Secured System for Storing E-Documents and Viewing Challan

Siva Pavan Naveen G
B-Tech Student, Computer Science and Engineering, Dayananda Sagar University, Bangalore , Karnataka, India.

Aayush Bohra
B-Tech Student, Computer Science and Engineering , Dayananda Sagar University, Bangalore , Karnataka, India.

Adithya Adarsh
B-Tech Student, Computer Science and Engineering , Dayananda Sagar University, Bangalore , Karnataka, India.

Akash A
B-Tech Student, Computer Science and Engineering , Dayananda Sagar University, Bangalore ,Karnataka, India.

Dr. Mouleeswaran S.K
Associate Professor , Computer Science and Engineering , Dayananda Sagar University, Bangalore ,Karnataka, India.

Abstract:- In this paper, we're publishing about an operation that makes use of blockchain in a veritably effective way. Blockchain is known for the eventuality for transubstantiation traditional assiduity. Also, by barring the centralized approach, we can assure the safety and vacuity of data and communication. This operation allows us to storeE-documents and corroborate documents. Along with this stoner can also view the forfeitures challan. The gate will allow the stoner to see the evidence of why they were fined. In our operation all the stoner data is stored on a block which is connected to other blocks forming a chain. As the name suggests, a decentralized operation doesn't have a centralized garçon. It's principally a peer- to- peer network. Also the data that's stored in blocks is nearly insolvable to view as a veritably secure encryption and mincing functions are used. Also if a hacker tries to make changes to the information in the block also, he she will have to make changes to all the clones of that block on the whole blockchain network and that can be relatively insolvable. Though blocks are on all bumps, they can not pierce the information in it, only the person for whom the information is can pierce it.

Keywords:- *Blockchain, Data Storage, Data securing,Smart Contracts ,Security.*

I. INTRODUCTION

Blockchain is a distributed database with decentralized, traceable, non-tamperable, secure and reliable features. It integrates P2P (Peer-to-Peer) protocol, digital encryption technology, consensus mechanism, smart contract and other technologies together. Abandoning the maintenance mode of the traditional central node and adopting the method of mutual maintenance by multiple users to realize the information supervision among multiple parties, thereby ensuring the credibility and integrity of the data. The blockchain platform can be divided into public chain, private chain and alliance chain. All nodes in the public chain can join or withdraw freely; the private chain strictly limits the qualification of participating nodes; the alliance chain is jointly managed by several participating institutions. Bitcoin was proposed by Nakamoto in 2008, which is the most successful case of digital currency, and is also the most typical application of blockchain. In addition, the blockchain has expanded its unique application value in many aspects and has shown its potential to reshape society.

- *Hash and Block Structure:*

The hash algorithm is a function that maps a sequence of dispatches of any length to a shorter fixed- length value, and is characterized by vulnerability, unidirectionality, collision resistance, and high perceptivity. Hash is generally used to insure data integrity, that is, to corroborate the data has been immorally tampered with. When the data tested changes, its hash value also changes similarly. thus, indeed if the data is in an unsafe terrain, the integrity of the data can be detected grounded on the hash value of the data.

SHA is a type of cryptographic hash function issued by the National Institute of norms and Technology(NIST) with the general characteristics of a cryptographic hash function. The SHA256 algorithm is a class of the SHA- 2 algorithm cluster, which generates a 256- bit communication condensation. The algorithm's computation process includes two stages: communication, preprocessing and main circle. In the communication preprocessing stage, double bit stuffing and communication length stuffing are performed on the information of any length, and the filled communication is divided into several 512- bit communication blocks. In the main circle phase, each communication block is reused by a contraction function. The input of the current contraction function is the affair of the former contraction function, and the affair of the last contraction function is the hash value of the original communication.

The core of the processing algorithm is the contraction function, which is a circle, where each circle consists of 16 step functions. Using different original sense functions in each circle, the processing of the algorithm is divided into two different cases, with five of the two original sense functions running in rear order. After all 512- bit packet processing is completed, the performing 160- bit affair is the hash value of the original communication.

For blockchain, hash functions can be used to perform block and sale integrity verification. In the blockchain, the hash value of the information of the former block is stored in the title of each block, and any stoner can compare the calculated hash value with the stored hash value. In turn, the integrity of the information of the former block is detected. Also, the hash function can be used to induce public-private key dyads.

The hash pointer is a data structure that contains, in addition to the usual pointers, some data information and word hashes associated with the information. A normal pointer is used to recoup information, and a hash pointer is used to corroborate that the information has been tampered. The blockchain is a list of hash pointers, each of which is connected by using a hash value. It's vindicated according to the hash value whether the data contained in the block is changed, thereby icing the integrity of the block information.

➢ *Electronic Document:*

Electronic document means any information in digital form that's conveyed to an agency or third- party, where information may include data, textbook, sounds, canons, computer programs, software, or databases. Data, in this environment, refers to a demarcated set of data rudiments, each of which consists of a content or value together with an understanding of what the content or value means; where the electronic document includes data, this understanding of what the data element content or value means must be explicitly included in the electronic document itself or differently be readily available to the electronic document philanthropist.

➢ *What is Cryptography:*

By concept, it is a method of developing techniques and protocols to prevent a third party from accessing and gaining knowledge of the data.

- *Terminologies*

✓ **Encryption**: It is a process of plaintext (normal text) to a ciphertext (random sequence of bits).
✓ **Key**: A small amount of information is required to induce the output of the cryptographic algorithm.
✓ **Decryption**: The inverse process of encryption, conversion of ciphertext to plaintext.
✓ **Cipher**: The mathematical function, i.e. a cryptographic algorithm which is used to convert plaintext to ciphertext.

➢ *Role of Cryptography in Blockchain:*

- *Why Use Cryptographic Hash Functions*

Well, cryptographic hash functions provide the following benefits to the blockchain,

✓ **Avalanche effect-** i.e., a slight change in the data can result in a significantly different output.
✓ **Uniqueness-** i.e., very input has a unique output.
✓ **Deterministic-** i.e., any input will always have the same output if passed through the same hash function.
✓ **Quickness-** The affair can be generated in a veritably small quantum of time.

Rear engineering isn't possible, i.e. we can not induce the input by having the affair and the hash function.

Further, hash functions have a major part in linking the blocks to one another and also in maintaining the integrity of the data stored inside each block. Any revision in the block data can lead to inconsistency and break the blockchain, making it INVALID. This demand is achieved by the property of the hash functions, called the ‘ avalanche effect’.

It’s this point that makes the data dependable and secure on the blockchain. And any changes in the block data will lead to this difference in hash value and make the blockchain invalid, making it inflexible.

II. LITERATURE REVIEW

Madura Rajapashea*, Muammar Adnanb, Ashane Dissanayaka, Dasith Guneratned , Kavinga Abeywardanee. Multi-Format Document Verification System American Scientific Research Journal for Engineering, Technology, and Sciences 2020. In this paper they proposed a method of a multi-format document verification scheme using digital signatures and blockchain and they also employ digital signature algorithms to sign document contents extracted using Optical Character Recognition (OCR) methods and attach this signature to the document by converting it into a 2D barcode format. This code can then be used on a shared document to retrieve the document's digital signature and OCR can be used to verify the signature. From this paper we took these signed documents and stored them in a decentralized storage solution backed by blockchain technology, increasing the solution's overall reliability and security.

Raza Abbas Haidri, Shivam Vatsyayan . Design of Hybrid Cryptography System based on Vigenere Cipher and Polybius Cipher. International Conference on Computational Performance Evaluation 2020. Cryptography Cipher text conversion. In this Paper they explained new hybrid security ciphers by combining the two most important Ciphers such as Polybius Cipher and Vigenere Cipher. This hybrid encryption cipher provides greater security as compared to classic ciphers. From this paper we referred to how Cryptography is utilized as a technique for the security, privacy, confidentiality and reliability of data.

Shipping Zhai 1,2, Yuanyuan Yang 1*, Jing Li1. Research on the Application of Cryptography on the Blockchain. IOP Conf. Series: Journal of Physics: Conference 2019. Blockchain Cryptography. In this Paper they explained the principles of encryption technology and were introduced briefly, such as hash function, asymmetric cryptosystem, and digital signature. From this paper we referred to how cryptography technology is introduced to elaborate the blockchain. And how we can use it for data securing purposes.

Kahina Khacef , Guy Pujolle, 33rd International Conference on Advanced Information Networking and Applications (AINA-2019), Mar 2019, Matsue, Japan. Secure Peer-to-Peer communication based on Blockchain. Blockchain, Smart contracts. In this paper the propose is to create a secure messaging solution based on the blockchain technology and explain why blockchain would make communications more secure, and we propose a model design for blockchain-based messaging maintaining the performance and security of data recorded on the blockchain, using a smart contract to verify the identities and their associated public keys, and validate the users certificate. And their system is entirely decentralized and allows users to exchange messages securely. From this paper we referred to how the most commonly employed approaches to ensure this property are PKI and S/MIME email encryption protocols, but indeed they are facing multiples security threats, such as the MITM attack and EFAIL attack.They used blockchain which is an innovative technology that overcomes these threats and allows to decentralize sensitive operations while preserving a high level of security. It eliminates the need for trusted intermediaries.

H. N. Datir [5] evaluated seven different attribute-based encryption algorithms, including ABE, KP-ABE, EKP-ABE, CP-ABE, CP-ASBE, HIBE, HABE, and HASBE, and came to the conclusion that Hierarchical attribute-based encryption (HASBE) provides the best access control mechanism. It is more versatile and efficient than previous methods, with less calculation overhead. The HASBE method employs a delegation mechanism to create a hierarchical structure of system users. Owing to versatile and resilient attribute set combinations, the HASBE system allows compound attributes and provides fast user revocation due to attributes assigned multiple values. Pooja More [6] presented an Attribute Based Key Aggregate Cryptosystem for cloud data security. To search the document saved on the cloud, the system employs a trapdoor key and searchable keywords. Once the document has been fetched, the aggregate key is used to decrypt and download a specific document from the pool of documents.

The trapdoor key is exposed to the public for a specific group, but aggregate key access is determined by the data owner's characteristics. The system employs a CP-ABE method with a fixed ciphertext and key size, which improves efficiency. Instead of connecting user attributes to a key, two distinct files are created, one for the key and the other for the collection of attributes. Ilya Sukhodolskiy and Sergey Zapechnikov suggested a blockchain-based cloud storage access management system. It offers a method for accessing data kept in untrustworthy settings, such as cloud storage. Data such as multimedia content, documents, and other types of data will be kept in cloud storage, with metadata identifying the file available only on the blockchain. Because the data kept in the blockchain is public, it is encrypted before being sent to storage and access is controlled.

To read a file, the user must meet the access policy and have the appropriate keys to decrypt and download it. The owner of the data provides the decryption keys.

➢ *Final Inference of Literature Review:*

- In this paper we collected these signed documents and stored them in a decentralized storage solution backed by blockchain technology, increasing the solution's overall reliability and security.
- This hybrid encryption cipher provides greater security as compared to classic ciphers. From this paper we referred to how Cryptography is utilized as a technique for the security, privacy, confidentiality and reliability of data.
- This Paper explained the principles of encryption technology and were introduced briefly, such as hash function, asymmetric cryptosystem, and digital signature. From this paper we referred to how cryptography technology is introduced to elaborate the blockchain. And how we can use it for data securing purposes.
- This paper we referred to how the most commonly employed approaches to ensure this property are PKI and S/MIME email encryption protocols, but indeed they are facing multiples security threats, such as the MITM attack and EFAIL attack.They used blockchain which is an innovative technology that overcomes these threats and allows to decentralize sensitive operations while preserving a high level of security. It eliminates the need for trusted intermediaries.
- Owing to versatile and resilient attribute set combinations, the HASBE system allows compound attributes and provides fast user revocation due to attributes assigned multiple values. Pooja More presented an Attribute Based Key Aggregate Cryptosystem for cloud data security. To search the document saved on the cloud, the system employs a trapdoor key and searchable keywords. Once the document has been fetched, the aggregate key is used to decrypt and download a specific document from the pool of documents.
- It offers a method for accessing data kept in untrustworthy settings, such as cloud storage. Data such as multimedia content, documents, and other types of data will be kept in cloud storage, with metadata identifying the file available only on the blockchain. Because the data kept in the blockchain is public, it is encrypted before being sent to storage and access is controlled. To read a file, the user must meet the access policy and have the appropriate keys to decrypt and download it. The owner of the data provides the decryption keys.

III. PROPOSED METHODOLOGY

➢ *File Upload:*

A file.pdf format is uploaded by the Verifier. Indeed though similar lines include unshaped data, it's assumed that they all follow the same pattern, which has been authorized by each department's internal nonsupervisory authorities. The sense of the system will be driven by this policy.

- *Information Extractor:*

The parser's detected fields will help the IE module in getting the right data and saving it in a table. The information view will be generated automatically by the module using Natural Language Processing(NLP)

- *Information-View Builder:*

The uprooted data will be reused and stored in a systematized way by the module. The module is in charge of delivering the view to the cybersurfer. The Verifier verifies that the view was created rightly, and by choosing the stoner name, he transfers the material to him her account.

- *Information-View Encryption:*

The view will be translated, and the blockchain will only keep the translated material. a stoner thesis has been successfully defended and passed. Every time a verification is needed, the blockchain will act as a backup system. In this script, the view will be deciphered, compared to the database view, and a determination made as to whether it's validated or not. An analogous approach is followed during the verification process. In this work, we don't give a complete picture, but we can claim that the difference lies in the database sense. The requested stoner thesis will be recaptured from the blockchain, translated, and also a record will be set up in the database indicator, which will be compared to the decrypted view. A positive match indicates that the stoner has been vindicated as the document's proprietor.

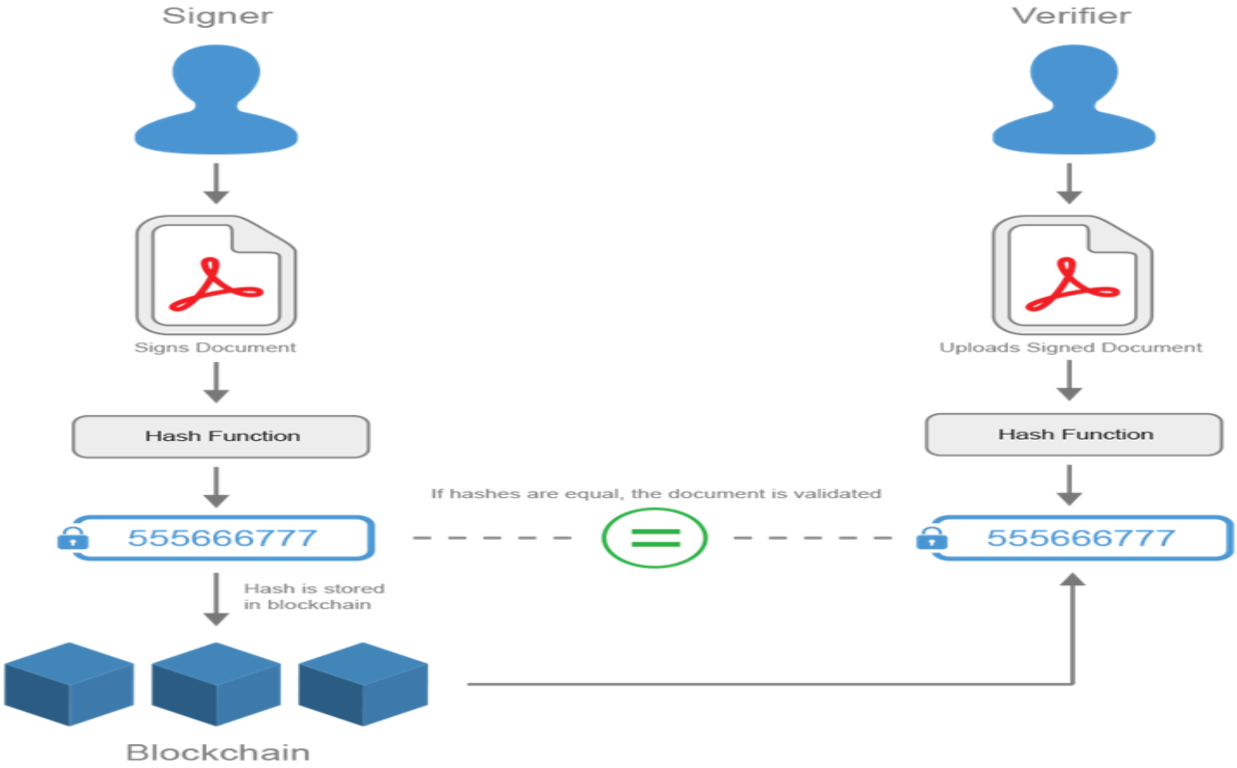

Fig 1 Information-View Encryption

IV. CONCLUSION

Blockchain technology has been in the key focus areas of development for all the multinational companies and also a huge number of start-ups are emerging in this technology from the past few years. Once the user's identities are confirmed by validating the document, the users will be able to access the e-documents such as license, RC, etc. The user when given a challan will also be shown a proof of when the challan was charged along with the amount payable. This introduces the main applications of cryptography in the blockchain and analyzes existing problems. Firstly, starting from the blockchain infrastructure, the blockchain technology is simplified. Secondly, cryptography technology is introduced to elaborate the blockchain. Finally, the existing security problems in the blockchain are analyzed.

REFERENCES

[1]. Nakamoto, S. (2008) Bitcoin: A peer-to-peer electronic cash system. Consulted., 165: 55-61.

[2]. Zhu, Y., Gan, G.H., Deng, D. (2016) Security Research in Key Technologies of Blockchain. Information Security Research., 12: 1090-1097.

[3]. Liu, X.F. (2017) Research on blockchain performance improvement of Byzantine fault-tolerant consensus algorithm based on dynamic authorization. Zhejiang University.

[4]. Wang, X., Lai, X., Feng, D. (2005) Cryptanalysis of the Hash Functions MD4 and RIPEMD. Advances in Eurocrypt., 3494: 1-18.

[5]. Shen, Y., Wang, G. (2017) Improved preimage attacks on RIPEMD-160 and SHA-160. Ksii Transactions on Internet & Information Systems., 12: 727-746.

[6]. Wang, H.Q., Wu, T. (2017) Cryptography in Blockchain. Journal of Nanjing University of Posts and Telecommunications., 37: 61-67.

[7]. Yuan, Y., Wang, F. (2016) Current Status and Prospects of Blockchain Technology Development. Acta Automatica Sinica., 42: 481-494.

[8]. Miyaji, A. (1994) Elliptic Curves Suitable for Cryptosystems. Ieice Transactions onFundamentals of Electronics Communications & Computer Sciences., 77: 98-105.

[9]. He, P., Yu, G., Zhang, Y.F. (2017) Prospective review of blockchain technology and application. Computer Science., 44: 1-7.

[10]. Zhai, S.P., Li, Z.Z. (2018) The data block chain of the key technologies Consistency. Computer Technology and Development., 8: 1-6.

[11]. An, Q.W. (2017) Research and application of key technologies for decentralized transactions based on blockchain. Donghua University.