IX International Conference on Multidisciplinary Research
(IEI, Chandigarh) Institution of Engineers, India , Chandigarh
21st December 2019 www.conferenceworld.in
Conference World
ISBN : 978-81-943584-6-6

Document Verification Through The Blockchain

Prof. Hiren M Patel[1], Prof Rashmin Prajapati[2], Prof. Viral Patel[3]

[1,2,3]Assistant Professor, [1,2]Computer Engineering Department, [3]Information Technology Department, SVIT Vasad.

Abstract:-*The paper can illustrates how a Blockchain can solve the existing problem of verifying the validity of digital assets such as a birth certificate, a document stating your will or a signed legal document specifying a business deal very efficiently and at a very low implementation cost. This example also shows that the solution relies on a number of non-Blockchain-related technologies and the Blockchain is used only for a very specific task of storing digital signatures of assets that prove their validity. Due to the characteristics of the Blockchain permanent decentralised ledger of information, these digital signatures can be public so it accessed by anyone. Hence anyone with access to the Blockchain can now verify the authenticity of a digital asset without having to rely on trusted intermediaries.*

Keywords:-Block Chain, Certificate, Document, Decentralised,Fingerprint,Signature,Verification.

I. Introduction.

The Blockchain is a public ledger used to record all the transaction in a decentralized data log rather than a physical ledger or a single database. While blockchain technology was originally used to create cryptocurrencies, Nowadays blockchain is being promoted to different areas like trading, file storage, payment services, identity management, financial exchanges, medical records management, education and more[1].

Unfortunately, in today's world, fake documents are epidemic and as most of you know there is no trouble in getting fake documents[3]. As the fake documents precisely look like the originals, it is cumbersome for the layman to identify the real and duplicate. Service providers have to burn through millions to verify the documents of candidates.

II. Existing problem

Certificates distributed in colleges or universities are mostly in the form of hard copy. Whenever applicants apply for the job at any public or private sector they have to produce those hard copies, while the organizations have to verify all certificates manually which is very time-consuming process and there are chances that some may have produce the certificate which is not legit and that may get unnoticed by the verifier during the process because of this ineligible candidate will get a chance. There had been lots of cases in past where people are caught selling fake certificates of different organization at low cost.

Many business processes in government institutions and organisations alike require original documents to be provided for verification purposes before any further processing can occur. Since some documents (e.g. birth certificates) may exist only once, the parties involved may experience reluctance in handling these important documents as they could get damaged, lost in the mail, etc.

The friction is a result ofRequiring original documents to be presented to comply with the institution's signature and verification processes andThe reluctance by the parties involved of having the responsibility to protect these important physical pieces of paper throughout the process.

The question is how can we create a digital proof that a digital asset soft copy of birth certificate, Degree Certificate,legal document has been certified or signed by an authorised organisation or government institution and secondly, how can anybody around the world verify the authenticity of a particular digital asset without having to rely on a 3rd party orintermediary?

III. Solution

The solution proposed does not suggest to store the digital asset on the Blockchain this would be a very inefficient and expensive approach. Instead it only stores the proof that a digital asset has been certified or signed by an institution on the Blockchain. If anybody would want to verify the legitimacy of a digital asset they can simply verify the digital asset by vetting it using the proof provided[2]. Hence, the Blockchain's role in this solution is to provide an immutable storage container for these proofs[5].At a high level the proposed solution includes the following steps:

1.Creation of a digital asset and storage of the digital proof or signature to the Blockchain.

2.Transmission of the digital asset via Email, file sharing, etc.

3.Validation of the digital asset using the signature stored on the Blockchain and vetting of the institution that issued the asset.

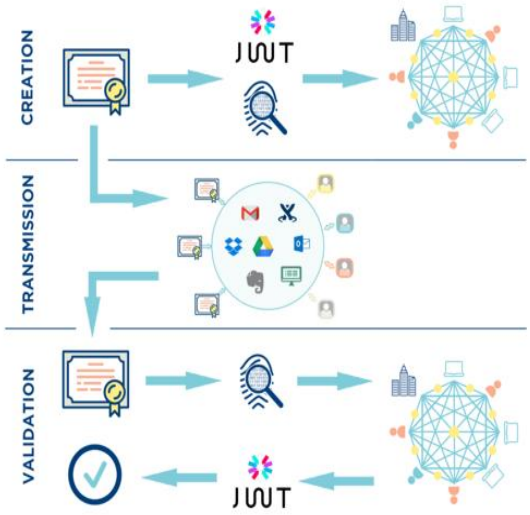

Fig.1 Flow of Document Verification

STEP 1: DIGITAL FINGERPRINT

Just like the fingerprint that is unique to a human being, digital assets also have a unique 'fingerprint'. To be more exact, a digital asset's fingerprint can be created by using so called cryptographic hash functions[11]. These

functions can take a file of almost any size like word, excel, pdf, image, etc as an input parameter to create a string of letters and characters its very unique fingerprint as an output.

However, this is a one-way process as it is not possible to reproduce the file from the digital fingerprint. There are a number of different hashing functions available for example you can use the MD5 hash algorithm[10].

STEP 2: CREATE A SIGNATURE

In the same way we can engage in a commercial contract by putting our 'unique' hand-writtensignature on a piece of paper, in Step 2, the digital fingerprint from Step 1 gets signed. In order to achieve this, Public-Private-Key-Pairs RSA Keys are required as

an input parameter for signing the digital fingerprint.One commonly used method to create digital signatures are JSON Web Tokens. JSON Web Tokens, an open industry standard commercial tool for generating and verifying tokens, are widely available and the process is very straight forward.

STEP 3: COMMIT FINGERPRINT AND SIGNATURE TO BLOCKCHAIN

In the last step, the digital fingerprint and the JSON Web Token Signature are 'uploaded' to the Blockchain. This is now the first time in this solution an interaction with a Blockchain is required[10]. It is important to keep in mind that not the digital asset itself but only the information about the asset its fingerprint and the signature get stored on the blockchain.

STEP 4: TRANSMISSION OF THE SIGNED DIGITAL ASSET

Using our existing ways of sharing information with tools such as email, online forms, file sharing platforms, etc., the digital asset can now be distributed to any party since it is a file like any other one. Note: There is no need to share the digital asset's fingerprint and the signature as they are stored on the Blockchain. Only the

digital asset itself should be shared.Any modification to the digital asset would also cause its digital fingerprint to change. As a result, the signature stored on the Blockchain would no longer match the digital asset's new fingerprint. Hence the new digital asset can no longer be considered as 'valid' as no corresponding signature exists.

STEP 5: DIGITAL ASSET VERIFICATION

The process for the recipient to verify the authenticity of a digital asset is similar to thesteps performed earlier starting with re-creating the digital fingerprint from the file that has been received. Next a request is launched to the Blockchain to retrieve the fingerprint's corresponding signature[13]. Lastly, 'apply' the RSA public key that corresponds to the RSA private key that has been used in Step 2 to verify the signature and consequently the validity of the digital asset.

STEP 6: CERTIFICATE PROVIDER IDENTITY VERIFICATION

The last step of the verification process is to verify if the institution that created this digital asset is a legitimate entity itself. Since anybody can create, sign and commit information to the Blockchain and pretend to be somebody else this is a very important step in the verification process[13]. This challenge has already been solved as well and it is called Extended Validation SSL where the certificate authority is required to conduct a thorough vetting of the institution by: 1) Verifying the legal, physical and operational existence of the entity and 2) Verifying that the identity of the entity matches official records among further checks[3].By using the URL that has been specified in the JWT we can now verify if and what SSL certificate has been provided by the institution behind this URL. This allows us to trust the legitimacy of the institution that created the signed digital asset in the first place.

IV. Conclusion and Feature Enhancement

This proposed solution illustrates how Blockchain technologies could be utilised to solve the problem of verifying digital assets. In this we had discuss basic problem of signature verification for document. We can also explore this problem with time stamping of signature so that they can expire like RC book, Driving licence that type of document has expiry date.

Now a day a storage is very expensive on the Blockchain, the goal is to store as minimal information as possible on the Blockchain. Hence, the URL and Keyid could be stored with Blockchain contract and not be part of the JWT.To optimise storage further, the JSON web token could be replaced with only the signed digital fingerprint. It is even possible to store the JWT off the Blockchain entirely.We can also Use interface base contract that establishes a standard for signed digital asset verification.

References:

[1] Satoshi Nakamoto, *"Bitcoin: A Peer-to-Peer Electronic Cash System,"* www.bitcoin.org.

[2] Hailong Yao, Caifen Wang, *"A Novel Blockchain-Based Authentication Key Exchange Protocol and Its Applications,"* 2018 IEEE Third International Conference on Data Science in Cyberspace.

[3] Marco Baldi, Franco Chiaraluce, Emanuele Frontoni, GuiseppeGottardi, *"Certificate Validation through Public Ledgers and Blockchains,"* In Proceedings of the First Italian Conference on Cybersecurity (ITASEC17), Venice, Italy.

[4] TareqAhram, Arman Sargolzaei, SamanSargolzaei, Jeff Daniels, Ben Amaba, *"Blockchain Technology Innovations,"* 2017 IEEE Technology & Engineering Management Conference (TEMSCON).

[5] Jiin-Chiou, Narn-Yih Lee, Chien Chi, YI-Hua Chen, *"Blockchain and Smart Contract for Digital Certificate,"* Proceedings of IEEE International Conference on Applied System Innovation 2017.

[6] W. Diffie, P. C. Van Oorschot, M. J. Wiener, *"Authentication and authenticated key exchanges,"* Designs, Codes and cryptography 2(2), 107-125 (1992).

[7] G. O. Karame, E. Androulaki, S. Capkun, *"Double-spending fast payments in bitcoin,"* Proceedings of the 2012 ACM conference on Computer and communications security, pages 906-917. ACM, 2012.

[8] T. Bui, T. Aura, *"Key Exchange with the Help of a Public Ledger,"* F. Stajano, J. Anderson, B. Christianson, V. Matyáš (eds) Security Protocols XXV. Security Protocols 2017. Lecture Notes in Computer Science, vol 10476. Springer (2017).

[9] Benyuan He, *"An Empirical Study of Online Shopping Using Blockchain Technology,"* Department of Distribution Management, Takming University of Science and Technology, Taiwan, R.O.C., 2017.

[10] ZhenzhiQiu, *"Digital certificate for a painting based on blockchain technology,"* Department of Information and Finance Management, National Taipei University of Technology, Taiwan, R.O.C., 2017.

[11] Xiuping Lin, *"Semi-centralized Blockchain Smart Contracts: Centralized Verification and Smart Computing under Chains in the Ethereum Blockchain,"* Department of Information

ISBN : 978-81-943584-6-6

Engineering, National Taiwan University, Taiwan, R.O.C., 2017.

[12] Yong Shi, *"Secure storage service of electronic ballot system based on block chain algorithm,"* Department of Computer Science, Tsing Hua University, Taiwan, R.O.C., 2017.

[13] S. Underwood, *"Blockchain beyond bitcoin,"* Commun. ACM, vol. 59, no. 11, pp. 15–17, 2016.

[14] G. Hurlburt, *"Might the Blockchain,"* no. April, pp. 12–16, 2016.