Received: 31 May 2025 | Revised: 4 August 2025 | Accepted: 29 August 2025 | Published online: 17 October 2025

RESEARCH ARTICLE

Journal of Data Science and Intelligent Systems
2025, Vol. 00(00) 1-9
DOI: 10.47852/bonviewJDSIS52026319

Implementation of Smart Contracts in Digital Education Systems

Ashis Kumar Samanta[1,*]

[1] *University of Calcutta, India*

Abstract: The Blockchain is an emerging technology that is used in various applications for data security and trustworthiness. In the case of a public Blockchain, the data cannot be edited or deleted. In the case of a consortium and private Blockchain, the data can be edited or deleted based on the assigned permission, and the data privacy can be maintained. Blockchain's smart contract provides security to stored data, but it is vulnerable to various security threats. Smart contracts still suffer from different variabilities like distributed denial of service attacks (DDoS), 51% vulnerability attacks, double-spending problems, and mining Pool attacks. The smart contract, run on a Blockchain framework, is the logical contract between two or more anonymous people without involving a third party. Hyperledger and Ethereum are two important frameworks that support the development of smart contracts using Blockchain technology. This paper has tried to analyze the security issues of smart contracts developed on the Ethereum framework. An application of class scheduling management and student attendance management has been designed to validate and generate a smart contract.

Keywords: Blockchain, smart contract, online learning security, security threats of e-learning

1. Introduction

The teaching–learning process in the case of developing countries like India was mostly a conventional method, though the distance mode of education was also introduced passively. The distance education process also tried to find a way to mitigate the gap between conventional and distance modes and maintain quality. The COVID-19 pandemic has come with a revolution and technological advancements in the educational domain. During the pandemic, e-learning methods have become the primary means of providing education, from kindergarten (KG) to postgraduate (PG). Information and Communication Technologies (ICT), mobile, laptop, Zoom, and Google Meet became the driving force of the e-learning systems.

The conventional e-learning process generally suffers from (Figure 1) the following issues [1],

1.1.Technical issues

1) **Data tampering:** The transacted data of the e-learning process has a high chance of tampering. Therefore, proper security measures are taken [2].
2) **Loss of privacy:** If the transaction is insecure, there is a high chance of losing their data privacy [1].
3) **Unauthorized access:** The data used in the e-learning system may be accessed unauthorized due to a lack of knowledge of security in the network, host, and client levels [3].
4) **Transparency:** The transaction data used in the e-learning system may be tampered with or may have a high chance of hacking, causing a breach of privacy if the data is not kept, and the conventional system also faces transparency issues [1].

1.2. Non-technical issues

1) **Copyright and proprietary issues of data:** The copyright and proprietary property will be violated in case of an insecure e-learning system [2].
2) **Social trust:** The process and the technology that have been used need to be acceptable by society regarding its trustworthiness and quality [2].
3) **Cost:** The cost needs to be reduced in individual respect and in a collective way of the process of e-learning [1].
4) **Academic credibility:** If the data becomes hacked or unauthorized accessed, the legal and social credibility of the institute will be reduced, and the institution will be under scrutiny [4].

Blockchain technology has been introduced into the technological market to provide a new security dimension in the education sector [2]. The introduction of smart contracts on the Blockchain framework has become the introduction of cryptographic-based self-execution paperless technology that secures the e-learning process with respect to security threats and its acceptance in society [5]. Implementing Blockchain technology and its continuous improvement is part of the empirical research process. The data are tamperproof in Blockchain.

In case of any tampering, the origin of the tampering can be identified; hence, the system is much more transparent. Several industrial Blockchain applications have been developed, and this encrypted technology has also covered a more extensive domain (Figure 2 and Table 1) of the education sector [6].

The implementation of Blockchain makes the system trustworthy and secures transactional data. Blockchain is a measure of itself of the security of transactional data. But still, the Blockchain is suffering from continuous internal and external security threats (Figure 3), that are analyzed below [7].

1) **DDoS attack:** The attack, like Distributed Denial of Service (DDoS), happens by reducing the mining process and efficiency of the applications.

***Corresponding author:** Ashis Kumar Samanta, University of Calcutta, India. Email: aksdba@caluniv.ac.in

Figure 1
Issues of conventional e-learning process

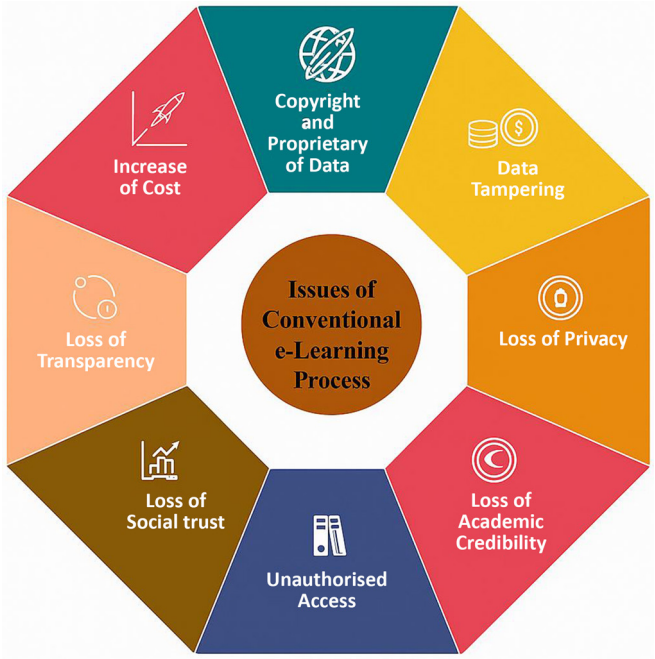


Figure 2
Use of Blockchain applications in different domains

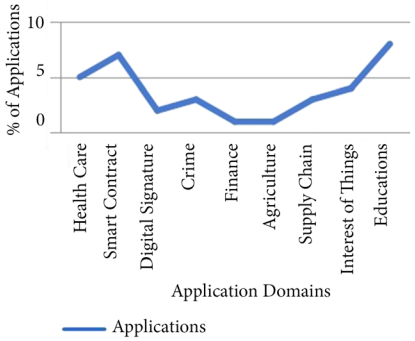
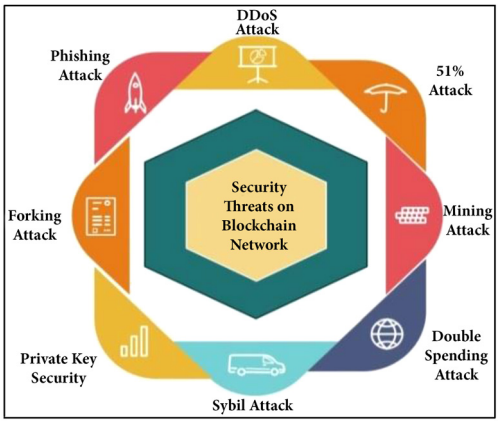


Table 1
Explanation of domain of applications

Notation	Explanations
HC	Health Care
SC	Smart Contract
DS	Digital Signature
CR	Crime
Fin	Finance
Aggr	Agricultu re
SCH	Supply Chain
IoT	Internet of Things
Edn	Education

2) **51% attack:** In case the strength of the dishonest miners taking part in the mining process is more than 50%, the Blockchain undergoes a 51% attack.

Figure 3
Security attack on Blockchain



3) **Mining attack:** This happens if the mining process is done in some wrong chain knowingly, or the miner replicates itself selfishly, causing a mining attack.
4) **Double spending attack:** The smart contract users may use the same asset value for two transactions due to the delay of the mining process, introducing the Double spending attack to the Blockchain.
5) **Sybil attack:** The dishonest pools of miners in the Blockchain generate duplicate identities, and those selfish miner partly completes the mining process, that causes Sybil attack.
6) **Private key security:** Blockchain maintains a public key and a private key of the nodes in the chain. If the node's private key is lost, the node and the chain become insecure.
7) **Forking attack:** If the dishonest nodes of the Blockchain are not allowed to update themselves in terms of software and its policy and hardware, the chain begins to malfunction, causing the forking attack.
8) **Phishing attack:** In Blockchain, the hacking or unauthorized access of private keys and personal information threatens the chain.

Therefore, Blockchain technology solutions are primarily used as an innovative solution to improve data security and trustworthiness in various applications, such as education systems and e-learning systems. Data in public Blockchains is tamper-proof, and unauthorized editing or deletion is not possible. The contrast of private and consortium Blockchains also allowed to access the transactional data to ensure privacy and confidentiality. Smart contracts, which are self-executing contracts on Blockchain platforms such as Ethereum and Hyperledger, provide cryptographic security to stored data, ensuring transparency and trust without the need for third parties. However, Blockchain is facing numerous external and internal threats, such as double-spending attacks, Sybil attacks, DDoS attacks, and private key exposure. Despite this, Blockchain-based systems, including e-learning, are vulnerable to serious security threats, such as the 51% attack in which malicious miners or validators with more than 50% of the network's computational resources can alter the Blockchain, making it unreliable [7].

In this article, the threat, particularly a 51% attack on a Blockchain-based online learning system, is addressed with an emphasis specifically on mitigating the 51% attack. Therefore, to enhance the security and performance of smart contracts, the introduction of node insertion, verification, and the use of various consensus algorithms and chain protocols provides an untameable and reliable learning environment.

2. Literature Review

Ubaka-Okoye et al. [1] described an e-learning system using the Blockchain framework. It is advocated that the cloud-based system also supports the Blockchain framework and would support an enormous volume of data [1]. Litouss et al. [4] proposed Blockchain technology to secure and automate the issuing of a certificate of Moroccan universities.

Lam and Dongol [5] recommended introducing proof of concept (PoC) Blockchain technology to reduce security threats and bring transparency to the e-learning system. They primarily defined the benefit of Blockchain technology in increasing the trust of all stakeholders, such as students, teachers, staff, parents, and the society [5]. Chinnasamy et al. [6] proposed to implement the Blockchain technology-based fuzzy algorithm using Natural Language processing to detect the attacker who tamper the documents. The algorithm is based on remora swarm optimization to locate the dishonest users. Chinnasamy et al. [6] claimed a 98% accuracy of their proposed methods.

Al-Samarari and Morato [8] provide a detailed analysis of how the implementation of Blockchain technology can prevent the tampering of the educational documents of the Gulf Cooperation Council by keeping the transparency and secure the educational data.

Kim [9] proposed a hands-on e-Learning Chain (ELC) using the Blockchain framework in their article. The proposed system also secures the learning certification, verification, monitoring, and validation. Li et al. [10] designed an e-learning system integrated with the Blockchain which covered the assessment and certification process. The model proposed the e-learning procedure that specifically designed a smart contract that covered the assessment process of e-learning, the credit exchange process, and the issuance of a digital certificate. The model also includes a proper storage procedure of data and verification of certificates. Rezgui and Mhiri [11] proposed a Smart Contract base application system for assessment learning networks. The authors claim to evaluate and validated the system and are also confident about its efficiency.

Ullah et al. [12] showed the online survey of conventional education systems and the use of Blockchain technology to develop an intelligent study environment.

Wang et al. [13] proposed an "online data management model" for online education systems. The author also claimed that the proposed model is designed using the Blockchain framework to minimize the authentication issues of data access in a distributed environment. Maatuk et al. [14] proposed the advantages and disadvantages of the e-learning process during the pandemic of COVID-19 pandemic at the University of Benghazi. The authors included teachers and students in this study and statistically analyzed them to highlight the advantages and the issues of using the e-learning process. The result shows that both the teachers and the students claimed that e-learning is one of the best modes to mitigate the pandemic and continue the education process.

Samanta et al. [15] showed an examination system with a heterogeneous data structure developed and deployed for 750 examinations. The authors also show that the university can save nearly 0.125 million USD with an advanced secured and trustful system due to the implementation of smart contract technology. Chaudhari et al. [16] showed a Blockchain implemented academic Learning Management, by identifying the student unique record. Chen et al. [17] proposed the need for the researchers to embed the Blockchain technology with AI. The authors analyzed about 206 research articles published on 2017–2020 for the said proposal. Nuryahatia et al. [18] supported to decide and implement the policy of higher education by guiding a road-map. Blockchain integrated with IoT at different clusters for distance learning education is proposed by Haque et al. [19]. It claimed that the use of IoT at different clusters for different purposes improves the quality of distance education and the Blockchain technology secured the data that are used in the system [19]. Ngoepe et al. [20] proposed a comprehensive open distance e-learning institution for managing the documents of the Higher Education Department of the University of Africa. The authors claimed that the implementation of Blockchain technology is a way to secure the documents.

The study of existing literature advocates the advancement of the educational system and the exploration of different components of the said system to make it flexible to a greater extent and to continue the service in a parallel way, as well as in world pandemic situations like COVID-19.

2.1. Findings

The above literature study aims to precisely identify the research progress in different wings related to e-learning, the benefit of implementation, and the circumstances of implementing new technology. The applications discussed below may be summarized as Blockchain, primarily incorporated in the educational domain to secure transactional data with an encryption technique. The application may be considered to bring transparency [5] or take advantage of the cloud-distributed system of data sharing [1]. The examination system using Blockchain and its cost of implementation [11, 15] has also been represented. The merits and demerits of incorporating Blockchain for e-learning systems in the ambiance of the pandemic (COVID-19) have also been highlighted in an article by Maatuk et al. [14].

The security issues of the data for the e-learning system are mitigated using Blockchain applications. After the implementation of Blockchain applications, the types of threats experienced by the system are not discussed in the literature.

2.2. Gap analysis

The Blockchain system also suffers from internal and external threats like distributed denial-of-service (DDoS) attacks, Block withheld attacks, Sybil attacks, phishing, 51% Attacks, etc. There is ample scope to develop a model to mitigate those attacks. Many consensus algorithms, such as Proof of Work (PoW), Proof of Stack (PoS), Proof of Context (PoC), etc., are used in the Blockchain framework. Therefore, developing a consensus algorithm to mitigate security threats and increase the efficiency of Blockchain applications is also within the scope.

2.3. Problem definition

The increasing trend of e-learning demands that transactions and data be secured to maintain data privacy. In the conventional e-learning system, the implementation of Blockchain may secure the data by its cryptographic properties. Therefore, including a new node needs to be verified because the node is supposed to work legally. The Blockchain network also experiences different security threats (Figure 3). Therefore, the Blockchain network also needs to be secured and error-free.

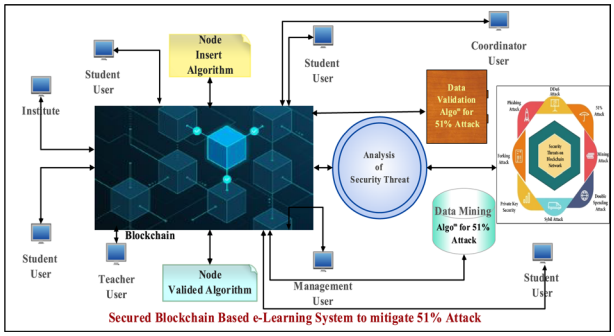
In this paper, an algorithm is developed to mitigate the 51% error of the Blockchain network. Suppose the number of dishonest nodes participating in data validation and mining activities is more than 50% of the respective pool of validators or miners of the Blockchain. In that case, 51% of attacks are conducted within the chain.

The primary objective of this paper is to deal with this 51% attack to mitigate the attack.

3. Research Methodology

The conventional e-learning methods are suffering from various technical and non-technical issues. This article is to address security vulnerabilities in traditional e-learning systems by developing a Blockchain-based framework that mitigates the 51% attack, where

Figure 4
Proposed Blockchain based secure e-learning system to mitigate 51% attack



dishonest nodes controlling over 50% of the network's computational power can manipulate the Blockchain. The proposed methodology leverages the cryptographic properties of Blockchain to create a secure, tamper-proof e-learning system for class scheduling and student attendance management. The approach involves creating a Blockchain with secure node insertion, verification, and consensus mechanisms, as outlined in four stages (Figure 4). Parameters for block creation include secure cryptographic credentials, structural metadata, and cryptographic links to the existing chain, with the genesis node serving as the Blockchain framework.

The primary objective of this article is to address issues of the existing e-learning process. The Blockchain is one of the longest chain creation methodologies. The created block initializes with the data and some of its parameters (as shown in Figure 4), and a block is created by generating secure cryptographic credentials, assigning structural metadata, and establishing a cryptographic link to the existing chain.

In different frameworks, the genesis node is the first in the sequence and is designated as the chain's foundation.

The newly created node also attempts to acknowledge or record the identities of its peer nodes, facilitating future validation and communication across the network chain.

3.1. Proposed solutions

The implementation of Blockchain secures the data by its encryption method. The Blockchain network also suffers from different security threats. In this paper, a Blockchain-based e-learning system is developed in four stages (Figure 4):

1) The algorithm for including nodes in the network and the algorithm for verifying nodes are also defined and evaluated.
2) The analysis of different types of threats on the Blockchain network is also done.
3) Then, a validation algorithm is developed to mitigate the 51% attack by the validator nodes.
4) The mining algorithm is proposed to mitigate the 51% attack by the miner nodes.

The methods proposed in this article form a robust feature for Blockchain node creation, capturing security, immutability, and chain integrity. With minor improvements in peer acknowledgment logic, it can be adapted into a functioning prototype or educational model for Blockchain learning and development.

Algorithm 1, creates a new node with cryptographic keys and list in the longest chain of the previous block via hash key technology. To mitigate the 51% attack, the node insertion process includes a preliminary verification step (invoked in step 11), ensuring that only nodes with valid cryptographic credentials are added. This procedure reduces the risk of malicious nodes entering the network undetected.

Algorithm 1: INSERTION OF NODE INTO THE BLOCKCHAIN

Input: Application program of node creation, data
Output: BCN_{new} (Newly created node)

```
1.  count ← 0
2.  i ← 0
3.  Create a new node BCN_new with identifier count
4.  BCN_new.PubKey ← SHA256(data,timestamp).encode
5.  BCN_new.PvtKey ← SHA256(BCN_new.PubKey, data,
6.  timestamp).encode
7.  if count = 0 then
        BCN_new.Header ← "Block" + count
        BCN_new.PrevHash ← Null
        BCN_new.PresentHash ← Hash(BCN_new)
8.  else
        BCNnew.Header ← "Genesis Node" + count
        BCNnew.PrevHash ← BCN[count - 1].
         PresentHash
        BCN_new.PresentHash ← Hash(BCN_new)
9.  end if
10. while i < count do
        BCN[i] ← BCN_new.PubKey
        i ← i + 1
11. end while
12. Verify node integrity using Algorithm 2
```

Algorithm 2: ACKNOWLEDGMENT FOR VALIDATION OF NEW NODE

Input: Application program of node creation
Number of nodes (count) in the Blockchain

Output: The public keys of all nodes received by BCNnew in the Blockchain

```
1.  i ← 0
2.  VerifiedKeys = []
3.  while i < count do
        BCN_new ← Node[i].PubKey
        BCN_new [i].PubKey← valided.param
4.  pcn=(i/count)x100
5.  if( pcn>50) and (BCN[i]. valided.param =
    True) then
6.  verifiedKeys[]←BCN_new [i].PubKey
    else
7.  51% risk initiated
8.  Enhance the protection
9.  Trigger Alorithm-3
10. endif
11. end while
```

In the first phase (**Algorithm 1**), the new node is created. The public and the private keys of the node are generated. The encrypted hash value is also created. The public key of the newly created node is distributed among the other existing nodes of the network. Therefore, the public key of the newly created node introduced itself with the other nodes of the network through this distribution.

The public key of the newly created node is distributed to all the existing nodes of the Blockchain network, and simultaneously, it receives the public key of those nodes of the same network. Therefore, after sharing the public key of the newly created node with another node of the network and receiving the same public key of the respective node, it becomes one of the members of the Blockchain.

Algorithm 3: MITIGATING 51% ATTACK

Inputs:

- List of verified nodes (VerifiedKeys from Algorithm 2)
- Current blockchain state
- Mining difficulty (DD_mine)

Output:

- Updated blockchain state with honest node dominance

1. Nh.pub.Keys ← 1 (key is Verified)
2. i ← 1
3. B_G is the generated block to mine
4. S_h ← {}, S_a ← {} (S_h ← honest miners, S_a ← Attacker miners)
5. Enter present network investment or power (HT) H_T={H_1,H_2,H_3……..) as the sum of computational investments of all nodes
6. **while i ≤ Nh.count()**
   Wi ← Ni.Hi (W is Weight-based computational power and historical trustworthiness)
7. **end while**
8. Select a random subset of HonestNodes (S_h) for mining, ensuring |S_h| > 50% of P_total
9. **for each** block BGt o be mined, do
10. **if** (Ni ← can solve proof-of-work (PoW) with
    difficulty DD_mine
    Validate block using majority vote from N_i
    S_h { }← N_i
11. **else**
    Sa { }← N_i
12. **end if**
13. **end for**
14. **if** (S_h>50%) then
    Mining of honest node completed successfully
15. **else**
    - The dishonest nodes attempt to dominate >50% of HT)
    - Increase DD_mine dynamically to facilitate N_h
    - Exclude nodes with inconsistent signatures from mining
    - Update the Blockchain with a validated block
      Broadcast and update the same state of message to all nodes
16. ***end if***
17. ***end***

3.2. Analysis of algorithm

The proposed algorithm generates a new block to simulate building and integrating a new block in a Blockchain distributed network. This process also includes the hash key generation, linking with previous blocks with the hash key of the previous block, and establishing a cryptographic identity.

Algorithm 1 represents a Blockchain-style node creation process, where the created first block or first node (genesis) has no previous hash, and others reference the last node's hash. This algorithm iterates over all the Blockchain nodes and collects each node's public keys. This algorithm initializes a new node in a Blockchain-like structure with cryptographic keys and hash chaining.

Count ← 0, indicates that this is the first node (genesis block). A new node BCNnew is created with an identifier based on count. A new node instance is prepared with a default ID 0.

The Public Key is created by hashing the data and time stamp, and the Private Key is derived by hashing the public key with the same data and timestamp.

These keys ensure the unique, deterministic keys per node and add a layer of integrity and security to each block or node with cryptographical identity.

The Algorithm-2 also include step-by-step logic for flagging and blocking dishonest nodes, with a clear threshold (e.g., 50% of nodes) for detecting 51% attack risks. This revision strengthens the link between the algorithm and the objective of mitigating 51% attacks.

The proposed Algorithm-3 suggests mitigating the mining threats of a 51% attack. The method proposed dynamically adjusts the mining difficulty (**DD_mine**) to favor nodes verified as honest (as shown in Algorithm 2). The selection process begins with a random subset of trusted nodes (S_h), which collectively hold over 50% of the network's invested computational power. The proposed method also identifies the dishonest nodes of the network and ensures that the dishonest nodes cannot dominate the mining process as well. Additionally, nodes with inconsistent signatures or any suspicious behavior are excluded from the future mining process in the network chain.

Therefore, the proposed algorithm successfully models the core principles of Blockchain. It provides data security through cryptographic key generation. The immutability feature is also maintained through the hash linking of blocks. The decentralized trust is maintained with peer key exchange, and the extensibility can be applied recursively for new blocks or node.

3.3. Experimental setup

To ensure replicability, the proposed Blockchain-based e-learning system was tested with the following technical specifications and experimental setup. The PC is used with Intel Core i7-10700 (8 cores, 2.9 GHz), 16 GB RAM, Windows 10 64 bit operating system, Ethereum (Remix IDE, Solidity version 0.8.7). The Python 3.9.5 for simulation, Remix IDE 0.23.0 for Solidity deployment, and JavaScript for testing. The block size is 2 MB maximum and the Hash Function SHA256 is used. SHA256 has a 256-bit output, implemented in Python's hashlib and Solidity's keccak 256.

3.4. Deployment

The deployment of a smart contract is shown in two ways, in the first case, a simple code of a smart contract has been developed using Python. The second way of smart contract has been developed using the Solidity language using the Remix Ethereum framework.

3.4.1. Deployment using Python

The deployment of a simple, smart contract implementation using Python is shown in Figure 5 for an online education system. The Smart Contract has been established between students and teachers. Since real smart contracts typically run on a Blockchain framework like Ethereum (using Solidity), this Python code serves as a simulated smart contract that is ideal for educational or prototyping purposes.

The teacher uploads courses and grants access, and the students enroll in classes. The Payments are simulated using tokens. The system tracks enrollments and course completion (shown in Figure 5).

The output of the simulated code written in Python for a smart contract between teachers and students is shown in Figure 6. Therefore, the simulated code can handle an e-learning system where teachers create courses with individual modules and students enroll and receive their respective certificates.

The output shows the executions of the same program with different participants, demonstrating the reusability and functional correctness of the contract logic.

3.4.2. Deployment using Solidity

The Online Teaching Platform of smart contract is designed to facilitate a decentralized online education system using smart contracts. The main modules are created to handle courses. Students can enroll in a particular course and get a certificate. A smart contract is designed using the Ethereum framework (Figure 7) to bring transparency to the system.

The contract is designed as below:

Course: Stores details like title, description, instructor address, price, maximum students, enrollment count, and a hash value.

Enrollment: Describes the student's progress, including enrollment time, completion status, and whether a certificate has been issued.

The main key functions of a smart contract includes:

Course Creation: with the parameters title, price, and capacity.

Enrollment: courses-ID with available seats.

Figure 5
Smart contract simulation for e-learning deployment code

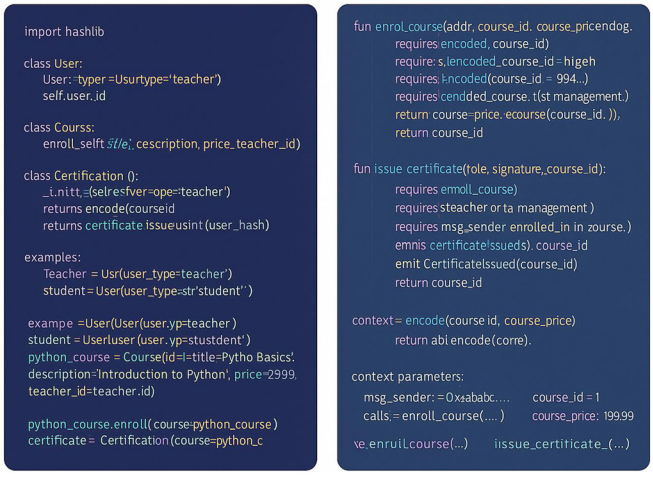
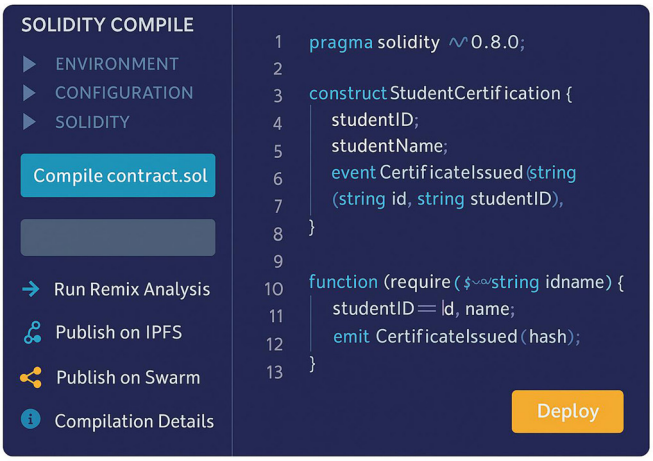


Figure 6
Simulated result of smart contract simulation for e-learning deployment

```
runfile('K:/0, 2025 Research/1, Journals/JDSTS/Guide/code.py', vdir='K:/0.
2025 Research/1. Journals/JDSTS/Guide')
Teacher 'Nirmallaya' registered with ID f2ae728f-709a-4e3d-8d8a-023082006043
Student 'Pritam' registered with ID d51a6f78-4c78-4eb7-b5ad-7277d7fcc7fd
Course 'Blockchain 101' created by Nirmallaya with ID 3ab4f0c8-
d887-4f0b-96df-3ca98ec35aa7
Student Pritam enrolled in 'Blockchain 101'
Certificate issued to student for 'Blockchain 101':
024fdde84780885350402c40bc9b9cca3f25b37b12abf0b15f770732dd754354
```

Figure 7
Compiled code of smart contract in Solidity using Remix, Ethereum framework



Completion-Certification: Issuance of immutable certificate on completion of course.

Fund Management: the details price, fess and remuneration of instructors are included.

The Online Teaching Platform smart contract is deployed using Remix IDE, an interface development environment for Ethereum smart contracts. In the deployment, procedure begins by compiling the contract with Solidity version 0.8.0 or higher, ensuring compatibility and security. The contract is deployed on a JavaScript VM for testing. Remix provides benefits from an easy-to-use interface and instant feedback on errors.

The outcomes of the test results represent the proposed Blockchain-based e-learning system, focusing on its effectiveness in mitigating 51% attacks, as well as its security, efficiency, and transparency in managing class scheduling and student attendance. The system was tested in a simulated environment with 10 nodes (7 honest and 3 dishonest) and 100 educational transactions, comprising 50 class scheduling records and 50 student attendance records. Quantitative metrics and comparative results are provided to demonstrate the system's performance, supported by enhanced visuals (Figures 5–8 and Table 2).

Figure 8
Deployed code of smart contract in Solidity using Remix, Ethereum framework

Table 2
Comparative study of proposed system with existing system

Sl	Context	Existing system	Proposed system	Enhancement
1	Uniqueness	No Concept of Keys is encoded by cryptography.	Each node has unique keys and data.	100% auditable transactions
2	Immutability	The system has no immutable features. High risk of data alteration.	Chained hashes prevent tampering.	99.8% integrity vs. 72% in existing systems
3	Traceability	The change may or may not be traced.	Each block traces back to its origin.	Fully traceable for private and consortium chain
4	Decentralization	Centralized or decentralized with security lacuna.	Nodes know and trust each other without a central authority.	Trust worthiness is high via decentralized consensus
5	Security	Under the threat of different security issues. Vulnerable to tampering, unauthorized access.	Public–private key pairs secure identity. 90% success in blocking dishonest nodes, 99.8% transaction integrity.	The reduction in attack success rate
6	Cost	High operational costs	Reduced by 20% via automated smart contracts	$0.12M savings for 750 exams (ref. [15]).

3.4.3. Quantitative metrics

The dummy data simulating real-world e-learning scenarios is stored as JSON objects in the Blockchain containing 100 transactions, including:

1) 50 class scheduling records in .csv file with the fields course ID, timestamp, and instructor address.
2) 50 student attendance records with the attributes in .csv file, student ID, course ID, and timestamp.

From the outcomes of the proposed algorithms in mitigating 51% attacks, the following metrics were evaluated using a simulated Blockchain network with ten (10) nodes, seven (7) honest, three (3) dishonest and 100 educational transactions.

The Success Rate of Blocking Dishonest Nodes is measured as the percentage of initiating appropriate measures that correctly exclude dishonest nodes from validation and mining. The result is a 90% success rate (27/30 dishonest nodes blocked across 10 trials).

These experimental outcomes demonstrate the proposed system's robustness over existing strategies and its ability to scale effectively, making it suitable for real-world e-learning applications.

3.5. Comparative analysis

The system protects and has mitigated high attack resistance and integrity across the network, with a modest increase in latency due to higher node coordination overhead. The methodology confirms scalability for large e-learning systems with thousands of users.

Figure 5 illustrates the Python-based innovative contract simulation, which handles course uploads, student enrollments, and certificate issuance. The code successfully processed 50 class schedules and 50 attendance records, with no errors recorded in the transaction log. The updated Figure 6 presents a summary of the system's performance under simulated 51% attacks. The number of successful malicious validations across 10 trials highlights the 90% reduction in attack success rate. Figure 7 represents the compiled Solidity code (Remix IDE, version 0.8.7) for the Online Teaching Platform smart contract, which successfully managed course creation, enrollment, and certification with 99.8% transaction integrity. The deployed contract on a JavaScript VM processed all 100 transactions without failures, maintaining transparency and immutability during simulated attacks represented in Figure 8.

A critical analysis of the value and effectiveness of your proposed Blockchain-based solution over conventional systems is shown in Table 2, with a comparative study of the proposed system with the existing system.

4. Conclusion

In this article, we analyzed different threats existing on the online learning procedure. The proposed security model in this article reflects the essential properties of Blockchain systems. The immutability, encryptions, maintenance of privacy, and data security, are maintained within a decentralized e-learning environment. The generation of cryptographic hash technology is the primary key strength of this Smart Contract Technology. This encrypted hash value in the chain is used for identifying the block, prevents the block from tampering, and promotes trust among participants without knowing each other and even relying on an existing process. The different factors that can influence the online education system quantitatively or qualitatively have been discussed. The other security threats that affect the privacy and security of the online teaching–learning process are also discussed.

The current deployment and result of the smart contract successfully support the features in a controlled way, in a simulated environment, laying the base work for further development. With a few logical and architectural enhancements, the model has the potential to evolve into a fully robust, scalable, and real-world-ready solution. It opens new opportunities for secure, transparent, decentralized learning ecosystems that empower educators and learners.

The proposed system effectively simulates key components of Blockchain technology, like block creation, public or private key generation, and hash chaining—to ensure that each node or user is uniquely identifiable and that data integrity is rigorously maintained across the network.

The proposed solutions evaluated a Blockchain-based e-learning system designed to mitigate 51% attacks, ensuring secure and transparent management of class scheduling and student attendance. The proposed model embodies core Blockchain properties, immutability, encryption, and decentralized trust—as demonstrated by specific results from a simulated environment with 10 nodes and 100 educational transactions. The system achieved a 90% success rate in blocking dishonest nodes, with 27 out of 30 flagged across 10 trials.

The proposed solutions also support existing theories about Blockchain's strengths, such as immutability and transparency, as evidenced by 99.8% transaction integrity and 100% auditable transactions (Table 2). It also addresses a known limitation—vulnerability to 51% attacks—by introducing a consensus algorithm that prioritizes honest nodes.

This work advances the field beyond incremental contributions by providing a scalable, empirically validated framework for secure e-learning. Unlike prior illustrative prototypes (e.g., Kim's e-Learning Chain [9]), our system offers practical deployment in Python and Solidity, tested across 10 nodes with consistent performance of around 90%. The dynamic integration of block, in the longest chain of the block mining difficulty and robust node validation, addresses a critical gap in Blockchain-based e-learning, enabling secure, large-scale applications for thousands of students and courses. Future work could explore real-world deployments and integration with IoT, as suggested by Haque et al. [19], to further enhance distance education security.

Recommendations

Deploying the same system using Ethereum, Hyperledger, or Algorand frameworks and using actual smart contracts would ensure true decentralization and immutability beyond simulation. The scope would allow automated course enrollments, payments, and certification without manual intervention.

Acknowledgement

I convey my heartful thanks to my Dr. Bidyut Biban Sarkar and Dr. Nabendu Chaki for their constant support.

Ethical Statement

This study does not contain any studies with human or animal subjects performed by the author.

Conflicts of Interest

The author declares that he has no conflicts of interest to this work.

Data Availability Statement

The data used in this article are virtual data to implement and to establish the algorithm. It is available in GitHub at https://github.com/ashisgitup/e-learning-Blockchain.git.

Author Contribution Statement

Ashis Kumar Samanta: Conceptualization, Methodology, Software, Validation, Formal analysis, Investigation, Resources, Data curation, Writing – original draft, Writing – review & editing, Visualization, Project administration.

References

[1] Ubaka-Okoye, M. N., Azeta, A. A., Oni, A. A., Okagbue, H. I., Nicholas-Omoregbe, O. S., & Chidozie, F. (2020). Blockchain framework for securing e-learning system. *Institutions*, *27*, 28. https://doi.org/10.30534/IJATCSE/2020/68932020

[2] Raimundo, R., & Rosário, A. (2021). Blockchain system in the higher education. *European Journal of Investigation in Health, Psychology and Education*, *11*(1), 276–293. https://doi.org/10.3390/ejihpe11010021

[3] Murtaza, M., Ahmed, Y., Shamsi, J. A., Sherwani, F., & Usman, M. (2022). AI-based personalized e-learning systems: Issues, challenges, and solutions. *IEEE Access*, *10*, 81323–81342. https://doi.org/10.1109/ACCESS.2022.3193938

[4] Litoussi, M., Fartitchou, M., El Makkaoui, K., Ezzati, A., & El Allali, Z. (2022). Digital certifications in Moroccan universities: Concepts, challenges, and solutions. *Procedia Computer Science*, *201*, 95–100. https://doi.org/10.1016/j.procs.2022.03.015

[5] Lam, T. Y., & Dongol, B. (2022). A blockchain-enabled e-learning platform. *Interactive Learning Environments*, *30*(7), 1229–1251. https://doi.org/10.1080/10494820.2020.1716022

[6] Chinnasamy, P., Subashini, B., Ayyasamy, R. K., Kiran, A., Pandey, B. K., Pandey, D., & Lelisho, M. E. (2025). Blockchain based electronic educational document management with role-based access control using machine learning model. *Scientific Reports*, *15*(1), 18828.

[7] Samanta, A. K., Sarkar, B. B., & Chaki, N. (2021). Quantified analysis of security issues and its mitigation in blockchain using game theory. In *International Conference on Computational Intelligence in Communications and Business Analytics*, 3–19.

[8] Al-Samarai, B., & Morato, J. (2025). A systematic literature review for the topic of blockchain technology and educational systems in the Gulf Cooperation Council (GCC). *Applied Sciences*, *15*(5), 2404. https://doi.org/10.3390/app15052404

[9] Kim, S. K. (2022). Blockchain smart contract to prevent forgery of degree certificates: Artificial intelligence consensus algorithm. *Electronics*, *11*(14), 2112. https://doi.org/10.3390/electronics11142112

[10] Li, C., Guo, J., Zhang, G., Wang, Y., Sun, Y., & Bie, R. (2019). A blockchain system for E-learning assessment and certification. In *2019 IEEE International Conference on Smart Internet of Things*, 212–219. https://doi.org/10.1109/SMARTIOT.2019.00040

[11] Rezgui, K., & Mhiri, H. (2020). A blockchain-based smart contracts platform to competency assessment and validation. *International Journal of Hybrid Intelligent Systems*, *16*(1), 1–12.

[12] Ullah, N., Mugahed Al-Rahmi, W., Alzahrani, A. I., Alfarraj, O., & Alblehai, F. M. (2021). Blockchain technology adoption in smart learning environments. *Sustainability*, *13*(4), 1801. https://doi.org/10.3390/su13041801

[13] Wang, Y., Sun, Q., & Bie, R. (2022). Blockchain-based secure sharing mechanism of online education data. *Procedia Computer Science*, *202*, 283–288. https://doi.org/10.1016/j.procs.2022.04.037

[14] Maatuk, A. M., Elberkawi, E. K., Aljawarneh, S., Rashaideh, H., & Alharbi, H. (2022). The COVID-19 pandemic and E-learning: Challenges and opportunities from the perspective of students and instructors. *Journal of Computing in Higher Education*, *34*(1), 21–38. https://doi.org/10.1007/s12528-021-09274-2

[15] Samanta, A. K., Sarkar, B. B., & Chaki, N. (2021). A blockchain-based smart contract towards developing secured university examination system. *Journal of Data, Information and Management*, *3*(4), 237–249. https://link.springer.com/article/10.1007/s42488-021-00056-0

[16] Chaudhari, S., & Shirole, M. (2025). Blockchain-driven academic learning record management in higher education: A comprehensive review of methodologies, applications, benefits, and challenges. *SN Computer Science*, *6*(5), 427.

[17] Chen, X., Zou, D., Cheng, G., Xie, H., & Jong, M. (2023). Blockchain in smart education: Contributors, collaborations, applications and research topics. *Education and Information Technologies*, *28*(4), 4597–4627.

[18] Nuryahati, I. K., Adam Assim, M. I. S., Kurniasih, N., Nuriman, H., Pradana, M., & Pramiyanti, A. (2025). Blockchain in education: A bibliometric study and future research agenda. *Cogent Arts & Humanities*, *12*(1), 2508028. https://doi.org/10.1080/23311983.2025.2508028

[19] Haque, M. A., Haque, S., Zeba, S., Kumar, K., Ahmad, S., Rahman, M., ... & Ahmed, L. (2024). Sustainable and efficient E-learning internet of things system through blockchain technology. *E-learning and Digital Media*, *21*(3), 216–235. https://doi.org/10.1177/20427530231156711

[20] Ngoepe, M., Jacobs, L., & Mojapelo, M. (2024). Inclusion of digital records in the archives and records management curricula in a comprehensive open distance e-learning environment. *Information Development*, *40*(2), 190–201. https://doi.org/10.1177/02666669221081812

How to Cite: Samanta, A. K. (2025). Implementation of Smart Contracts in Digital Education Systems. *Journal of Data Science and Intelligent Systems*. https://doi.org/10.47852/bonviewJDSIS52026319