Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 12, December-2019

Survey on Trustless Crowd Intelligence Eco System Management using Block Chain

Ms. P. S. Patil[1]
[1] Dept of Computer Science and Engineering,
D.K.T.E. Society's Textile & Engineering Institute,
Ichalkaranji (An Autonomous Institute), India.

Prof. K. S. Kadam[2]
[2] Dept of Computer Science and Engineering,
D.K.T.E. Society's Textile & Engineering Institute,
Ichalkaranji (An Autonomous Institute), India.

***Abstract*— Block-chain is an innovative concept that involves two entities, the block, which is made up of data and the chain which is hash key. Every block contain reference of next block throw hash key. This process of chaining the data blocks together makes the block-chain network secure as it eliminates backtracking and tampering, as well as the transactions, are made transparent at the same time. The block-chain framework is a highly secure and advanced framework that can be utilized for various implementations other than the very popular crypto-currency. Due the nature of the system, a lot of random keys are being generated and this is very crucial for a system to maintain its space complexity, as the keys would exponentially increase in number and take up a lot of space. Therefore, the Key Space Complexity determines the number of keys being generated and if the key space is being managed efficiently, as the number of keys generated is directly proportional to the space complexity of the system.**

***Keywords*— Block chain, Hash key, Key Space Complexity**

1. INTRODUCTION

Block-chain is an innovative concept that involves two entities, the block, which is made up of data and the chain which is a concept that contains information and is responsible for the security of the data. The concept of block-chain is actually quite old and has gained traction very recently. The technique for block-chain was introduced by a group of researchers back in the early 1990s. The applications for block-chain at that time were envisioned as a timestamp for documents, this would prevent any problems associated with backdating as the block-chain would not allow that to happen, as well as reduce the tampering of sensitive documents which would allow for this service to be used as a form of a Notary. This is due to the immense security offered by the Block-chain technology, but it was largely unused as the world went forward with encryption and other techniques for security and block-chain on the most parts was ignored.

All of that changed when Satoshi Nakamoto decided to utilize the obscure block-chain to design a digital crypto-currency called Bit-coin. Bit-coin gained immense popularity due to its highly useful, tamperproof and resilient alternative to the Fiat Money. Due to the rise in popularity of the bit-coin, block-chain became the talk of the town. It brought back a lot of developers that were not even aware of this highly efficient system of block-chain. This resulted in a surge in researches that utilized the block-chain framework for various applications most of them centered on the crypto-currency essentially creating a revolution in the banking industry that is underway. The notoriety of the Bit-coin and other crypto-currencies has eclipsed the Block-chain framework, where most of the people believe that it can be used only for highly secure transactions using crypto-currency, but the block-chain is more than that, it can be used in a variety of applications other than crypto-currency. To leverage the benefits of the block-chain platform it is imperative to understand how this framework manages to secure the transactions highly efficiently as once the data is secured in a block it cannot be changed. The block in the block-chain is made up of 3 entities, namely, the data, the hash and the hash of the previous data. Taking the example of how bit-coin works, the data in a particular bit-coin network consists of transactional data, such as the sender, receiver and the number of coins transferred. The

Hash is like a fingerprint of the data, like metadata, that identifies the block and its contents. Whereas the hash of the previous block is the data of the previous block, this is how a chain of blocks is formed, called the block-chain. This process of chaining the data blocks together makes the block-chain network secure as it eliminates backtracking and tampering, as well as the transactions, are made transparent at the same time. All the blocks of data in the block-chain are similar to each other in composition, except for the first block which does not have a previous block and is called the Genesis block. The bit-coin framework also introduces a concept of proof of work that further prevents the corruption or tampering of data by putting a time limit of 10 minutes on each block. The proof of work is associated with the creation of hash which is imperative for a new block to be created.

The block-chain framework is a highly secure and advanced framework that can be utilized for various implementations other than the very popular crypto-currency. The data in the block-chain cannot be tampered or edited which is a requirement for a number of applications, such as storing medical records, collection of taxes or creating a digital notary. The secure framework of Block-chain is highly useful and can be used for a variety of applications.

2. LITERATURE REVIEW

B. Guo explained the concept of VCS (Visual Crowd sensing) that utilizes a collection of smart devices with inbuilt cameras and other sensors that are capable of deriving valuable information from the surroundings and various targets [1]. It was a subsection of the large sensing paradigm called the MCS (Mobile Crowd sensing) which faces a similar set of drawbacks such as high data

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 12, December-2019

processing cost, low-cost transmission data redundancy elimination, and identification, etc. Further he evaluate the Visual Crowd sensing, the authors have implemented a generic framework successfully. The main drawback of the study is that the generic framework was not tested significantly for performance evaluation.

K. Zhang introduced the concept of Internet of Things or IoT is a very innovative concept that could interconnect various devices with each other and the internet for some truly novel applications.[2] To connect the various IoT devices to the internet, a central Wi-Fi access point or a Smartphone is required. This is quite problematic for an average user and complicated for implementation. Therefore, the authors envision a low-power Wide-area IoT networks for the connection of the various Internet of Things devices to the Internet seamlessly. The main drawback of this technique is that it cannot accommodate the heterogeneous set of Internet of Things Applications.

J. Xu elaborated on the platform of crowd sourcing as a promising area of research as it is quite useful to achieve completion of massive tasks with the help of a large number of workers which are usually semi-skilled [3]. The authors in this paper have implemented a system that evaluates the workers based on indices, such as, platform improvement, latency, cost and Quality. The researchers have also deployed a system to incentivize the workers based on a reward or penalty system. This encourages the workers to achieve a better quality of work. The major drawback of this research is that it has not been experimented extensively to be subjected to analysis.

J. Jiang introduced the security threats associated with the UASNs or Underwater Acoustic Sensor Networks. There are quite a few attacks that could be utilized to compromise a UASN, such as the network layer being compromised with a DoS attack, the Data Link layer being subjected to a collision attack or the jamming attacks at the physical layer. Due to storage, communication and computational constraints of the UASNs, encryption is not a preferred choice for security. Therefore, the authors have presented a trust model based on cloud theory for the UASNs [4]. The major drawback of this technique is that it has been implemented in a simulation environment and lack real-time implementation.

X. Fan expressed the increment in the number of navigation applications and mapping services that have been particularly aimed at the mobile computation community. There has been an increase in the number of applications as well as devices capable of harnessing the Global Positioning System to provide navigation to its users on the move. The authors studied carefully and detailed the growth of the navigation industry as well as present a novel framework for a crowd-sourced road navigation system that can provide the much-needed impetus to the mobile community [5]. The major drawback is that the design has only been concentrated towards providing the last mile assistance to the users.

M. Wollschlaegar focused on the current trends in the area of industrial informatics and what is the future direction it seems to be going towards. The researchers stated that the industrial communication has seen a lot of growth recently and has been going heavily towards IoT (Internet of Things) and automation, as it can provide highly efficient results [6]. This is also heavily influenced by the crowd-sourcing as there has been a significant increase in industries that have been formed due to immense crowd-sourcing and have been highly successful in their business models.

P. Lindgren introduced the IEC 61499 is an integral part of control systems and is essential for the specifications of the distributed control systems. The IEC 61499 achieves this feat with the help of function block. As the function blocks have been specified for having a specified logical resource and interfaces, the end-to-end delay experienced varies according to the event. So, to reduce the end-to-end response time of the IEC 61499 the authors presented a low complexity implementation technique that can assess the delay and identify the network chains [7]. The major drawback of this technique is the increased computational complexity observed.

J. Kong [8] elaborated the increase in the generation and consumption of data in recent years which has been growing every day. The trend follows in the area of vehicular systems as well, where self-driving cars and enhanced driving safety have been inactive research and generating a lot of useful data. Most of the data is not able to be reciprocated between the researchers efficiently, which can hamper the research negatively. Therefore, the authors in this paper describe an innovative Data sharing model based on Block-chain framework in vehicular edge computing and networks. The major drawback of this technique is the increased time complexity of the system.

H. Liu introduced the concept of EVCE computing or Electric Vehicles Cloud and Edge Computing, as an innovative concept that can provide seamless connection to the vehicles in a heterogeneous wireless vehicular network. The networks have been increasing in popularity since the surge in the number of electric vehicles on the road. Therefore, the authors in this paper outline an innovative technique for implementation of block-chain in the network for securing the communications in the network [9]. The technique aimed to secure the inter-vehicular communications and the various connections to the cloud system susceptible to security threats. The major drawback in this technique is that it has not been implemented but applied as proof of determination.

Z. Li elaborated that there are a lot of hurdles in achieving a secure and transparent transaction with nontransparent and trustless energy markets in an Industrial Internet of Things network, due to the fact that it is a peer-to-peer network. It was a security risk while trading energy in a vehicle-to-vehicle grid network, energy harvesting networks and micro-grids. Therefore, the authors implement a Consortium Block-chain to enable secure transactions and communications between the various entities in the Industrial Internet of Things network (IIoT) [10]. The drawback of this technique is that it significantly increases the space and computational complexity of the whole system.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 12, December-2019

3. RELATED WORK

3.1 System Architecture:

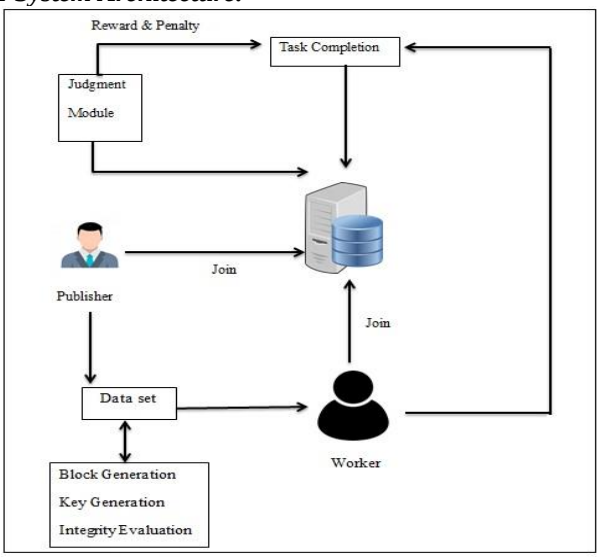

Figure 3.1 System Architecture

3.1.1 Data Transmission Key Allocation

Here in this step a transmission key is being created using the encrypted data from the prior step. It eventually forms the chain in between the blocks, which is secured and light weight.

3.1.2 Block cipher

Once the system is deployed, then the publisher is registered with the system by providing all his credentials. Then, based on the user credentials a synchronous key is generated with the help of MD5 hash key. In this process random characters are selected based on the hash key character positions and ASCII code summation technique by using MD5.

This Step feed with a plain text file to encrypt using the key generated in the last step. Once the plain text is received, It is along with the key is submitted to Reverse circle cipher algorithm to get the cipher text. This process divides the plain text into blocks of size ten and then they are constantly rotated based on the indices of the blocks. For each rotation of the blocks, public key K_{PUB} ASCII codes are summarized and then they are neutralized using the MOD function to replace with the characters of blocks by the other character.

3.1.3. Reward and Penalty Ranking

This incentive-based system is one of the most important modules of the proposed methodology. When a task is uploaded on to the platform by the publisher, the appropriate workers are authorized by the system to access the text file containing all the details of the job to be done.

The worker then follows the guidelines stipulated in the document and executes the task. After the completion of the task, it is judged by the Publisher if the job was completed satisfactorily or not. This is enabled by performing entropy estimation using Shannon Information gain. Higher the entropy indicates a better the performance of the job. Based on the entropy a reward or a penalty is levied for the worker by the platform. The entropy estimation is done with the help of the equation given below.

$$IG = -\frac{P}{T}\log\frac{P}{T} - \frac{N}{T}\log\frac{N}{T} \quad \text{_____(1)}$$

Where,
P=Publisher
T= Total number of likes/dislikes.
N= T-P
IG = Information Gain of the user

3.1.4. Job preparation through creation of blocks

The task to be accomplished is described in detail by the publisher in a text file. This text file needs to be encrypted before being uploaded to the platform. Thus this text file with the task is sent to the next module that performs the encryption.

3.1.5. Rank optimization

According to the various tasks allotted by the publisher and the quality of the work performed by the worker, a rank is issued to the worker. This is based on various parameters such as the completion of the work in the stipulated time and adherence to the guidelines outlined in the task. This rank is optimized at every instance of a job being completed for that particular worker. The Integrity of the block is also performed in this step for the accuracy and reliability of the data present in the block.

3.1.6. User interface designing

This methodology for the crowd intelligence system is proposed for a secure exchange of data and other resources between the stakeholders, namely, workers, publishers, etc. Due to the nature of the crowd intelligence platform, there is a very low level of trust between the publishers and the workers. Therefore, a secure interface has to be implemented to allow the interaction between the stakeholders. For this effect, an innovative interface is developed utilizing the Swings framework in Java with the following guidelines:

3.1.6.1. Registration:

This section deals with the identification of the users. On this platform there are various different users, such as publishers, workers, etc. All the appropriate users of this platform must be registered accurately.

3.1.6.2. User Authentication:

The various different users must be authenticated by the credentials given in the registration. This is necessary to maintain the security of the system.

3.1.6.3. Operations:

This section is very important because it outlines the different responsibilities and actions/operations every user can perform like, publishing the task, uploading the completed task, etc. This is based on their authority and tasks required to be performed on that particular user.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 12, December-2019

3.2. Experimental Evaluation

The proposed system uses a 8 byte secure hash key which is generated through the random function applied on the obtained hash keys through the block cipher data and block key. This eventually reduces the time and space complexity in handling of the whole process more efficiently.

6. REFERENCES:

[1] J. Mir et al, "Improved Two-Layer Backward-Compatible HDR VideoCoding: A Performance Comparison with Single-Layer HLG", IEEE International Conference on Consumer Electronics (ICCE), 2017.

[2] D. Kundu et al, "No-Reference Quality Assessment of Tone-MappedHDR Pictures", IEEETransactions on Image Processing, 2017.

[3] Y. Fand, H. Zhu, K. Ma, and Z. Wang, "Perceptual Quality Assessment of HDRDeghosting Algorithms", IEEE International Conference on Image Processing (ICIP), 2017.

[4] Y. Liu et al, "An Adaptive Perceptual Quantization Method for HDR Video Coding", IEEE International Conference on Image Processing (ICIP), 2017.

[5] M. Azimi, R. Boitard and M. Pourazad, "Performance Evaluation of Single Layer HDRVideo Transmission Pipelines", IEEE Transactions on Consumer Electronics, 2017.

[6] T. Vo and C. Lee, "Robust HDR Video Synthesis Using Superpixel-Based IlluminationInvariant Motion Estimation", IEEE International Conference on Consumer Electronics-Asia (ICCE-Asia), 2018.

[7] J. Mir, S. Talagala and A. Fernando, "Optimization of HEVC λ-domain Rate ControlAlgorithm for HDR Video", IEEE International Conference on Consumer Electronics (ICCE), 2018.

[8] Y. Mai and C. Chiu, "Patch-Based HDR Video Processing for FastMoving Object Reconstruction", International Conference on Computing, Networking and Communications (ICNC): Multimedia Computing andCommunications, 2017.

[9] H. Najaf-Zadeh et al, "VR+HDR: A System for View-Dependant Rendering of HDR video in Virtual Reality", IEEE International Conference on Image Processing (ICIP), 2017.

[10] A. Perrin et al, "Quality Assessment of an HDR Dual-LayerBackward-Compatible Codec Compared toUncompromised SDR and HDR Solutions", IEEE Transactions on Broadcasting, 2018.