DOI: https://doi.org/10.36094/sc.v89.2023.An_Efficient_E-certificate_Management_System.Mondal.120

ARTICLE

Sci. and Cult. 89 (3–4) : 120-124 (2023)

AN EFFICIENT E-CERTIFICATE MANAGEMENT SYSTEM IN E-LEARNING USING BLOCKCHAIN

SOUMEN MONDAL*, ANIRBAN PANJA** AND SUNIL KARFORMA***

Blockchain is a cutting-edge information technology that allows users to create ever-growing lists of data sequences. Individual higher education organizations or groupings of educational institutions can use blockchain in their automated management systems. Because there is no efficient anti-forge system in place, occurrences that result in the falsification of academic credentials are frequently recognized. The digital certificate system based on blockchain technology will be offered to overcome the problem of certificate counterfeiting.

Introduction

If we go to any educational website, we'll see that one of the most essential topics is the number of certificate courses that will be available online. It's uncertain if this move will be permanent, but it wouldn't be unreasonable to expect a growing percentage of courses to be taught online in the future. Huge volumes of data on institutions and individuals are being stored and transferred digitally via a variety of networks in this industry. As a result, threats from hackers and other unethical actors are all too common. Many educational organizations continue to provide certificate programs, training opportunities, and even whole academic degrees in a virtual format, either on their own or in cooperation with training partners. As part of the academic training process, a substantial amount of personal information is sent between the individual, the educational organization, and several third-party vendors. The possibility of this data being compromised is not insignificant. Blockchain is a cutting-edge technology that combines information security with the capacity to distribute certificates and study materials among a large network of counter parties in a purely digital manner, securing and protecting this new model of online education. It is now more vital than ever for everyone (online educators, online education institutions, and private sector blockchain firms) to enhance the educational process and product to increase the quality of education and services.

* Research Scholar, Department of Computer Science, The University of Burdwan, West Bengal-713104, India.
e-mail: mailtosoumenmondal@gmail.com

** Research Scholar, Department of Computer Science, The University of Burdwan, West Bengal-713104, India.
e-mail: anirbanpanja192@gmail.com

*** Professor, Department of Computer Science, The University of Burdwan, West Bengal-713104, India.
e-mail: sunilkarforma@yahoo.com

Introduction to Blockchain

The concept of blockchain was first introduced by Satoshi Nakamoto in his thesis, "Bitcoin: A Peer-to-Peer Electronic Cash System," in 2008[1]. The phrases 'block' and 'chain' refers to the data structure used to enter data into the ledger. A 'block' is a unit of data storage, whereas a 'chain' is a chronological string of blocks ordered using cryptographic hash algorithms. As blockchain follows the Distributed Ledger Technology (DLT) which makes the transaction history of any digital asset tamperproof and transparent due to the property of decentralization and cryptographic hashing. Blockchain technology is implemented using three basic concepts: transaction or data in hash form, mining the block into the chain, and smart contracts. The outcomes of all transaction data are added to a block when a specific amount of time has passed. After the validation of transactions, the block is appended into the chain known as mining. The node

(miner node) that adds the block to the chain is selected by solving some mathematical puzzle known as a consensus algorithm. The chain is a chronological string of blocks that are connected using some cryptographic hash method. Blockchain technology becomes more popular because of its core properties. First, the distributed ledger in the network only allows the addition of new blocks such that once the data is stored in a block it cannot be deleted or altered by anyone which ensures the immutable properties of a blockchain. Figure 1 depicts how the blocks are interconnected in a chain in chronological sequence, with the previous block's Hash value stored in the following block. To prevent data forgery, the elliptic curve-based digital signature (ECDSA) is attached with each transaction in a block. The block of transaction data is then added to the previous chain by solving some mathematical puzzle depending upon the blockchain type known as consensus algorithm and will be distributed across the network, making them indestructible as a result, blockchain technology features a dispersed, decentralized, and untrusted data storage structure. The dispersed and decentralized nature of the network is maintained via distributed data storage and communal network maintenance. Blockchain technology effectively decreases the probability of data loss over the whole network when compared to traditional centralized databases, consider it a single node attack.

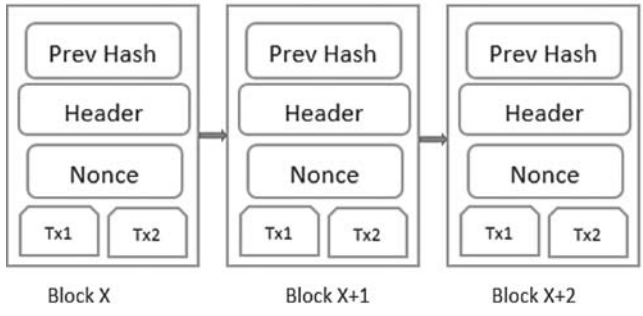

Fig. 1 Structure of a Blockchain

Blockchain technology is a great answer to the difficulties of online education because of its high trustworthiness and security. In particular, blockchain enables fair course credit certification by offering adequate and non-tamper-able academic records for online education without the help of any intermediary. Smart contracts can also increase the efficiency of course sharing in online education, while cryptographic-based data processing protects the user's privacy. As a consequence, incorporating blockchain technology into online education is a potential endeavor.

Types of Blockchain: Different types of blockchains are discussed as follows:

Public Blockchain: A public blockchain that is accessible to anybody with an internet connection. Anyone with an internet connection may become an authorized node and can join the network by signing up for a blockchain platform. There is no requirement for any special permission to join a public blockchain network. As a result, it's a permission-less, non-restrictive distributed ledger system. A public blockchain node or user has access to the whole blockchain data, may validate transactions, or may execute proof-of-work consensus for a newly created block, and can mine. The most basic use case for public blockchains is cryptocurrency mining and trade. As a result, Bitcoin and Ethereum are the most extensively utilized public blockchains. Public blockchains are usually safe if users adhere to security rules and standards. It is, however, only harmful when the participants do not follow the security guidelines.

Private Blockchain: This type of blockchain, called permissioned blockchain, has some sort of limitations in which the network is controlled by a single company. This technique is often used within a corporation or organization where only a limited number of people are permitted to join a blockchain network. The organization can control the security, authorizations, permissions, and accessibility of the network. As a consequence, private blockchains provide the same functionality as public blockchains, but the network is comparatively smaller, more restricted, and not fully decentralized as public blockchain platforms. This type of blockchain network can be used in voting, supply chain management system, digital identity, asset ownership, and other applications for better security and efficiency.

Consortium Blockchain: A federated blockchain, sometimes called a consortium blockchain, is a semi-decentralized approach in which many organizations control the blockchain platform. It is not a public platform, but rather a permission one. The consortium blockchain combines the 'low-trust' paradigm of public blockchain with the single trusted entity' approach of private blockchain. Several companies can act as a node in this type of blockchain and can share information and mining processes[2]. Consortium blockchains are frequently used in the bank sector, government sector and other public sectors also[2].

Hybrid Blockchain: This type of blockchain inherits the properties of both private and public blockchains and transforms them into a hybrid blockchain. It combines the advantages of both private and public blockchains, making private and public permission-based systems possible. Users may decide what they want to achieve with a hybrid

network rather than having to adjust their ideas due to technological limits. Because of the hybrid blockchain system's versatility, users may easily combine a private blockchain with several public blockchains.

Distributed Ledger: A distributed ledger is the consensus of shared, copied, and synced digital data over a decentralized network. Transactions between network participants, such as the transaction of assets or data, are recorded in the distributed ledger. The network's participants control and agree on the modifications to the ledger's records by consensus. There is no involvement from a central authority or a third-party mediator, such as an agency or organization. Each digital asset in a distributed ledger has a timestamp and a unique cryptographic signature which makes it a fully verifiable and immutable record of all transactions [over the network.

Consensus Algorithm of Block-chain: A consensus algorithm is a mechanism for all peers in a blockchain network to agree on a common understanding of the distributed ledger's current state[3]. Consensus algorithms are used in this technique to give resiliency to blockchain networks and to develop trust among unknown peers in a distributed environment.

Now we'll look at a few different consensus methods and how they function.

Blockchain Consensus Algorithm: Proof of Work (PoW): Proof of Work (PoW) is a technique for generating a cryptographic hash. Cynthia Dwork and Moni Naor initially proposed the notion in 1993, and Satoshi Nakamoto reintroduced it in the Bitcoin whitepaper in 2008[1]. Proof of Work's origins in blockchain systems may be traced back to Adam Back's Hashcash, which was created as a solution to combat email spam and denial-of-service assaults.

Blockchain validators in a PoW system must go through a low-probability random process. Before a good proof of work can be created, a lot of trial and error is necessary. It takes data as an input from a block header and runs it through a cryptographic hash function to acquire the right nonce. To win the problem, PoW requires a lot of computational power.

Blockchain Consensus Algorithm: Proof of Stake (PoS): To address the inherent difficulties of PoW, the PoS consensus method was devised in 2011. Apart from their comparable operation, PoS and PoW have some key distinctions and properties, particularly when it comes to respecting the validation of newly created blocks on the specific blockchain network. This consensus method varies from the Proof of Work (PoW) mining consensus in that it uses a system to validate blocks based on the stake of network participants. Validations of the stake resources are in the form of digital money or tokens, rather than executing hash functions. Based on the amount of processing power allocated, the validator for each block is subsequently chosen at random from among the stakeholders.

A pseudo-random election method verifies a node's allocation and evaluates the party's commitment to ensure the network despite each PoS system may execute the algorithm differently. The Ethereum blockchain, the world's largest blockchain network in respect of developer activity, has started to shift from the PoW algorithm to the PoS algorithm to maximize the network scalability and the reduction of excessive power waste[4].

Smart Contract: Smart contracts are basic computer programs or transaction algorithms that execute when specified conditions are met and are recorded on a blockchain. They're frequently used to automate the contract implementation without the need for a centralized authority, legal system, or external enforcement mechanism[5]. They can also automate a workflow by triggering the next phase when specific conditions are satisfied. Smart contracts are composed of simple "if/when...then..." logic written in Solidity or other languages dependent on the framework and stored on a blockchain . The actions are performed by a network when the predefined conditions are satisfied. After completion of the transactions, the blockchain is updated. This implies that the transaction can't have been tampered and the results are only available to those who are allowed to see them. A developer can then create the smart contract, however, nowadays organizations that use blockchain for e-learning are increasingly offering templates, web interfaces, and other online tools to make smart contract creation easier[6].

The Way Blockchain can help to Improve the Security of E-learning Systems

In comparison to a standard e-learning system, the security and efficiency of the e-learning system can be further improved using blockchain technology in the following areas.

Verification of Student Details and Accreditation: Blockchain technology provides a new dimension for maintaining the academic records of student credentials of an educational institution. No intermediary is needed here to verify academic degrees, diplomas, and other academic testimonials. With blockchain technology, it will be considerably easier to verify the service and quality of education provided by most educational institutions.

Reduce Forgery: Fake academic degree credentials have been utilized by job candidates on several occasions. Due to geographical distance, the employer or interviewer may be unable to check the student's details to verify the applicant's skills. The online education industry is one of the most popular targets for scammers and hackers. Hackers might theoretically change and remove data from educational systems. For all academic qualifications, blockchain guarantees a consistent and transparent ledger. It's difficult to change student information once it's been recorded on an online ledger. To alter the data, we will need authorization from network users.

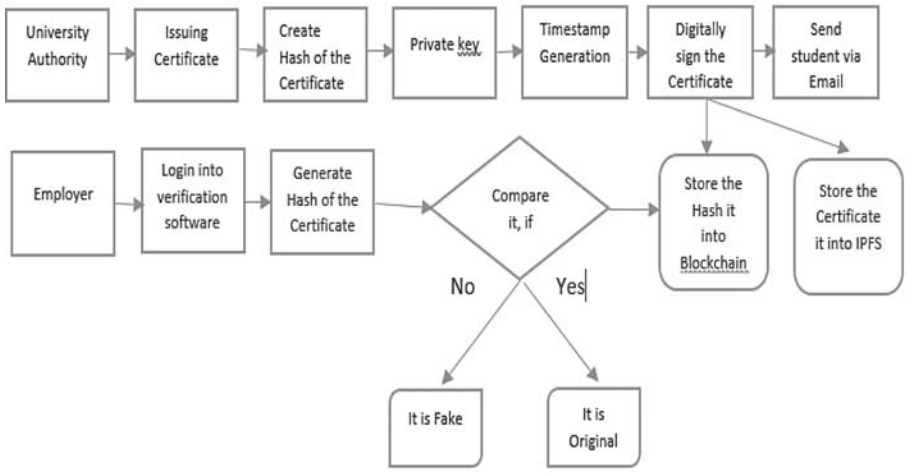

Fig. 2 Flow diagram

Distributed Learning System: Educational institutions may employ blockchain technology to provide distributed online learning. It enables real-time communication between students and teachers. Institutions will no longer be able to dictate the kind of programs that should be offered or the charges that should be paid for each online program once blockchain technology decentralizes online learning.

Prevents copyright and Digital Rights Violation of Study Materials: Plagiarism is a big issue that educational institutions are attempting to address. It may be quite costly for students to replicate digital information while writing a term paper or a research project. For example, a university may invalidate such students' credentials due to plagiarism. Content creators will have the capability to efficiently manage the spread of copyright educational materials on the internet using blockchain technology. All people will be able to keep academic information in a secure and safe chain using advanced encryption technology.

This guarantees that only authorized network users have access to the data. Owners of learning materials may keep track of who has accessed their digital content, authenticate who has accessed it and authorize users to use it.

Developing a Better Platform for Online Education: The development of improved online learning systems will be aided by blockchain technology. Universities and other educational institutions may collaborate with students and professors to create user-friendly education systems and a digital environment. Students from faraway regions can have access to and share study resources from reputable universities using the online education approach. They can also access educational services and download learning materials from a remote location. Learning becomes more convenient for everyone when students, teachers, and developers communicate quickly.

Proposed Model for Certificate Management Using Blockchain

It is not always possible to provide a hard paper certificate due to distant learning. Certificate fraud has become more common as a result of the availability of current, low-cost scanning and printing equipment. This jeopardizes the authenticity of the certificate holders and the university that issued it. It is necessary to confirm that the graduate's diploma is genuine and that the holder is the rightful owner. A graduation certificate must also be authenticated to ensure that the information on it is correct and that it comes from a trustworthy source. A significant amount of time will be spent either calling the university to authenticate a certificate or waiting for a response from the school to confirm that the certificate is legitimate and the information is proper to verify its legality. This treatment is time-consuming and expensive.

Users can keep important documents as digitally signed assets, such as academic certificates, using blockchain technology. These digitally signed documents ensure data protection and file exchange with companies or other authorities for recruiting or admittance. This groundbreaking technology development entails issuing authority to generate certificates that are then stored in a blockchain network with a digital signature[7]. When an employer needs information about a student for a job or an educational institution needs a student's past academic qualifications or papers, they may readily obtain it. The method suggested in this work is made up of two parts:

one is the issuing of a digitally signed academic certificate, and the other is certificate verification, which is linked to component veracity. Figure 2 depicts the whole design.

Digitally Signed Academic Certificate Issuance: The university administration is the first to offer a signed certificate digitally. The following approaches are used in this article to victimize the blockchain, as shown in Figure 2.

Generate Hash: It is a one-way cryptographic hash that generates a digest of a text, or data file based on a specific algorithm. SHA-256 is a 'one-way' mathematical function that takes variable size input and produces a fixed size (256-bit) output that cannot be inverted. As a result, comparing 'hashed' values of texts is beneficial over decrypting the text to obtain the original version. We construct a hash of the digital certificate and place it in the block to make the certificate temper proof. Data can't be tampered with since SHA-256 provides a nearly unique digest.

Digital Signature (ECDSA): The ECDSA (Elliptic Curve Digital Signature Algorithm) is an elliptic-curve-based cryptographically secure digital signature system (ECC). The mathematics of the elliptic curve is based on cyclic groups over finite fields. The ECDLP issues are the foundations of ECDSA (elliptic-curve discrete logarithm problem). The ECDSA sign and verify mechanism operates as follows. It works by multiplying EC points. ECDSA provides the same security level and generates small keys and signatures compared to RSA keys and signatures. The certificate issuing authority digitally signs the certificate which ensures the authenticity and the originality of the certificate. The verifier can verify the signature by using the public key provided by the institution.

Verification

JSON and pdf format of the documents are used to store the IPFS. The hash reference of the documents is saved as well as the pdf copy is uploaded to the InterPlanetary File System (IPFS). The JSON files are imported by Hyper ledger to generate an asset[8]. This is a peer-topeer distributed file system that helps to connect computer devices through a shared file system.

By using this IPFS system, the verifier can efficiently verify without any intermediary. The verifier receives the hash code from a student, through which the verifier can view the certificate. So without any doubt, the verifier can easily validate the ownership and the originality of the documents.

Conclusionn

In this study, a blockchain model for educational credential verification was presented as a way to enhance the verification process. As a result, the likelihood of certificate forgery will be minimized, while certificate secrecy, security, and validity will be enhanced. Our solution simplifies the process of producing certificates and reduces the amount of time it takes to validate them manually. More investigations based on diverse blockchain applications are being conducted in numerous fields these days. ❐

References

1. Satoshi Nakamoto, Cryptography Mailing list at https://metzdowd.com. (2009).
2. Ramakrishna Raju, Rohan Mital, Rohit Mital, 2019 IEEE/AIAA 38th Digital Avionics Systems Conference (DASC) (2019).
3. Z. Wang, J. Lin, Q. Cai, Q. Wang, J. Jing, and D. Zha, IEEE Transactions on Dependable and Secure Computing, 1–17 (2020).
4. Han Sun, Xiaoyue Wang, Xinge Wang, International Journal of Emerging Technologies in Learning (iJET) (2018).
5. M.A. Khan and K. Salah, *Future Generation Computer Systems*, **82**, 395–411 (2018).
6. M.B. Mohamad Noor and W.H. Hassan, *Computer Networks*, **148**, 283–294 (2019).
7. D. Li, Y. Jia, X. Gao, and N. Al-Nabhan, *Security and Communication Networks*, **2020**, Article ID 6679022, 12 pages (2020).
8. Blockchain based Internet of Things, Springer Science and Business Media LLC, (2022).