International Journal of Research in Engineering, Science and Management
Volume-1, Issue-11, November-2018
www.ijresm.com | ISSN (Online): 2581-5792

A Secure Storage Method Based on Blockchain for Authentic Documents

D. Bhaskar[1], P. Nathan[2], G. Karan[3]
[1]*Professor, Dept. of Computer Science and Engg., SRM Institute Of Science and Technology, Chennai, India*
[2,3]*Student, Dept. of Computer Science and Engg., SRM Institute Of Science and Technology, Chennai, India*

***Abstract*: It's been years since technology has started to evolve into something new but still, we have been signing bonds and legal documents in papers. This is because we don't have trust on the cyber security and so tech was not used in most of the trust related sectors. Ever wondered how we can build the system into digital print and stop using papers in the most secure way possible? This was enabled by the recent hype and amount of interest going on in the cryptocurrencies and blockchain space and we got sparked to take the same underlying technology of bitcoin i.e. the blockchain to the area of legal documents and bonds related to properties, and other things .The very fundamental use of blockchain is encryption that makes it unbreakable and decentralization. The possibilities are endless when there is hope and aim.**

***Keywords*: Blockchain, data storage, database, decentralization, single point failure, documents, central authority**

1. Introduction

In today's world security is a growing concern and it has been ages since we started using papers for important documents. One of the main reason we don't use digital storage to keep important records is security and we now have new technologies that can be applied to greatly improve that factor. The solution we are trying to apply here being Blockchain where we store the documents on different places we call nodes in a hashed manner and also gain the ability to retrieve the file wherever and whenever we want.

This makes storing and viewing the documents much easier that the existing system where physical papers are used.In this system we upload the documents into the system where many nodes are present to store them which all are connected and sync whenever there is a new transaction involved,i.e,whenever a new document is added.This consensus [1] helps us to keep the document safe and immutable where upon if it is changed in one node the other nodes will recognize that there has been a change in the document and show an error in syncing the particular document and the system that there is a change in.

This system is also added with a client side encryption and decryption facility which enables a 3 layer protection of the document. Thus making it more secure than before and more accessible that the physical documents. This decentralized server also enables the ability to prevent the server from ever going down due to the overloading or DDoS [2] attacks. Thereby making this system best for applying in the field of document storage. Since we are using this for government based systems we need not worry about the nodes as there will already exist a system in every government office that can be used as a node for the network.The system thereby includes the features of Immutability, High Security and a server that never goes down. [3]

2. Related work

Records Keeper is an open public mineable blockchain for record saving and securities. They majorly concentrate on banking, government documents, patents etc.

Block Sign is a blockchain service for legally signing any document, contract, or agreement. It just signs documents and adds a timestamp to it. [4]

Stampery: They generate immutable and independently verifiable records of everything that is important for business. [5].

Actually it's even possible to add documents to existing blockchains such as bitcoin, ethereum as raw data in it [6]. But the usability is very low in this case. It's hard to save MBs of data in it. The sentence case of walking turn on documents uploaded don't have ability to store post kind of data in their respective databases.

3. Overall framework

The framework consists of four main parts:

A. The storage
B. The maintenance
C. The issue system
D. The verification system

A. The storage

The plan we have is not to follow the same principles and ideas that the existing blockchains contain. As mentioned earlier the storage system will be so compatible with high size documents that is in MBs. So the plan is we will not save all the documents in all the nodes. We will be determining parameters like, say the minimum number of nodes required for a document to be healthy on the network. We determine this number by keeping the size of the document in this mind and the amount of times it's been accessed everyday. So lately we have been developing a database that's decentralized and can store large

amount of data like documents and this technology is based on node js and file systems.

B. The maintenance

So we will be starting a network but who will maintain it ?One idea is to make a Windows or Mac OS or Linux installable and executable file that needs to be installed on every system of a document issuer and verifier. Say in the example of government issued ID, certificates, patents, etc. we require the software to be installed on every government office in each and every town or city. While this weak and maintained recordable system is where documents can be stored in an encrypted manner.

C. The issue system

Only authorised people can issue documents that can be maintained by authority of some kind that continuously checks the originality of the issuer's organisation. The issuers will also be running a node that they sync with the network.

D. The verification system

Only verified people like colleges organisations can have the ability to verify documents.

4. Design and Implementation

Splitting the design into two parts

A. Client Side
B. Nodes Side

A. Client side

What basically happens in the client is that, when a user uploads a file into our system, the encryption system is completely executed in the user system only, and the encrypted data will be sent over the network which reaches the nodes in a completely unreadable form. [7]

B. Node side

On the node side all the encrypted data is collected and is stored on a k number of nodes so as to not waste much memory, the selection process of such nodes is the concept of minimum number of peers for a data block.

1) The Concept of minimum number of peers for a data block

This is a new idea that we have come up with so as to limit the number of peers needed for a certain amount of data on the network [8].Let us say we have n number of nodes in the network out of which we decide say k number of nodes which is the minimum number that is required to keep the data in a safe state. Now say out of these case states one node goes offline, and so the remaining will be K -1 and the network will automatically be fine and we find another node that is willing to be a peer and connect it to the database. We consider that this will be useful for examples like saving documents on blockchain and as you know that these documents usually have a large data size so it is practically impossible to save all the documents on all the nodes so we use this idea to limit the number of nodes for a particular set of data. This also will be useful in various other applications like the health data, machine monitoring resources etc.

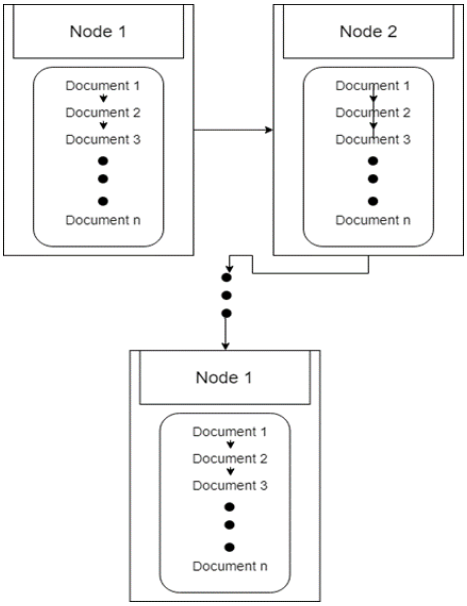

Fig. 1. Overall framework structure

5. Results

So as far as the results concerned it's been a difficult time understanding core of it to many people. People nowadays are so buzzed about Bitcoin, Ethereum etc. but the technology is not just limited to money. It has various other use cases also [10]. One of them that we have identified is documents. The applications of this tech is to be used in government management, record management, office files etc. are huge areas to look for.

6. Conclusion and Future work

There has always been a confusion whether as to use a centralised document storage system or a decentralized document storage system[11] for your application, the answer for this question is that it depends on the developer and they should decide whether or not to use it by analysing the type of operations that has to be done on the application service developing, so for an application High security, availability of documents 24x7 and immutable documents like real estate documents, school college certificates etc. of huge number of people.

References

[1] Bitcoin.org. (2018). Bitcoin - Open source P2P money. [online] Available at: https://bitcoin.org/en/
[2] En.wikipedia.org. (2018). Denial-of-service attack. [online] Available at: https://en.wikipedia.org/wiki/Denial-of-service_attack
[3] Anon, (n.d.). Blockchain - How to Store Documents or Files - Reskilling IT.
Available at: https://vitalflux.com/blockchain-store-documents-files/
[4] Anon, (n.d.). "Can Blockchain Solve Your Document And Digital Signature"

https://www.forbes.com/sites/oracle/2018/04/02/can-blockchain-solve-your-document-and-digital-signature-headaches/
[5] Anon, (n.d.). Document Certification through the Blockchain-Martin https://www.martinstellnberger.co/document-certification-through-the-blockchain.
[6] Anon, (n.d.). Dubai Wants All Government Documents on Blockchain by 2020 https://www.coindesk.com/dubai-government-documents-blockchain-strategy-2020/ [Accessed 2018].
[7] Anon, (n.d.). What is blockchain and records management - Iron mountain. http://www.ironmountain.com/resources/general-articles/w/what-is-blockchain-and-why-should-records-management-professionals-care
[8] dzone.com. (2018). Blockchain and Distributed Ledger Technology for Documents - Dzone Refcardz. https://dzone.com/refcardz/blockchain-and-distributed-ledger-technology-for-d [Accessed 30 Oct. 2018]
[9] Halaburda, H. (2017). Blockchain Revolution without the Blockchain. SSRN Electronic Journal.
[10] Technology for secure identity documents. (2008). Washington: U.S. G.P.O.