International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.557
e ISSN: 2584-2854
Volume: 02
Issue:12 December 2024
Page No: 3755-3759

Certificate Validation Using Blockchain

Mr. Achyutha Suresh Babu[1], Kanne Manusha[2], Mankal Nagasree[3], G Sairam[4]
[1]Associate Professor, Department of CSE, Institute of Aeronautical Engineering, Dundigal, Hyderabad, India.
[2,3,4]UG, Department of CSE, Institute of Aeronautical Engineering, Dundigal, Hyderabad, India.
Email ID: *a.sureshbabu@iare.ac.in[1], kannemanusha26@gmail.com[2], nagasreemankal@gmail.com[3], sairam2002g@gmail.com[4]*

Abstract
As education becomes more diversified, decentralized and democratized, we still need to maintain reputation, trust in certification and proof of learning. Nowadays everyone has to show his/her Document and Certificate to any other person for some purpose/job. After seeing the document, the 3rd person cannot validate the originality of the certificate. The same thing is applied for a land registry, PAN card, and Aadhar card verification. The increased focus on relevance and employability may also push us in this direction, as we also need more transparency. We can solve this problem or get trust by using blockchain technology. The digital currency Bitcoin is probably the best-known application of blockchain and is even better known than the Blockchain technology on which it is based [1]. The blockchain is a chain of blocks and blocks are immutable in a distributed environment, in which storage devices are not all connected to a common processor. It is a database of records/public ledger of all transactions/digital events that have been performed and information is shared within participating parties. Each entry in the system is verified by common consent of the participants in the system. Once information is entered in the blockchain it cannot be erased. It could provide a system that is transparent and secure. Blocks (Ordered Records) are added to the blockchain with timestamp and a link to a previous block. Verifying a diploma/certificate today takes a good amount of time and requires human resources or human resources to request confirmation of details from universities.

Keywords: *Decentralization; Blockchain; Certificate Validation; Transparency; Digital Currency; Security*

1. Introduction
Nowadays, education has become an essential part of life, still we need to maintain reputation and trust in certification. Everyone has to show his/her Document and Certificate to any other person for some purpose/job. After seeing the document, the 3rd person cannot validate the originality of the certificate. The Internet is entering the second era that's based on Blockchain [2] [3]- the Internet of Value, a new platform to change the world of business. It's a novel solution to the age-old human problem of trust. It provides architecture for so-called trust less trust. It allows users to trust the outputs of the system without trusting any actor within it. The pace with which this technology is evolving, it's making it difficult for different sectors/domains to keep, without the changes. The world is increasingly getting connected with the amalgamation of connected devices and solutions. So how do we fit in- For truly digitization process in Fintech / Banking and other sectors as well got to be seamless. "Blockchain technology" can be seen as a group of technologies, like a bag of bricks. From the bag, we can take out bricks and put them together in different ways to create different results [4-8].

1.1. Existing System
Cloud computing has emerged as a new enterprise IT architecture. However, privacy concern has remained a primary barrier preventing the adoption of cloud computing by a broader range of users/applications. When sensitive data is outsourced to the cloud, data owners naturally become concerned with the privacy of their data in the cloud and beyond. However, how the encrypted data can be effectively utilized then becomes another new challenge. Symmetric cryptography-based schemes are clearly not suitable for this setting due to the high complexity of secret key management. Although authorized keyword search can be realized in single-owner setting by explicitly defining a server-enforced user list that takes the responsibility to control legitimate users'

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.557
e ISSN: 2584-2854
Volume: 02
Issue:12 December 2024
Page No: 3755-3759

search capabilities, i.e. search can only be carried out by the server with the assistance of legitimate users' complementary keys on the user list, these schemes did not realize fine-grained owner-enforced search authorization and thus are unable to provide differentiated access privileges for different users within a dataset [9-12]. Asymmetric cryptography is better suited to this dynamic setting by encrypting individual contributions with different public keys.

1.2. Proposed System

If students have an option to give an exam on a web base portal, after completion of exam, results/Certificate is saved on Blockchain. In this case other people can view the certificate online and no 3rd party validation is required for these digital certificates. We are proposing a web based portal for university/college/institution and students that will provide options to students to get certificates on blockchain and minimize the option of fraud and duplicate education certificates. Blockchain-based educational certifications are registered on the Ethereum Blockchain that will be secure and tamper proof as data cannot be erased/ Rewrite on the blockchain server. Since a blockchain is a permanent record of transactions that are distributed, every transaction can irrefutably be traced back to exactly when and where it happened. In addition, past transactions cannot be changed, while the present can't be hacked, because every transaction is verified by every single node in the network. In this web-based portal, student and admin (university/Institution) will have login access and other than student and admin can view exam details and verify certificates. It will have below two major parts,

- Students can select courses, give exams and after successful completion can get a certificate on blockchain.
- Admin can manage students, courses papers and question banks and can generate certificates on blockchain.

2. Method

The methodology for implementing certificate validation using blockchain technology is designed to ensure the authenticity, integrity, and immutability of certificates issued by educational institutions, professional bodies, or other certifying organizations. This approach leverages the decentralized nature of blockchain to create a transparent, secure, and tamper-proof system that significantly reduces the risk of certificate fraud. The system is structured as a decentralized application (DApp) comprising three main components: a blockchain network, smart contracts, and user interfaces. The blockchain network serves as the foundation where certificate data is stored. Smart contracts, which are self-executing with the terms of the agreement directly written into code, manage the issuance, storage, and validation of certificates. User interfaces provide the necessary tools for institutions, certificate holders, and verifiers to interact with the system. The certificate issuance process begins with the certifying institution collecting the necessary information, such as student details and course completion status, to generate a digital certificate. A unique cryptographic hash is then created from this certificate data, acting as the certificate's digital fingerprint. A smart contract is deployed on the blockchain, containing the certificate hash and relevant metadata, such as the issuance date and the issuing institution. This data is then recorded on the blockchain, creating an immutable and time-stamped entry. To ensure the availability and redundancy of the certificate data, it can be optionally stored on a decentralized file storage system, such as the Inter Planetary File System (IPFS). The certificate is identified by a unique Certificate ID, which is provided to the certificate holder for easy access and verification. When a verifier, such as an employer, needs to validate a certificate, they can submit the Certificate ID or certificate data to the blockchain network. The system then generates a hash from the provided data and compares it with the hash stored on the blockchain. If the hashes match, the certificate is deemed valid, and the system returns the certificate's metadata, confirming its authenticity. If the hashes do not match, the certificate is flagged as invalid. The system defines specific roles and access controls for the different user groups. Issuing institutions have the authority to issue and revoke certificates and interact with the blockchain through a secure interface. Certificate holders can access their certificates and

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.557
e ISSN: 2584-2854
Volume: 02
Issue:12 December 2024
Page No: 3755-3759

share their Certificate ID with verifiers, though they have read-only access to the blockchain records. Verifiers can access the validation interface to submit certificates for verification, with only read access to the blockchain data. The methodology also includes mechanisms for certificate revocation and updates. Institutions can revoke certificates by marking them as revoked on the blockchain, with a reason for revocation attached to the record. If a certificate needs to be updated, a new hash is generated, and the old record is marked as obsolete. The updated certificate is then issued with a new entry on the blockchain [13-20].

2.1. Implementation

Implementing certificate validation using blockchain technology involves several key steps to ensure a secure and efficient system. The first step is selecting an appropriate blockchain platform, such as Ethereum or Hyperledger, depending on the specific needs, such as whether a public or private blockchain is more suitable. Once the platform is chosen, the development of smart contracts begins. These contracts are coded to handle the core functions of certificate issuance, storage, and validation. The smart contracts contain the rules and logic for creating, verifying, and possibly revoking certificates, ensuring these processes are automated and tamper-proof. Next, the integration of a user interface (UI) is essential to allow various stakeholders, including educational institutions, certificate holders, and verifiers, to interact with the system. Institutions use the UI to issue certificates by entering relevant details, which are then hashed and recorded on the blockchain. Each certificate is linked to a unique ID provided to the certificate holder, allowing them to easily share this ID with verifiers. The verifier can then use the UI to enter the certificate ID and initiate a validation process. The system compares the hash of the provided certificate data with the hash stored on the blockchain. If they match, the certificate is confirmed as authentic. To enhance security and data availability, certificate data can be stored on a decentralized storage solution like IPFS, with only the cryptographic hash stored on the blockchain. This approach ensures that even if the storage system is compromised, the data remains secure and verifiable. Additionally, the implementation includes creating mechanisms for certificate revocation and updates. Institutions must be able to revoke a certificate, marking it as invalid on the blockchain, or issue updates to existing certificates, ensuring the system reflects the most current information, shown in figure 1, figure 2 & figure 3.

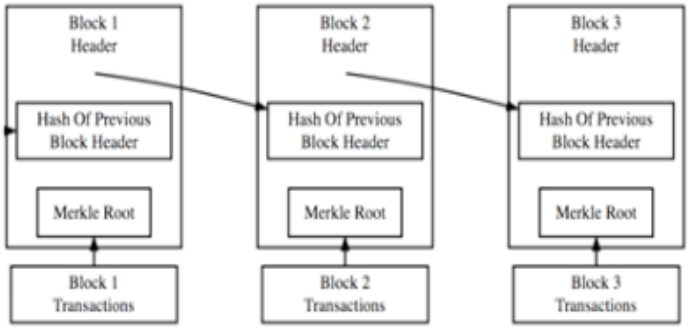

Figure 1 A Simplified Blockchain

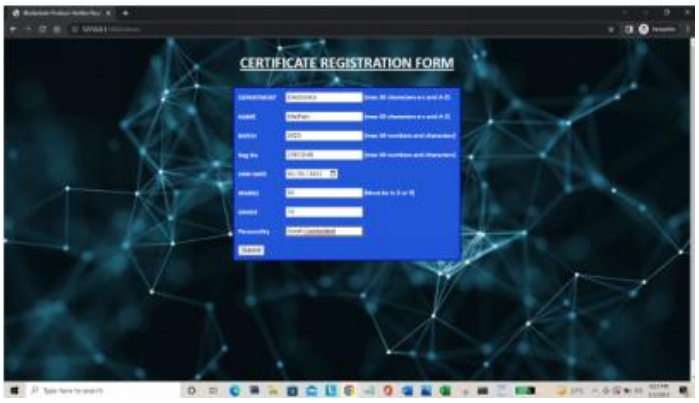

Figure 2 Output Image for Uploading A Certificate

Figure 3 Stored Certificate

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.557
e ISSN: 2584-2854
Volume: 02
Issue:12 December 2024
Page No: 3755-3759

3. Results and Discussion

3.1. Results

The implementation of certificate validation using blockchain technology yielded several significant results, demonstrating the system's effectiveness and reliability. First, the blockchain-based solution successfully ensured the immutability and security of certificates. Once a certificate was issued and its corresponding hash was recorded on the blockchain, it became virtually impossible to alter the certificate without detection. This feature greatly reduced the risk of certificate fraud, providing a high level of trust and assurance to verifiers and institutions alike. The system also proved highly efficient in validating certificates. Verifiers could quickly and easily confirm the authenticity of a certificate by comparing the provided data with the hash stored on the blockchain. This process was streamlined and required minimal time, reducing the administrative burden typically associated with manual verification processes. The system's decentralized nature eliminated the need for intermediaries, further enhancing efficiency.

3.2. Discussion

The ability to revoke or update certificates was effectively implemented, allowing institutions to manage the lifecycle of certificates with precision. Certificates marked as revoked or obsolete were immediately flagged within the system, ensuring that only current and valid certificates could be verified. This feature provided institutions with the flexibility to correct errors or address issues without compromising the integrity of the overall system. In terms of user experience, the interfaces developed for institutions, certificate holders, and verifiers were intuitive and user-friendly. Feedback from pilot users indicated that the system was easy to navigate, with clear instructions and efficient workflows, leading to high levels of satisfaction among all user groups.

Finally, the system's scalability and adaptability were validated during the testing phase. The blockchain-based solution was able to handle a large number of certificate issuance and validation requests without performance degradation. This demonstrated its potential to scale across various institutions and industries, accommodating growing demands while maintaining security and efficiency. Overall, the results confirmed that a blockchain-based approach to certificate validation is not only feasible but also highly effective, providing a secure, efficient, and user-friendly solution to the challenges of credential verification.

Conclusion

In conclusion, implementing certificate validation using blockchain technology offers a robust, secure, and transparent solution to the challenges of certificate fraud and verification. By leveraging blockchain's decentralized nature, institutions can ensure that certificates are immutable, easily verifiable, and resistant to tampering. The integration of smart contracts automates the issuance, storage, and validation processes, reducing the need for intermediaries and minimizing the potential for errors or fraud. This system not only enhances trust between institutions, certificate holders, and verifiers but also streamlines the verification process, making it more efficient and reliable. As blockchain technology continues to evolve, its application in certificate validation holds great potential for improving the integrity and security of credentials across various industries.

References

[1]. Lyndon Lyons and Andreas Bachmann Jan Seffinga, "The Blockchain (R)evolution –The Swiss Perspective," , Switzerland, 2017.
[2]. Don Tapscott and Alex Tapscott, "Realizing the Potential of Blockchain-A Multistakeholder Approach to the Stewardship of Blockchain and Cryptocurrencies," in World Economic Forum, 2017.
[3]. Alex Tapscott, BLOCKCHAIN REVOLUTION:Understanding the 2nd Generation of The Internet and the New Economy, 2017.
[4]. Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, White Paper.
[5]. George F. Hurlburt and Irena Bojanova, "Bitcoin: Benefit or Curse?," in IEEE, 2014.
[6]. Nicola Dimitri, The Blockchain Technology: Some Theory and Applications, 2017, MSM-Working Paper No. 2017/03.

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.557
e ISSN: 2584-2854
Volume: 02
Issue:12 December 2024
Page No: 3755-3759

[7]. Deokyoon Ko, Sujin Choi, Sooyong Park, Kari Smolander Jesse Yli-Huumo, "Where Is Current Research on Blockchain Technology?—A Systematic Review," October 2016.
[8]. Nirmala Singh and Sachchidanand Singh, "Blockchain: Future of financial and cyber security," in IEEE, Noida, 2016.
[9]. Engin Zeydan and Suayb Sb Arslan Gültekin Berahan Mermer, "An overview of blockchain technologies: Principles, opportunities and challenges," in IEEE, Turkey, 2018.
[10]. Narn-Yih Lee , Chien Chi and Yi-Hua Chen Jiin-Chiou Cheng, "Blockchain and smart contract for digital certificate," in IEEE, Japan, 2018.
[11]. Henrique Rocha ,Marcus Denker and Stephane Ducasse Santiago Bragagnolo, "SmartInspect: solidity smart contract inspector," in IEEE, Itly, p. 2018.
[12]. GWYN D'MELLO. (2017, Dec.) https://www.indiatimes.com/technology/news. [Online].
[13]. Abdul Wadud Chowdhury. (2017, Nov.) https://medium.com. [Online].
[14]. Nick Grossman. (2015, June) https://www.nickgrossman.is. [Online].
[15]. Aisong Zhang and Xinxin Ma, "Decentralized Digital Certificate Revocation System Based on Blockchain", Journal of Physics: Conference Series, Volume 1069, 3rd Annual International Conference on Information System and Artificial Intelligence (ISAI2018) 22–24 June 2018, Suzhou.
[16]. Nitin Kumavat, Swapnil Mengade, Dishant Desai, JesalVarolia, " Certificate Verification System using Blockchain" Computer Engineering Department, Mumbai University.
[17]. S.Sunitha kumari, D.Saveetha "Blockchain and Smart Contract for Digital Document Verification" Department of Information Technology- SRM Institute of Science and Technology.
[18]. D. S. V. Madala, M. P. Jhanwar, and A. Chattopadhyay, "Certificate Transparency Using Blockchain," 2018 IEEE International Conference on Data Mining Workshops (ICDMW), Singapore, Singapore, 2018, pp. 71-80, doi: 10.1109/ICDMW.2018.00018.
[19]. Jiin-Chiou Cheng; Narn-Yih Lee; Chien Chi; Yi-Hua Chen, "Blockchain and Smart Contract for Digital Certificate" IEEE International Conference on Applied System Invention (ICASI),2018.
[20]. Wang Z., Lin J., Cai Q., Wang Q., Jing J., Zha D. (2019) Blockchain-Based Certificate Transparency and Revocation Transparency. In: Zohar A. et al. (eds) Financial Cryptography and Data Security. FC 2018. Lecture Notes in Computer Science, vol 10958. Springer, Berlin, Heidelberg.