International Research Journal of Engineering and Technology [IRJET] e-ISSN: 2395-0056
Volume: 08 Issue: 04 | Apr 2021 www.irjet.net p-ISSN: 2395-0072

Storing Digitally Signed Document Using IPFS and Ethereum Smart Contract

Parag P Chinawale[1], Shobhana A Khedekar[2]

[1]*Student, Computer Engineering Department, Mumbai University, Datta Meghe College of Engineering, Navi Mumbai, Maharashtra, India*
[2]*Student, Computer Engineering Department, Mumbai University, Datta Meghe College of Engineering, Navi Mumbai, Maharashtra, India*

Abstract - *With the emerging digitalization, the risk for tampering of data has increased. Digital signatures are considered to be one of the aspects that require additional security. New emerging technologies could be apt to provide it with more secure methods of transmission and storage. Various algorithms are used to create digital signatures. When the output of an encrypted digital signature is integrated with Blockchain, it can be a promising technology for data storage and transfer that is both safe and secure. This research paper shows how the combination of Algorithms and Blockchain can be used to improve the future.*

Key Words: Blockchain, Digital Signature, Encryption, security.

1. INTRODUCTION

Stuart Haber and W. Scott Stornetta, two research scientists, first outlined blockchain technology in 1991. They decided to introduce a computationally feasible approach for time-stamping digital records in order to prevent them from being backdated or tampered with. Later in 2009, Satoshi Nakamoto created the world's most well-known cryptocurrency, Bitcoin, which is based on blockchain technology. From that very moment blockchain emerged into the world of digitization.

The use of blockchain to store data with a timestamp, as well as the complicated hash encryption used to connect the chains, establishes a data chain, allowing tampering with a single or whole chain more challenging.

This increasing success of blockchain turned several businesses such as Amazon, BMW, Credit Suisse, Google, and others to it for help. Blockchain has proved its utility in different financial services, strong security, transparency, and efficiency in the workplace.

With the rising prevalence of Blockchain alongside the emerging technology, Digital Signatures are employed all over the internet too. Digital Signature contains proof that all transfers were carried out solely by the real owner. Thus, the probability of manipulating a Digital Signature persists because it can be used as an authentic signature. As a consequence, the digital signature must be conveniently secured.

Companies all over the world are focusing on adopting new platforms to optimize business processes. The adoption of digital signatures provides an efficient and much more convenient solution, resulting in increased market growth. The following is a review of the digital signature demand according to PRESCIENT & STRATEGIC INTELLIGENCE:

Chart -1: Market for Digital Signature

Technological developments can be used to mitigate such attacks.

In recent few years, the drawbacks of digital signature are highlighted in aspects of storage of digitally signed documents. Storing of this data can be made easy and tamper-free using blockchain as a storage medium.

IPFS is a decentralized method of data storage. IPFS generates a hash from which the data can be located on the server. Every generated hash is unique.

Ethereum is a blockchain that can store data securely without getting the data tampered with.

A digital signature proves its owner's identity and he or she can't repudiate his or her sign. Digital Signature is implemented by public and private key algorithms and hash functions [3]. A digital signature can be created using the DSA encryption algorithm. The DSA digital signature is a pair of large numbers represented in a computer as strings of binary

digits. [2] The digital signature is computed using a set of rules (i.e., the DSA) and a set of parameters such that the identity of the signatory and integrity of the data can be verified.

The following java code is to generate a DSA digital signature.

```
public class CreatingDigitalSignature {
    public static void main(String args[]) throws Exception {
        // Accepting text from user
        Scanner sc = new Scanner(System.in);
        System.out.println("Enter some text");
        String msg = sc.nextLine();

        // Creating KeyPair generator object
        KeyPairGenerator keyPairGen = KeyPairGenerator.getInstance("DSA");

        // Initializing the key pair generator
        keyPairGen.initialize(2048);

        // Generate the pair of keys
        KeyPair pair = keyPairGen.generateKeyPair();

        // Getting the private key from the key pair
        PrivateKey privKey = pair.getPrivate();

        // Creating a Signature object
        Signature sign = Signature.getInstance("SHA256withDSA");

        // Initialize the signature
        sign.initSign(privKey);
        byte[] bytes = "msg".getBytes();

        // Adding data to the signature
        sign.update(bytes);

        // Calculating the signature
        byte[] signature = sign.sign();

        // Printing the signature
        System.out.println("Digital signature for given text: " + new String(signature, "UTF8"));
    }
```

Fig -1: DSA Algorithm Implementation

The above code is used to generate a digital signature using the DSA algorithm.

2. PROPOSED METHOD

Using IPFS the digitally signed document can be stored on the decentralized storage server which will create a unique hash code and the unique hash will be stored in blockchain. As the Ethereum blockchain is here used of integrity [4]. Each block in the blockchain contains a Unique timestamp. This mark serves as a source of variation in the block's hash and to avoid its manipulation smart contract is being used.
The basic proposed system is shown as follows:

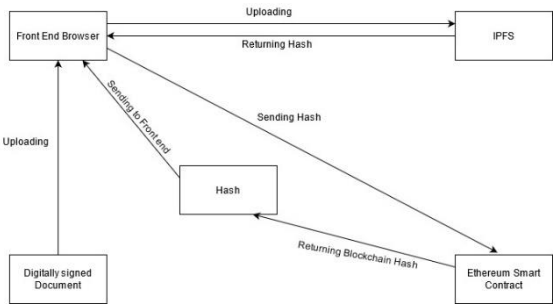

Fig -2: Flow of Proposed System

In the above flow diagram, the Digitally signed document is uploaded to the front-end browser for this Metamask chrome extension is used which is connected to the IPFS (InterPlanetary File System). After the upload of the file to the decentralized storage on IPFS, it generates a unique hash that can identify the file uniquely. This hash is sent to the front-end browser and then the browser sends it to the Ethereum Smart contract and saves the hash. This process is done at the backend of the browser. The blockchain generates a new hash of the block in which the hash generated from IPFS is stored. The generated blockchain hash is then sent to Front end browser. Whenever the file is called the hash that has been generated from the blockchain is fetched.

For providing an advanced level of security to the file, a digitally signed file can be password protected

3. RELATED WORK

Implementation of IPFS was for,[4] making data storage decentralized was implemented that would provide a better backup of data.

Digital signature is used, [1] from few previous years as a legitimization of document.

The various methods for [1] creating a digital signature are RSA, SBS technique etc. [2] The technique in the proposed system is using DSA algorithm.

4. CONCLUSION

With the increasing technology the main issue isn't the storage but the storing data securely is. This will help to retrieve data even if the user's server fails as it is a decentralized way to store data. The digital signature should be stored more securely as it contains the legitimation of the document. Storing the document on a third system by putting passcode on file makes it more secure.

REFERENCES

[1] [Aishwariya Mali, Chinmay Mahalle, Mihir Kulkarni, "Digital Signature Authentication and Verification on Smart Phone using CRiPT Algorithm", May 2017 International Journalism of Engineering and Technology.

[2] Hermina Alajbegović, Dževad Zečić, Hasan Jamak, "DIGITAL SINATURE ALGORITHM [DSA]", 10th International Research/Expert Conference" Trends in the Development of Machinery and Associated Technology" TMT 2006, Barcelona-Lloret de Mar, Spain, 11-15 September, 2006.

[3] Mehran Alidoost Nia, Ali Sajedi, Aryo Jamshidpey, "An Introduction to Digital Signature Schemes", Computer Engineering Department, University of Guilan-Rasht, Iran.

[4] Nishara Nizamuddin, Haya R. Hasan, Khaled Salah, "IPFS-Blockchain-based Authenticity of Online Publications", Department of Electrical and Computer Engineering. Khalifa University of Science, Technology and Research, Abu Dhabi, UAE.

[5] ABHISHEK ROY, SUNIL KARFORMA, "A survey on digital signatures and its applications", Research Gate January 2012.

[6] P. Morgan, "Using Blockchain Technology to Prove Existence of a Document", https://bravenewcoin. com/news/using-blockchain-technology-to-prove-existence-of-a-document/ last accessed 2018/2/20.

G. Zyskind, O. Nathan, A Pentland, "Decentralizing Privacy: Using Blockchain to protect personal data", Security and Privacy Workshops [SPW], 2015 IEEE Conference Proceedings, pp 180-184, San Jose, CA, USA [2015].M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989. R. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press. K. Elissa, "Title of paper if known," unpublished.