International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 07, July-2021

Counterfeit Detection of Documents using Blockchain

Rajesha[1], Rohini Krishna Mohite[2], Sahana S[3], Shilpashree B N[4], Rakesh K R[5]
[1, 2,3,4] U.G Student, Vidyavardhaka College of Engineering, Mysuru, India
[5]Asisstant Professor, Vidyavardhaka College of Engineering, Mysuru, India

***Abstract*— Document verification is a domain that involves various challenges and monotonous processes to authenticate the documents. The verification for each type of document is to be processed in distinct ways. The issuing of documents is not transparent and hence fake documents can be created. Documents or certificates generated by organizations play a vital role for students. With the increase of forged documents, credibility of both the students and the organization is imperiled. Verifying a document takes some time and also requires more human resources to request for the confirmation of the data provided. Managing documents or records often comes at the cost loss of data or document counterfeits.**

In the digital world, blockchain technology has recently emerged as a potential mean for authenticating the document verification process and is a significant tool to combat document fraud and misuse. In this paper, we aim to enhance the document verification process using blockchain. We propose a system which uses the InterPlanetary File System [IPFS] protocol and also a peer-to-peer-network for storing and sharing data in a distributed file system. By using this blockchain technology, we can provide a more secure and efficient digital certificate validation.

Keywords:- Document verification, Authenticity, Blockchain, Inter Planetary File System, Smart Contracts

INTRODUCTION

Documents or any records of students are commonly issued as a paper document. These documents are easy to counterfeit, and can be lost or jeopardized. Blockchain technology is a system that records the data in a way that makes it difficult or non-viable to change or hack the system. A blockchain is a digital ledger of transactions that is duplicated and distributed across the entire network of computer systems on the blockchain.

The certificates issued by the organizations are in the form of a paper document and the contents on the paper can be easily changed with the advanced technology. This is a threat to both the organization that issues the document and the one who receives the document. Hence it is necessary to validate the document from an authentic source. To carry this process it takes time to cross-verify with the organization as well as the receiver and it can be expensive too.

Blockchain technology is recently introduced to improve the document verification process and combats the document fraud and misuse. This technology is intended to avoid the problem of fake certificates or fraud in any of the documents. Counterfeiting of documents certificates happens because there is no upper-level authority to validate the documents. Since people are not aware of this technology many blockchain applications have been failed. The blockchain provide an immutable data storage. Blockchain technology is used to reduce the forgeries of the documents. The documents that are present on the blockchain must fulfill the basic criteria's such as authentication, authorization, confidentiality, ownership and privacy.

I. BLOCKCHAIN TECHNOLOGY: CHARACTERISTICS

Blockchain technology uses many other techniques to counterfeit the documents like distributed consensus algorithms, cryptography and mathematics. Blockchain technology has six characteristics and they are as follows:

1. Immutability

Immutable means that can't be changed or altered. Every node on the system has a copy of the digital ledger and for a person to add a document or make changes to the document, the node needs to check its validity and majority of the nodes should vote for the changes and this process is transparent.

2. Decentralized

Decentralized means that the blocks are not authorized by a single person. The person with private key will have full access to the node. Some of the benefits of this feature are user control, no third-party and it is authentic.

3. Enhanced Security

Blockchain uses encryption and other methods for its security. Cryptography plays a vital role in this feature as it acts as a firewall to the hackers. Every document in the blockchain is hashed cryptographically and they have unique identification.

4. Distributed Ledgers

Distributed ledger is the database that is shared and synchronized across multiple nodes in the network. Due to this feature of blockchain no malicious changes can be done and the verification of the owner is performed.

5. Consensus

Consensus is an algorithm through which all the nodes of the blockchain network come to a common agreement on the present data state of the ledger and be able to trust unknown nodes in a distributed system. Each consensus algorithm has its own unique way to make decisions.

6. Faster Settlement

It takes more time to process a transaction and to complete the settlements in traditional banking and even this can be jeopardized by many means of sources. This feature

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 07, July-2021

compared to the traditional banking allows the user to transfer money relatively faster and this saves more time.

II. BLOCKCHAIN TECHNOLOGY: STRUCTURE

Blockchain is a chain of blocks that contains information. Each block in the blockchain contains six elements and they are as follows:

1. Data

The data in the block chain depends on the user and the type of transaction it can be either currency transactions or transaction of the documents between the nodes.

2. Timestamp

Timestamps shows how the blocks are connected in a chronological order and it marks the time for each transaction on the block in a blockchain by recording the time when and what has happened on the blockchain.

3. Previous Hash

When a transaction is executed, a hash value is generated and broadcasted to the network and this is unique to each block.

4. Nonce

A nonce is a random value that is used in the protocol for the guarantee to transmit the data and this protects against the attacks on the blocks.

5. Hash

The hash values are 256 bits or 64 characters. This value is recorded in the block header of the present block and the content is the body of the block.

Blocks are generally bound to a size hence allowing a limited number of transactions per block.

6. Transaction List

The transactions that are done on the particular block are stored here and the information and the information can be viewed by the user with the private key.

The first block in the blockchain is the genesis block. The structure of a blockchain is shown in Figure 1.

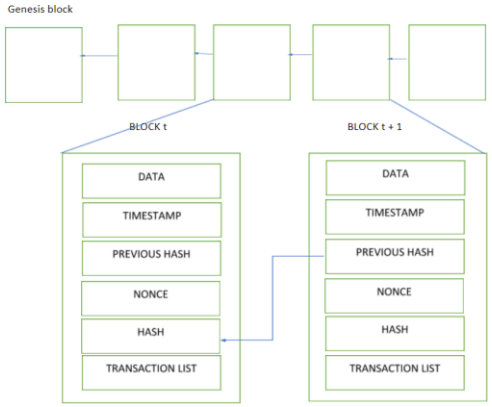

Figure1. Structure of Block chain

III. OBJECTIVES

To terminate the existing technologies where the certificates are issued on papers and are to be validated using human resources which consumes more time , we use the immutable characteristic of the blockchain provides more security and transparency in the transactions of the proposed system which issues digital certificates with more accurate information without any involvement of the third-party.

IV. RELATED WORK

A. Gayathiri, et.al [1] developed an application to validate the certificates using blockchain. Sampling and quantization are used to convert paper certificates into digital certificates. Hash value is generated using chaotic algorithm. Admin can perform two operations such as registering students and uploading student's certificate. Administrator login into to this application through admin login to upload the student's certificate which converts the analog image into digital image. By using verifier login id and password, they can validate their certificate.

Shanmuga Priya R, et.al [2] proposed a system to validate certificates online using blockchain. This system is proposed to reduce the certificate forgery. In this system, the user first fills all the required basic information and gets confirmation through email. An e-certificated will be generated with a QR code. For each certificate a serial number will be created and it will be automatically recorded in the blockchain. Each verified graduate will receives an electronic file of their certificates and an inquiry number. This system provides information accuracy and security.

Omar S. Salesh, et.al [3] proposed a system for verifying educational certificates using hyperledger fabric framework. Academic certificates represent the skills, knowledge, aptitude achieved by an individual through education. Since these certificates have more value, people try to produce fake certificates. This system aims to enhance the process of document verification. Hyperledger platform is used. System administrator will assign a unique identity to each user. Authenticated access of flow of data to and from the hyperledger will be ensured by the encryption API endpoints. Documents uploaded by the owner will be linked with the owner identity protecting the ownership. Documents verification will be performed by the verifier ensuring confidentiality and privacy.

Meerja vali Shaik, et.al [4] proposed a system for issuing certificates using smart contracts based on blockchain technology. Certificates are valued currency for students. Nowadays duplicate certificates look original and it requires great efforts to identify which is real. To solve this above problem, they have developed a smart contract that performs functions such as issuing the certificate, verifying the certificate and revoking the certificate. Administrator requires person name, document id, and issuer name and certificate type to issue a new certificate. After filling the details, a new certificate will be issued with a timestamp and gas price is charged for this operation. Students can verify whether their documents exist in the blockchain network. Revoke function shows the details of the document.

Mili Rafi, et.al [5] proposed a certificate management and validation system using blockchain. The main participants

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 07, July-2021

of this system are Admin, student and verifier. All the details of the students entered by the admin are deployed in the hyperledger fabric, which is done via composerRestServer. Upon verifying the certificate preview, the university enters the digital signature. Hash code is generated. Only the approved certificates are deployed in the hyperledger. Students receive a copy of their certificates using QRcode. Students can share their QRcode to the verifier, using that the verifier can verify their certificate without any difficulties.

Clemens Brunner, et.al [6] developed a platform for issuing and verifying the documents in a public blockchain which is called as SPROOF. This platform does not have any limitations on the issuer. Only the hashes of the data are added to the blockchain within the transaction. A key derivation function (KDF) is used to derive one or more private keys from a master key. Issuer establishes a public-private key pair to create a new account. In order to prove the ownership of a document to the verifier, the public key along with its corresponding private key is used. The receiver has to register at an issuing institution in order to upload documents in this platform. Hierarchical Deterministic Wallet is used for key management. This platform follows the principles of Web of Trust.
Alsadig Bashir Hassan, et.al [7]proposed a system that the number of universities and the number of graduates is constantly increasing, verification of documents are needed due to this verification process of these degree certificates generates a lot of new job opportunities. A proof check of certificate is done from and trustable source while recruiting by the employer. Some academic centers allow a quick and simple online query to verify the authenticity of their certificates, without even asking who requires that information. Some assign the role to third parties (whether by default or as required by regulations) or market the service. Finally there are times when there is no alternative but to contact the office of the academic secretary at the educational institution directly, so that we can confirm if a diploma or qualification is valid or not while, academic credential fraud is a fact and comes through counterfeiting, as well as through the involvement of the authorities and employees of the institute. The frequency of these events is also adequate to detect the emergence of dedicated companies.

Jayesh G. Dongre, et.al [8] proposed an identity document forgery is a process by which authorized identity document is modified and copied by unauthorized party or parties to be used. They represent rich tools and techniques that highly support the creation of faked identities .This review paper investigates the current techniques for counterfeiting document forgery threats along with their achievements and limitation. These techniques are insufficient to mitigate ID forgery threats. New methods and techniques need to be identified.ID fraud is built on the foundation of a factious identity, often created with a combination of real data and fabricated information. For example the fraudster may one's person social security number, combine it with another person's name, and use someone else's address to create a brand new identity. The perpetrator can then use this fraudulent identity to apply for credit, make major purchases, or a variety of other activities that give the identity a financial history.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 07, July-2021

Author\s	Title	Technique\s	Result	Shotcoming\s
A. Gayathiri, J. Jayachitra and Dr.S.Matilda	Certificate validation using blockchain	Sampling, Quantization, chaotic algorithm	Using this mobile application, students can view and validate their certificate.	
Shanmuga Priya P and Swetha N	Online Certificate Validation using Blockchain	Ethereum blockchain, Smart contract.	This system creates an e-certificate containing a QR Code and generates a serial number for the certificate.	
Omar S. Salesh, Osman Ghazali and Muhammad Ehsan Rana	Blockchain based framework for educational certificates verification	Hyperledger Fabric Framework.	This framework mainly focuses on authentication, authorization, privacy, confidentiality and ownership.	The documents uploaded by the owner can be viewed on demand, for fixed durations of time.
Meerja vali Shaik, Ch. Rupa, M N S Koundinya, Rohith Gadde and Harish Donepudi	Blockchain based Certificate Issuing System using Smart Contracts	Metamask, Smart contract.	This system generates, verifies and revokes academic certificate.	To create a function which eliminates the fake certificates already exists in the society.
Mili Rafi, Sherin Mary Shaji and Prof. Ashly Thomas	Certificate Management and Validation system using Blockchain	Hyperledger Fabric Framework.	Using userid and password, students can view their certificates. The approved certificate is deployed in hyperledger.	
Clemens Brunner, Fabian Knirsch and Dominik Engel	SPROOF: A Platform for Issuing and Verifying Documents in a Public Blockchain	Distributed hash table, Hierarchical deterministic wallet	The ability to prevent receivers from hiding certain documents.	
Alsadig Bashir Hassan,Yahia A.Fadlalla	A Survey on Techniques of Detecting Identity Documents Forgery	Cryptography	60% of fake documents can be detected through detection machines	Many fake documents have not yet been detected, therefore more works in field is highly encouraged
Jayesh.G.Dongre, Dr.Kishore.T.Patil, Sonali M. Tikam and Vasudha B. Gharat	Education Degree Fraud Detection and Student Certificate Verification using Blockchain	Open-source Ark blockchain platform.	Students benefit from a single and transparent view of their completed courses, while have access to up to date data regardless of a student's educational origins.	Events which cause the graduation certificate to be forged are often seen due to the lack of an effective anti- forge mechanism.

V. CONCLUSION

In this paper, we proposed a solution to the problem of counterfeit of the documents based on blockchain technology. The blockchain technology provides the authentication, authorization, privacy, confidentiality and ownership to the documents of the user which are the required properties of the digital documents. Hence, the students as well as the organization are benefited with this system.

REFERENCES

[1] A. Gayathiri, J. Jayachitra and Dr.S.Matilda, "Certificate validation using blockchain, IEEE 7th International Conference on Smart Structures ans Systems ICSSS 2020.

[2] Shanmuga Priya P and Swetha N, "Online Certificate Validation using Blockchain", Special Issue Published in Int. Jnl. Of Advanced Networking and Applications (IJANA)..

[3] Omar S. Salesh, Osman Ghazali and Muhammad Ehsan Rana, "Blockchain based framework for educational certificates verification", Journal of Critical Reviews, Volume-7, Issue-3, 2020.

[4] Meerja vali Shaik, Ch. Rupa, M N S Koundinya, Rohith Gadde and Harish Donepudi, "Blockchain based Certificate Issuing System using Smart Contracts", International Journal of Innovative Technology and Exploring Engineering (IJITEE), Volume-9, Issue-7, May 2020.

[5] Mili Rafi, Sherin Mary Shaji and Prof. Ashly Thomas, "Certificate Management and Validation system using Blockchain", International Research Journal of Engineering and Technology (IRJET), Volume- 7, Issue-5, May 2020.

[6] Clemens Brunner, Fabian Knirsch and Dominik Engel, "SPROFF: A Platform for Issuing and Verifying Documents in a Public Blockchain", 5th International Conference on Information Systems Scurity and Privacy (ICISSP) 2019.

[7] Alsadig Bashir Hassan and Yahia A. Fadlalla, "A Survey on Techniques of Dectecting Identity Documents Forgery", Suden Conference on Computer Science and Information Technology (SCCSIT) 2017.

[8] Jayesh G.Dongre, Sonali M. Tikam, Dr. Kishore.T.Patil and Vasudha Gharat, "Education Degree Fraud Detection and Student Certificate Verification using Blockchain", International Journal of Engineering Research & Technology, ISSN, Volume-9, Issue-7, July 2020.