Blockchain based Document Verification in Secure Cloud Network

Younis Wrdko Ahmed Mohammed, Department of Computer Technology, College of Science and Technology,Sabha,Libya
Osama Abdulla Elmahdi Elgahali, Department of Computer Technology, College of Science and Technology,Sabha,Libya
Melad Mohamed Salim Elfighi, Department of Computer Technology, College of Science and Technology,Sabha,Libya

Abstract—In the present world Internet and communication technologies plays a vital role and most of the people want to accumulate the features of it to accomplish their communication needs. Simultaneously, the present system of Government allows many scams and corruptions during over service claims for accident recovery claims, disaster recovery fund claims and so on. In this paper, a new concept is introduced with the integration of advanced technologies such as Communication, Internet and Security, which is achieved by means of Blockchain establishment. This Blockchain oriented systems are usually de-centralized, which gives Robust, Secure, Reliable, authentic, immutable and transparent service areas while any system oriented transactions. This paper concentrates on document verification schemes, which will be helpful for people who suffered due to disasters such as flood, earthquake and so on. Initially, this system expects the user to apply for the disaster recovery claim with proper proof, which will be verified by the volunteers and most of the volunteers giving acceptance to the respective claim means, that particular claim will be created as a 'Block' for future scanning purposes and the denoted claim will be released to the respective applicant without any manual interventions.The blocks are initiated by means of Genisis Block, which leads further blocks one by one as a chain nature such as Block1, Block2 and etc. The Miner Request and Verification process is the document verification process, which is cleared by the volunteers of the proposed framework. The identity of each blocks and the user maintenance into the proposed system is handled by SHA-256 bit hashing technique, which will provide the ultimate security level of the proposed system. These kind of disaster time claim management and document verification process is fully electronic and nobody can do scams over the system, so, that the proposed approach of document verification process using Blockchain concept is highly robust and secure to accomplish one's needs without any security issues, delay, manual flaws and interventions.

***Index Terms*—Blockchain, Document Verification, Genisis Block, Volunteer, Miner Request, Disaster Claim Management, SHA-256, HashingTechnique**

.

I. INTRODUCTION

Blockchain a concept was initially launched in 2008, and it is launched by Satoshi'Nakamoto. Initially Blockchain was used over Bitcoin-Currency oriented manipulations, which is also known as digital-currency. Blockchain has been adopted in various fields over further years slowly, mainly the Blockchain application is used in many commercial and non-commercial sectors such as Banking, Share Markets and many more [1][2][3][4]. Blockchain network is a de-centralized peer-network, which interconnects several information and maintains it as a block for further references. Usually the initial block over the Blockchain environment is named as a 'Genisis Block', from that the block will be incremented one by one such as Block-1, Block-2 ...Block-n. The chain nature creates a link between each and every block associated with the environment and each and every new block are double verified over the previous blocks while stored in to it. The

identity of each and every user is hashed and maintained into the server, so that the identity cannot be catched by anyone even the intruder may be a service provider.

The hashing algorithm we used in this proposed system is Secure Hash Algorithm (SHA) 256 bit, which will provide the ultimate key security feature and nobody can break it because of its uniqueness. This is the reason the intruders and attackers cannot guess the Blockchain series and links presented into it, that's why the Blockchain is still robust and secure compare to all other existing schemes [5][6][7]. Indian population crosses 134 Crore as well as with this high population, the cycle of giving and checking the recognizable proof documents such as Country-Passport, Adhaar-Card, PAN-Card, Voters-ID, and so forth of every single resident must be dependable, secure' and fast. The current frameworks set up are utilitarian, yet the efficiency and security should be improved as the cycle normally takes half a month and the residents applying for the records may need to visit the responsible position workplaces on different occasions to get records effectively. This isn't just awkward and time devouring yet additionally fiscally and platform worthy.

In this proposed paper, a new methodology is described to authenticate with high-security and eliminate the process of corruption during disaster recovery claim period by means of an advanced document verification scheme using Blockchain methodology. The most important of using such systems with Blockchain based document verification process and the volunteers' involvement with this system are clearly monitorinzed and described in detail over further chapters.

II. Blockchain and its Composition

A. Blockchain

The term Blockchain can be divided into two separate terms: 'Block' and 'Chain'. The term 'Block' contains a pre-defined set of records/documents/files, which will be marked by a unique identity. In some situations, the security enhancement norms hash the unique identity, so that nobody can crash the created block by means of its security. The term 'Chain' acts as a bridge, which interlinks two unique blocks one and another, usually the hash concepts are applied to generate the security norms for the generated blocks. Normally the algorithm called Secure-Hash is used, which is also known as 'SHA-256' bit algorithm [8][9]. The linking between these two is generated by the specified hash algorithm as well as the generated hashing is known as 'Chain'.

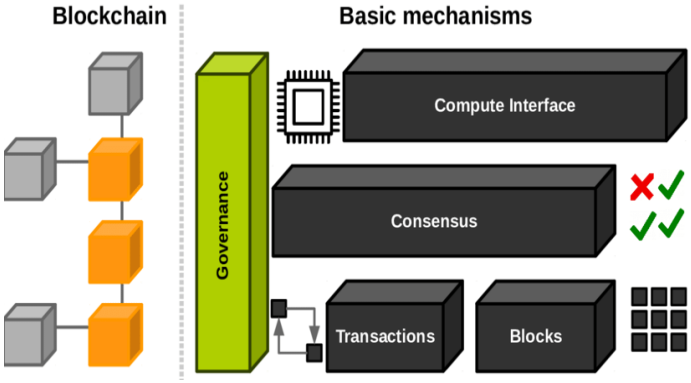


Fig.1 Overview of Blockchain Model

B. Nodes

Node is the storage-server portion of the Blockchain. The data transaction on the Blockchain are confirmed and stored to the chain by the identified nodes'. The nodes can be any sort of gadgets such as PCs, laptops, server-machine and etc, contingent upon the necessities of the chain. Every checked node has the transaction history of the whole chain and according to the theory; the Blockchain dwells on each node. Nodes play out the following capacities:

- Accept or reject transactions dependent on their legitimacy.
- Store records of the apparent multitude of transactions that occur.
- Broadcast substantial transactions all through the chain for different hubs to synchronize with the Blockchain.

C. Networking

In the networking norms, all the generated nodes are linked via Chain nature with one another and the specified networking-area is the place for all other items of the Blockchain.

D. SmartContract

SmartContract is a bit-code that sudden spikes in demand for a Blockchain. It works as a non-disavowal agent, implying that it locks both the parties in each transaction, so proprietorship cannot be blocked.

III. Problem Statement

In the regular scenario of document verification process, each and evry document need to be crosschecked by the person and report to the authority regarding the respective document. Once the document meets all the requirements and upto the satisfactory level, the document will be considered as a eligible document and it is moved for further clearance. In this scenario, one unavoidable problem is available, which is

known as corruption. The funds issued by the Government are only durable to its applicant, but the some Government officials charge some feasible amount for clearing that claim amount, from the applicant. The processing time and overall duration for clearing the amount to the applicant is lengthy, because manually one person from Government side need to visit to the applicant house and verify the documents and physical scenarios over there and provide the no-objection certificate to the applicant, that certificate need to be given to the authority for clearing the claim amount. In this case, the person who is coming to verify the documents over the applicant house/respective place charge some amount as much as they can for clearing the procedures. This situation raises a concern over the proposed system. First of all, the claims for disaster cases is purely given to the respective affected individual not for the Government officials.

The main motto of this application is eliminating these issues and proposes a new system which is durable in all cases and reduces the physical visiting scams over the applicant place/area. As well as the proposed system concern regarding the security issues over the claim releasing process. The proposed system need to concentrate more on verification process, because the process is manual means, the official can directly visit into the applicant affected area and cross-verify each and everything and provide the clearance certificate to the applicant. In this situation, there is no doubt in verification process, but while this system is come into online, then entire process need to be cross-checked twice compare to the manual process as well as the proposed work need to concentrate more on time management process. And security to the application and the application identity is more important compare to the manual process, only the applicant and system details should be visible only to the respective authority. So, that the privacy of the applicant and the corresponding application is highly preserved. For all the entire work of proposed system need more concentration in development of new system, which should be robust, fault-tolerant, fast in process, secured and reliable.

IV. Related Study

In the year of 2017 [10], the authors "Harry'Halpin.et al.," proposed a paper titled "Introduction to Security and Privacy on the Blockchain [10]", in that they described such as: Blockchain is an exploit, which reveals the power of terms in information technology industry such as security, novelty, robustness and reliable. This paper in major focuses on privacy and security, which is established over Blockchain network by means of analyzing the encryption-and-decryption problems. This paper considers the norms of Bitcoin schemes and usecases in general and analyzes the ways of security achieved over there in past [10]. The main advantage of the paper is solving the small issues presented over the Blockchain establishments over Bitcoin principles and which is also useful for establishing a smooth-bridge between academia and Blockchain-group.

In the year of 2017 [11], the authors "Aravind'Ramachandran. et al.," proposed a paper titled "Using Blockchain and smart contracts for secure data provenance management [11]", in that they described such as: Blockchain innovation has advanced from being a permanent record of exchanges for digital forms of money to a software-intuitive condition for forming solid applications. Despite the fact that, Blockchain innovation has been utilized to address different challenges, as far as anyone is concerned none of the past work centered on utilizing Blockchain to build up a protected and permanent logical information provenance the board system that consequently confirms the provenance records

In the year of 2017, the authors "IvanMartinovic., et al., [12]" proposed a paper titled "Blockchains for Governmental Services: Design Principles, Applications, and Case Studies[13]", in that they described such as: Blockchain innovation is the subject of exceptional and developing consideration among governments, innovation designers, and private financial specialists. The most unmistakable contemporary utilizations of Blockchain innovation are digital currencies, for example, Bitcoin. The exploration and organization of other functional applications stays restricted, nonetheless. The paper [12] contends that the Estonian-Governments' utilization of Blockchains to help public administrations shows the innovations' numerous points of interest. These favorable circumstances run from higher straight-forwardness to deal with proficiency to expanded security against different cyber attacks. This paper [12] likewise examines the innovations' expected application in different settings and nations where Blockchains are pulling in expanding government consideration and for which the Estonian-Experience offers conceivably valuable exercises.

V. Proposed Blockchain Document Verification Process

This paper concentrates on the real-time problem solving procedures. It concerns regarding the document verification process over natural disaster bounding. The people who are all affected by natural disasters are required to register into the proposed application, in which the authorization process need the details of the user such as Name, Mobile Number, Address and so on. This authorization process apply SHA-256 bit encryption logic to cipher the given identity and maintain it into the server, so, that the service provider even cannot access the records, because all we know the SHA algorithm is a uni-Directional encryption algorithm. With that the identity of user is managed over the server.

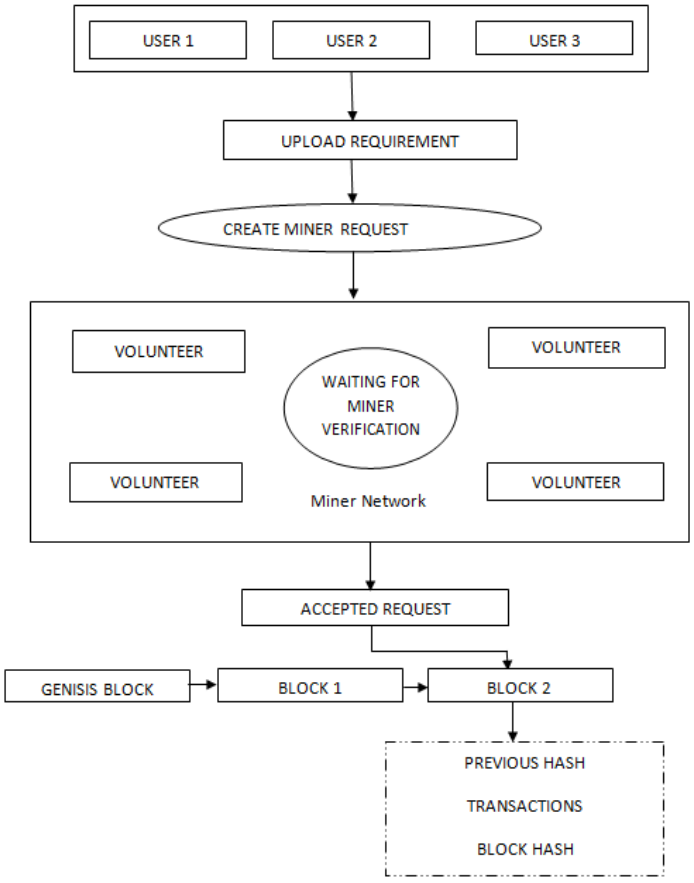


Fig.2Proposed System Architecture

The next step the user has to provide the affected area or material details with proper specifications, which will be practically proved over the results and discussion section with proper snaps of it. In this application user have to upload the affected portion image to the server that will be coming for verification. This user identity and the requested claims will be properly maintained into the server as a unique block and no one can duplicate with the created blocks. The concept of Blockchain is applied over each and every step of implementation and in which each block has a separate and unique identity key, which is also hashed by using SHA-256 algorithm. The block, which is created initially, is called Genisis Block and from this only the next blocks will be drawn one by one such as Block 1, Block 2 and so on. Once the user successfully registered his/her identity into the system and applied for the claim that will be moved to the authorities for verification.

The Blockchain procedure usually follows the architecture of 'Miner Network', in this case the proposed system invites volunteers to act as Miner logic, through which the verification processes are handled efficiently. The volunteers, who wish to join with this network, can register their identity to the application and the proposed web application forwards that request to the respective authorities. Once the authority give acceptance to the volunteer, that point onwards, the respective volunteer can do verification of nearby affected places and report them accordingly. The proposed system of verification process does not belong to single volunteer verification. Because if a volunteer verify the particular place and give no-objection certificate means, it is doubtful to others and which will lead again a corruption issues. Instead of that, the total volunteer count will be dividing into two and the majority will be considered as a result. Likewise more than half percentage of volunteers give result as successful verification means, that will be considered as successful claim request, otherwise that will automatically be rejected by the server. The verified identities and details are again summarized under a unique block, so, that the same user cannot be raising the same claim request for single disaster. Once these all process are cleared, the authorities can easily get to know which one is the proper claim request and which one is not. The same process of security enabling with Secure Hash Algorithm of 256-bit is handled over here to maintain the block unique identity to avoid the security issues over proposed system.

VI. Results and Discussions

The proposed system results are attained by using JavaScript web application and the backend handlings are done by using MySql server. The major portion of the results is highly tolerant and robust, which will be more user-friendly in nature and professional in look. The overall application is intended to provide a good solution to the document verification process and the Blockchain is a booster to give boom to the proposed system. Through the appliance of Blockchain concept and the security of SHA-256 bit hashing algorithm, the entire system is more beneficiary and attack free in nature. The following summary illustrates the proposed system results clearly with each and every step with proper system output design scenario.

The following figure, Fig.3 shows the authorization page view of the proposed system, in which it collects the respective user Name, E-Mail-ID, Mobile Number and Address as an input.

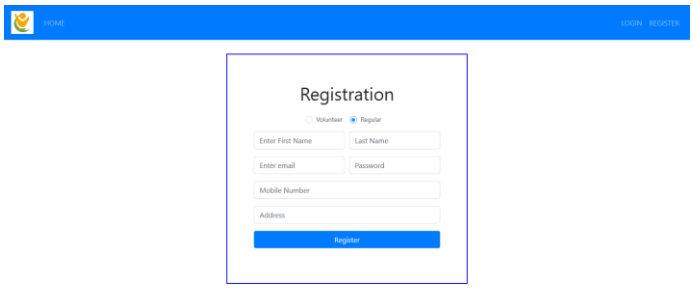


Fig.3Registration/Authorization Page

The following figure, Fig.4 shows the Login or Authentication page view of the proposed system. The registered users can login into the proposed system through this way and access the features available into the portal.

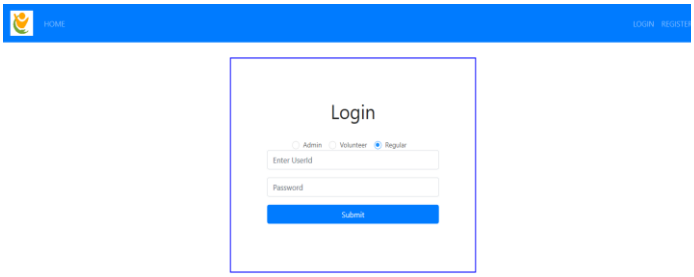


Fig.4Authentication Page

The following figure, Fig.5 shows the Document Uploading page of the proposed system, in which it collects the Place, Description and contact details from the respective user and upload those details into the server.

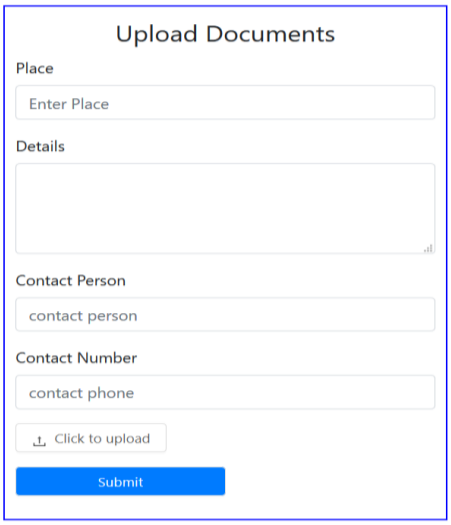
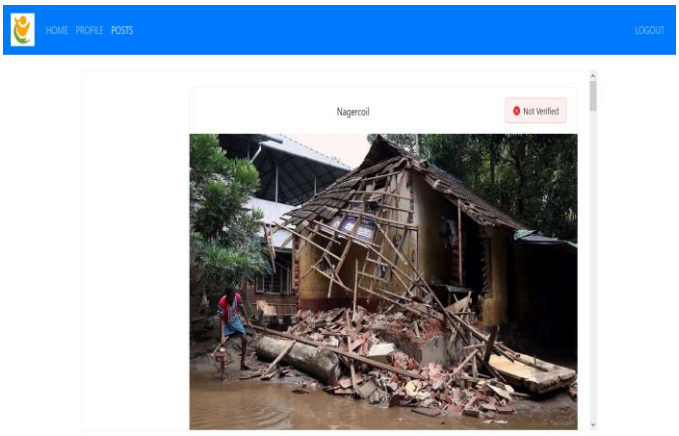
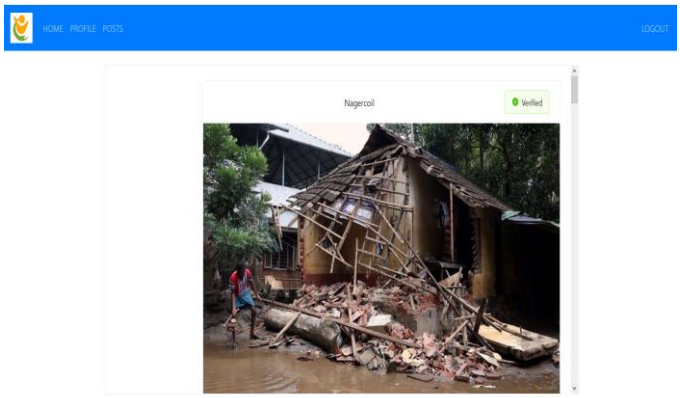


Fig.5Upload Documents to Server

The following figure, Fig.6 shows the Status of Request from the server to the respective user.



(a)



(b)

Fig.6Status of User Request (a) Not Verified and (b) Verified

The following figure, Fig.7 shows the Administrator Homepage view of the proposed system, in which it shows the available user details including volunteers to the administrator from the server.

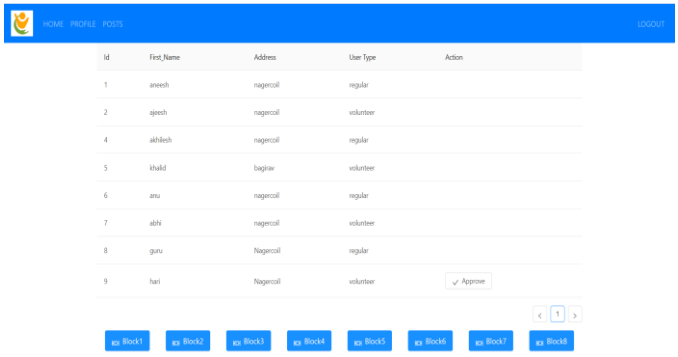


Fig.7Administrator Home Page

The following figure, Fig.8 shows the Block Content view of the proposed system, in which it shows the available contents in the block.

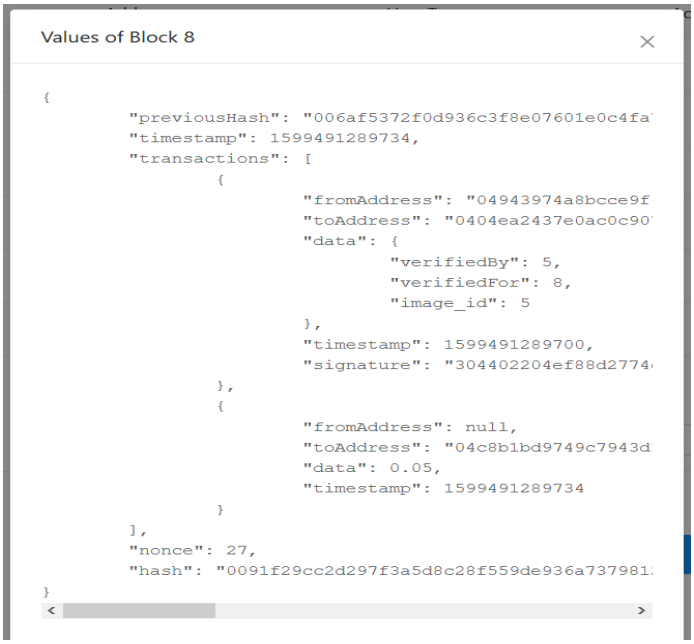


Fig.8Block Content

VII. CONCLUSION

Blockchain is the most admirable technology and it is highly utilized in all fields globally. The Blockchain application over public sector banks and other government sector scenarios shows the proof to its intelligence and robustness against vulnerabilities. This proposed system perfectly prove the concept of Blockchain based document verification process as well as clearly demonstrate the concept Miner Verification and Block establishments over the environment by using JavaScript Web Application with MySql backend support. By using this application, the user can submit the request regarding their natural disaster affections and easily claim the remunerations for that without any intervention. The volunteers' part is most important in this scenario, because based on their confirmation the total work need to be getting concluded. The security for the data and identities are handled by using Secure Hash Algorithm with 256-bit operating nature. The overall scenario of the proposed system clearly dictates the power and security of Blockchain based document verification process in detail and the results and discussion section shows the physical proof to its efficiency. In further the proposed system can be extended by means of adding or changing some security parameters such as AES or any related algorithm to enhance the robustness.

References

[1] Heng Hou, "The Application of Blockchain Technology in Egovernment in China",2017 26th International Conference on Computer Communications and Networks, ICCCN 2017.

[2] Weber I. Gramoli V, Ponomarev A, et.al., "On availability for blockchain-based systems", Proceedings of the IEEE Symposium on Reliable Distributed Systems (2017).

[3] Ahram T. Sargolzaei A. Sargolzaei S. et.al, "Blockchain Technology Innovations".

[4] Svein Ølnes and Arild Jansen , " Blockchain Technology as a Support Infrastructure in e-Government" , DUO 2017.

[5] Vipul H. Navadkar , Ajinkya Nighot , Rahul Wantmure "Overview of Blockchain Technology in Government/Public Sectors" , June 2018 International Research Journal of Engineering and Technology (IRJET).

[6] Parol Jalakas, "Blockchain from Public Administration Perspective: Case of Estonia", Tallinn 2018.

[7] Zibin Zheng , Shaoan Xie, Hong-Ning Dai, Xiangping Chen , " An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends", IEEE June 2017.

[8] Blockgeeks, What is blockchain. Last accessed: March 7, 2019.

[9] Coral Health, Start your own hyperledger blockchain, www.medium.com. Last accessed: March 7, 2019.

[10] Harry Halpin and Marta Piekarska , " Introduction to Security and Privacy on the Blockchain" , IEEE 2017 European symposium.

[11] Using Blockchain and smart contracts for secure data provenance management, Aravind Ramachandran and Dr.Murat Kantarcioglu, September 2017.

[12] Ivan Martinovic, Lucas Kello, Ivo Sluganovic , "Blockchains for Governmental Services: Design Principles, Applications, and Case Studies", December 2017 University of Oxford.