Race attack and Eclipse attack due to Ganache. Ganache simulates Ethereum private Blockchain and is inherently secured against Sybil, Race and Eclipse attacks. Ganache implements Casper algorithm to prevent against Sybil. Eclipse attack is prevented by limiting the incoming and outgoing connections in Ganache. Ganache auto mines a transaction and add it to a block as soon as it is sent on the Ethereum network so race attack is not applicable on the application. Replay attack can be executed on the application because it is built on non-fork blockchain.

The application was unable to prevent the Denial of Service and Man in the Middle attack. However, Man in the Middle attack can be prevented using HTTPS protocol and Denial of Service attack can also be prevented using any commercial blockchain platform like Ethereum, Hyperledger, R3Corda, and Hashgraph.

6. Conclusion and Future Work

In this paper, a Smart Contract for Central Sector Scheme of Scholarship for College and University Students was designed and implemented. In the existing procedure of CSS Scheme, there were several difficulties like lack of traceability of application form, loss of application form in transit through Indian Postal Service, lack of transparency between students and the Education Boards, and lack of bank account verification. With the help of blockchain, we were able to achieve transparency among the student entity and the Education Board entity. With the automation of the existing CSS Scheme, the students no longer faces the challenge of lost application form in transit. Various check points have been introduced in the automated system to keep track of application forms. Hence, the proposed system was successfully able to overcome the above-mentioned difficulties. CSS Scheme consists of four entities: Education Board, Students, Colleges, and Banks. Blockchain-based Smart Contract for CSS Scheme provides a user-friendly environment for students and maintains a transparent connection between students and their respective Education Boards. The web interface of the Smart contract was successfully tested against Denial of Service attack, Time-Jacking attack, Phishing attack, Man in the middle attack, Brute force attack on passwords using the bot, Sybil attack, Eclipse attack, Replay attack, Overflow attack, Underflow attack, and Race attack but failed against the Denial-of-Service attack and Man in the Middle attack.

In future, the testing of the Smart Contract will be performed against attacks like Impersonation attack, Session-Hijacking attack, Decentralized Anonymous Organization (DAO) attack, and Quantum computing based attacks, to make it more secure and robust. Currently, the system is limited to a web-application. In future, it can be extended as a dedicated smartphone application.

References

[1] Singh M. (2013) “Direct Benefit Transfer”. Available at https://dbtbharat.gov.in/data/documents/archivel1.pdf.

[2] Malik R. (2015) “Central Sector Scheme of Scholarship for College and University Students - Inviting of applications for Fresh 2015 Batchon National e-Scolarship Portal”. Available at https://mhrd.gov.in/sites/upload_files/mhrd/files/CSSSCU.pdf.

[3] Nakamoto S. (2008) “Bitcoin: A peer-to-peer electronic cash system”. Available at http://bitcoin.org/bitcoin.pdf.

[4] Can Kus Khalilov M. and A. Levi. (2018) “A Survey on Anonymity and Privacy in Bitcoin-Like Digital Cash Systems”. IEEE Communications Surveys and Tutorials,: 1-1.

[5] Tasatanattakool P. and C. Techapanupreeda. (2018) “Blockchain: Challenges and applications”. International Conference on Information Networking (ICOIN), Thailand: 473-475.

[6] Vujicic D, D. Jagodic and S. Ranđić. (2018) “Blockchain technology, bitcoin, and Ethereum: A brief overview”. 17th International Symposium INFOTEH-JAHORINA (INFOTEH), East Sarajevo: 1-6.

[7] Hughes L, Y. K. Dwivedi, S. K. Misra, N. P. Rana, V. Raghavan and V Akella. (2019) “Blockchain research, practice and policy: Applications, benefits, limitations, emerging research themes and research agenda”. International Journal of Information Management 49: 114-129.

[8] Gupta N. and Punam Bedi. (2018) “E-waste Management Using Blockchain based Smart Contracts”. International Conference on Advances in Computing, Communications and Informatics (ICACCI), Bangalore: 915-921.

[9] Singh A. and Kapil Sibal. (2013) “Annual Report 2008-09”. Available at https://mhrd.gov.in/sites/upload_files/mhrd/files/document-reports/AR2008-09.pdf.

[10] Kumar M. R. (2018) “Central Sector Scheme of Scholarship for College and University Student”. Available at https://scholarships.gov.in/public/schemeGuidelines/Guidelines_DOHE_CSSS.pdf.

[11] Yoshida and A. Biryukov. (2006) “Analysis of a SHA-256 Variant”. Selected Areas in Cryptography, Berlin: 245-260.

[12] Antonopoulos A. M. (2014) “Mastering Bitcoin: Unlocking Digital Crypto-Currencies”. 1st editon., O'Reilly Media, Inc..

[13] Johnson D, A. Menezes and S. Vanstone. (2001) “The elliptic curve digital signature algorithm (ECDSA)". International journal of information security 1: 36-63.

[14] Christidis K. and M. Devetsikiotis. (2016) “Blockchains and Smart Contracts for the Internet of Things”. IEEE Access 4: 2292-2303.

[15] Macrinici D, C. Cartofeanu and S. Gao. (2018) "Smart contract applications within blockchain technology: A systematic mapping study". Telematics and Informatics, 35: 2337-2354.

[16] Buterin V. et.al. (2013) "Ethereum white paper". Available at http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf.

[17] Wang S, L. Ouyang, Y. Yuan, X. Ni, X. Han and F. Wang. (2019) "Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends". *IEEE Transactions on Systems, Man, and Cybernetics: Systems:* 1-12.