International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 01 | Jan 2020 www.irjet.net p-ISSN: 2395-0072

Proof of Document using Multichain and Ethereum

Malika Acharya

Master of Technology, Department of Computer Science, Rajasthan Technical University, Kota, Rajasthan.

Abstract - *In the past years, we have been hearing a lot about cryptocurrency and Blockchain which has brought new scope and technology into the hands of developers and common man. Blockchain technology was first introduced in a whitepaper which went like this : "Bitcoin: A Peer-to-Peer Electronic Cash System," by Satoshi Nakamoto in 2008.Though Blockchain being a completely new field, many companies are trying to implement Blockchain too. A Blockchain contains of a block which contains a hash of cryptography of the previous block, timestamp and transaction data*

***Key Words*: Multichain, Ethereum, Digital Signature. Hash, AWS, Ether token**

1. INTRODUCTION

Blockchain is one of the recent topics that have changed the whole scenario of transaction intermediation. The development of this has undoubtedly led to a complete different world of the cryptography chain blocks. It is a technology that allows transactions to be grouped in blocks and being recorded, allows the ledger to be accessed by different servers. The main player over here is the nodes made by connecting two or more systems. The main feature of this technology is information is distributed but not copied. Originally this was whole and sole for the tech community of digital currency but now its potential in other field is also tested. The two other features that come in forefront are first that there is no single point of failure and second that it can't be any one controller entity. It's highly durable and robust and though it's still in the development phase its addresses the two main requirements of transaction which are transparent and incorruptible. Accessible from anywhere this is the distributed ledgers which are private and centralized making the Blockchain distributed in nature due to its nodes. A distributed ledger proves transactions and facts by generating random but unique hash codes which can be checked afterwards that the file existed before. The basic idea of any large transaction with nodes and peer to peer computing is of the distributed and decentralized system and blockchain does not offer it rather it's the crux of the block chain. This decentralization is the very soul of the transaction done using blockchain. In today's world the transaction is considered as worth ongoing if besides being secured and authenticated it's also economic and no doubt blockchain assures that the peer to peer transaction happen in cost effective nature.

2. LITERATURE REVIEW

Multichain is attended only when two blockchain nodes connect but the connection is aborted when there is no desired result from the P2P connection. By default the transaction fees and block incentive is null but you can set these in param.dat file. We will build our tool using multichain where customers don't have to pay for using this service, it is free of cost and there is no scope of loss for us.[1] This will be providing a platform to all users to make their documents secure and which cannot be hacked by anyone. The main reason why the documents cannot be hacked by anyone is the documents are uploaded the node. [2] Only a unique hash code is generated for every document. To verify the document later, the hash codes will be matched and a perfect match means the document is original and genuine. Many more new and advanced definitions are being introduced in our Dapp where the transaction will be done using wallets and tokens, every newly registered customer will be provided a wallet and some tokens in it which they will use for every transaction. If someone is a one-time user and don't want to register then they can use our service by just paying the required ethers for their transaction. [3]. We shall be providing wallets to the customers where they can transact using our own build token using ethers. These tokens they have to buys from us which will be a type of virtual money. These ethers will decide how many documents the user can upload. Adding both of them to the picture has made the POE more efficient than all other POEs. This is because we are building our Dapp at a whole new level where we are combining two different platforms at a single place which no one has ever done.[4] The time related blocks organization gives the name blockchain. The transaction in the same blocks are known to be committed at the synchronous time but else the existence is considered to be ambiguous.[5] Wallet is the string of letters that appear as address in blocks of blockchain during a transaction where as the private key is a address field whose identity is covert. The mix of both these is actual criterion for the encryption forming the soul of blockchain transaction. Once the validity of the block is established its the transaction is rewarded a block and it's that stage where the information stored is considered to be the irrevocable.[6]. Using both Multichain and Ethereum to be implemented in the POE, the task is quite difficult to maintain the nodes. And mainly, we are building our tool using Ethereum blockchain where customers have to pay for using our service by the concept of virtual money.[7]

3. METHOLODOGY

3.1. TECHNOLOGY USED

The technologies used in the work are dived in two heads firstly Web and secondly the Services. The technologies used under each section are illustrated in the following section briefly

3.1.1. WEB

1 HTML

Developed by Berner-Lee it is the most widely used to develop web. It stands for Hyper Text Markup Language. Hypertext stands for the link in the document that allow the user to navigate to the other pages or other document smoothly and securely. Markup Language is the procedural communication of the presentation and computation between the computers. HTML is tag based language

2 CSS

CSS (Cascading Style Sheets) used in coordination with HTML is used to set the layout of the WebPages. Generally the separate CSS is preferred but now-a-days varied versions of the CSS are also available. The preference of separate CSS sheet is high and above because on requirement of any changes in the layout all you have to do is to access the CSS sheet and make the changes

3 Java Script

A lightweight/JIT complied language that is used when there is a need of the dynamic content and thus it is one of the 3 important languages that are needed for the webpage development. Starting from the animation to photos to any sort of dynamism in the webpage is the whole-and-sole stake of the JavaScript. It is prototype-based language multi-paradigm, dynamic language, supporting object-oriented, imperative, and declarative.

4 JQuery

A cross-platform JavaScript Library developed explicitly for the HTML scripting and document traversal, event handling and AJAX etc, for making things simple and easy with the handy API supporting variety in browsers and Operating System. JavaScript though an easy and handy yet a code intensive and comparatively lame. JQuery is thus considered a better option to make the layout of the pages more alluring and enticing

5 Bootstrap

A front end framework with high grid system and fast and speedy to support dynamic content on web based application. It aids in speedy loading and high responsiveness in the content. The basic advantages of the technology includes its high community support and customizable framework with a very low rate of browser bugs. Whatever may be the scenario, who ever may be the developer the bootstrap always provides consistent content in the dynamic frame

6 Scikit Learn

It is a library which is free software machine learning used in Python Programming. It is basically coded in python. But for performance issue it uses some algorithm which is written in **Python**. Python implements vector machine which is a wrapper around LIBSVM. It provides a variety of learning algorithm by means of a reliable interface in Python. Before using Scikit-learn we have to install a library which is built upon a SciPy i.e. Scientific Python. The Library is particularly on modeling data. To support Python 2.7 we need scikit-learn version 2.0.

3.1.2. SERVICES

1. AWS

A comprehensive cloud computing platform providing a services IaaS, PaaS, SaaS. In our work on we are using **Ubuntu 16.04 LTS.** Periodically upgraded by SmartAMI it provides a reliable, economic, confidential and secured environment for the development and deployment of the application. It is the responsibility of the SmartAMI to complete and fulfill all the dependencies that it requires. Since it's on AWS environment the work is run without any issues. Provided by Canonical Group Limited the product is secure and offers 29000packages to choose from repositories.

2. Git Bash

A Microsoft Windows environment provision that is an emulation layer for a Git command line experience. Bash stands for BOURNE AGAIN SHELL. A shell can be defined as a terminal application used to interface with an operating system through written commands. Bash is a popular default shell on Linux and MacOS. Git Bash is used as a tool for installation of Bash comprises of 2 parts:

- Git: A version control system (VCS) used to track file changes.
- Bash: A very common UNIX shell command line interface.

3. Multichain[8]

A perfect platform for the deployment of the private blockchain, multichain is supported by the Windows, Mac, Linux servers. Putting the simple API and command-line interface in the solution lineage it aims at the following:

- Making the blockchain activity transparent to selected participants
- Transaction controls being permitted
- Data mining is done securely and at a minimum costs

4. API by Slim Framework[9]

Slim was first developed by Josh Lockhart in 2013 since then this has been the most popular PHP framework that allows the developers to design the application easily and thus has proved to be the great competitor for other PHP frameworks like Larvel, Symphony, etc. There are certain pre-requisites that are imperative to begin with the framework:

i. PHP
ii. Composer
iii. Git

1. Composer

PHP has some dependencies that need to be sorted and Composer does the same by allowing the developer to attach the libraries needed. To quote this there is a difference between composer and package mangers like Yum or Apt. It does not do any installation in the global level but all it does is decide on the pre-work on basis. It very clearly allows the user to decide the libraries on which your work on depends

2. Libphp-multichin by Kunstmaan Labs.

To overcome the shortcomings of blockchain that count to limited capacity, irrelevant data, transaction costs, single asset this multichain fork solution was developed

3.2. METHODOLOGY

1. Proof of existence is the application that shall proof the existence of any particular document.

First we need to build a front-end for the work on using HTML, CSS, JS, jQuery & Bootstrap. Using the Bootstrap template , the front-end will be created which is of form structure requesting to provide user related information then a space showing file to generate POE, at that particular area we need to drag and drop the JSON file for which the hash code needs to be generated. Then by using jQuery, coding of SHA-256 Hash generator has to be done. The header.php file is created using JQuery which is included in the index.php file.

2. Working on AWS :

Create Amazon machine image of Ubuntu 16.04 LTS with in bound security group of – 1. HTTP TCP 80 SSH TCP 22 and outbound security group allowing all. Generating a new key pair and downloading it to connect with our AMI in future. Download git-bash and -ssh command is used for connecting our local machine with the instance. LAMP is installed on Ubuntu for web services.

3. Working on Multichain[10]

Creating a new blockchain based on Multichain's default parameters is the primary work and for this we first start the blockchain and then generate the genesis and block. Creating a stream (by creating stream we will be able to use some storage for storing and retrieval of data). Publish our first data using key and value.

4. Creating API

With this we aim to create an API format that is done using Composer. After downloading composer we install slim framework and then Xampp for the localhost. A demo is created and tested on the localhost to check get and post methods are working or not. On success of demo, libphp – multichain by kuntsmaan Labs is installed in slim framework

3.3. INSIGHT TO SYSTEM

1. Web interface

Web page is first insight to the paper. The language for designing the front page is javaScript. The page shows up the menu for various services.

2. Hash Code Generation

With the extensive use of the JQUERY we can easily develop the SHA 256 hash code generator purview that will generate a hash code and will provide the digital signature wallet so required.

3. Results

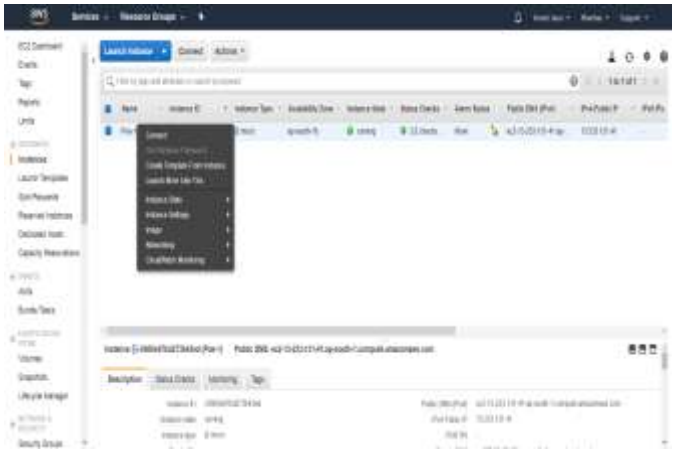

Fig1 : Setup Amazon We Services EC2 Instance with Apache, PHP, MySQL

Fig 2: Starting multichain(multichain [chain-name] -demon)(chain-name is the name of our multichain)

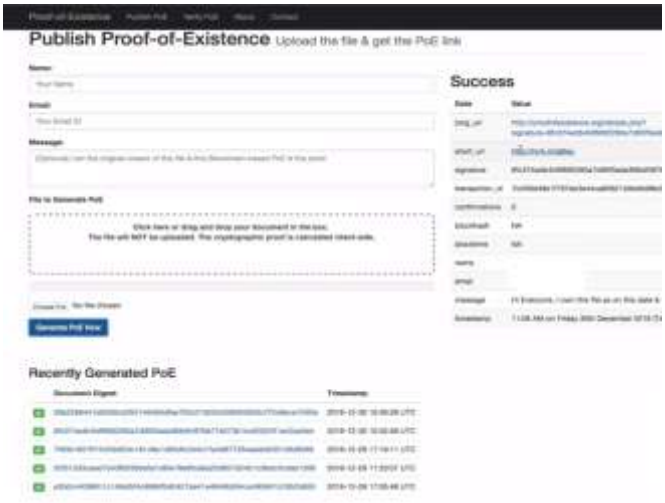

Fig3: API form

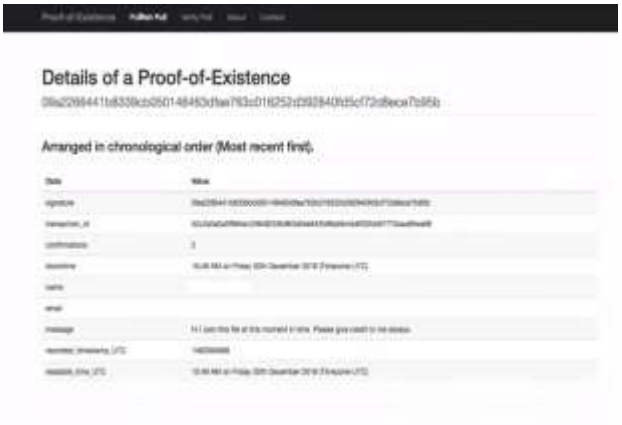

Fig 4: Digital signature generated

On creating a PoE we have will be able to see the PoE link and this will serve the purpose. The result so generated will be accompanied by the timestamp so that the user can check all the previous attempts chronologically with the served token. After uploading the document what is retained at the Ethereum end is the unambiguous proof of the document that serves the purpose of the work on and details the subject efficaciously. One can easily check the details of the generated signatures.

The work on embarks on establishing the consolidated proof of existence of the document in the simple process of matching the hash code and then generating a required digital signature using Ethereum and multichain.

4. FUTURE WORK

The future scope of the work on is vast and varied. The application can be used in different disciples and will be of worth. Some of them are discussed below:

i. Food supply chain using iot and machine learning: For checking purity of milk using Blockchain setting a benchmark for milk purity.

ii. In University/Colleges, verification of documents e.g registration, marksheets, certificates, etc. The medium through which the documents in Universities is removed. Faster verification is done and forgery of documents is prevented.

iii. In hospitals and clinics, verification of prescriptions, reports, patient's profile, etc. All types of reports are given a particular timestamp to record the time at which the patient is checked.

iv. In companies, industries, factories, all types of data. Customers, employees and all others have personal and work related data which needs to be protected and secured.

v. Land Agreements and all types of agreements. The third party for land agreements charges huge amount of money for settlements. POE can easily remove that because the document can be easily be verified by the help of POE.

Voting systems: Unique id can be generated having different timestamps can be used for voting. One vote can be casted from a unique id having a different timestamp. Thus from one id, only one vote can be casted which is uploaded in the Blockchain thus can be accessed with a key.

5. CONCLUSIONS

The paper aims to analyse the system and its utility in terms of real time models and baseline is the consolidated percepts of information provided.

The system of Proof-of-Existence using Multichain and Ethereum Blockchain is not only going to help people at all sectors but also a very useful service to common people. This work on can settle land agreements, rental agreements, all types of academic details of students of schools and colleges. It will make these types of data secure by its unique hash generation and its ability to connect itself through nodes

thus available almost all the time. Thus, this work on can be our biggest solution to various manual verification by officials and gazetted officers. This system will remove all types of third party involvement in all social and government matters in terms of records and documents.

The concept of tokens and ethers will also keep a count of the services being used by customers. As the Multichain service is free of cost, customers can try the service of our work on then make it more secure using Ethereum part of it. This system will create a huge revolution in industry where first we have to make everyone familiar with the Blockchain technology as very few people know about this emerging technology. Thus, this work may provide a kick-start to the many undiscovered technologies hiding beneath it[11]

REFERENCES

[1]. Yli-Huumo J, Ko D, Choi S, Park S, Smolander K (2016) Where Is Current Research on Blockchain Technology?—A Systematic Review. PLoS ONE 11(10): e0163477

[2]. Atzori, Marcella, Blockchain-Based Architectures for the Internet of Things: A Survey (2016).

[3]. Crosby MA, Pattanayak P, Verma S, Kalyanaraman V (2016) BlockChain Technology:Beyond Bitcoin. Applied Innovation, No. 2, pp. 6–10

[4]. Kim, Henry M. and Laskowski, Marek (2016) Towards an Ontology-Driven BlockchainDesign for Supply Chain Provenance. CoRRabs/1610.02922.

[5]. Sun J, Yan J, Zhang K (2016) Blockchain-based Sharing Services: What Blockchain Technology Can Contribute to Smart Cities[J]. Financial Innovation.

[6]. Xu J (2016) Are Blockchains Immune to All Malicious Attacks? [J]. Financial Innovation

[7].Mario Dobrovnik, David Herold, ElmarFürst and Sebastian Kummer Journal: Logistics, 2018, Volume 2, Number 3

[8]. Atzei, N., Bartoletti, M., Cimoli, T.: A survey of attacks on Ethereum smart contracts (SoK). In: Maffei, M., Ryan, M. (eds.) POST 2017. LNCS, vol. 10204, pp. 164–186. Springer, Heidelberg (2017).

[9]. Bhargavan, K., Delignat-Lavaud, A., Fournet, C., Gollamudi, A., Gonthier, G., Kobeissi, N., Kulatova, N., Rastogi, A., Sibut-Pinote, T., Swamy, N., Zanella-Béguelin, S.: Formal verifica tion of smart contracts: short paper.

[10]. Bartoletti, M., Pompianu, L.: An empirical analysis of smart contracts: platforms, applications, and design patterns

[11]. Nærland K, Müller -Bloch C, Beck R, Palmund S (2017) Blockchain to rule the waves—nascent design principles for reducing risk and uncertainty in decentralized environments

BIOGRAPHIES

Malika Acharya, is pursuing Master Of Technology in Rajasthan Technical University. She owns great interests in documents safety and is keen to learn newer technologies and integrate them to new and innovative projects.