iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** VII **Month of publication:** July 2019

DOI: http://doi.org/10.22214/ijraset.2019.7140

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue VII, July 2019- Available at www.ijraset.com

Survey on Privacy Preserving Technique of Blockchain Algorithm and its Data Structure

A. P. Shinde[1], A. J. Patil[2], S. S. Patil[3]
[1]*HOD, Computer Technology, BVJNIOT*
[2, 3]*Leturer, Computer Technology, BVJNIOT*

Abstract: ***Encrypted algorithm used is a decentralized technique. It has enough power to resolve any business related issues. Cryptography secures the records in a blockchain transaction and each transaction is tied to previous transactions or records. One of blockchain's benefits is its inherent resiliency to cyber-attack. While not immune to all forms of cyber risk, blockchain's unique structure provides cyber security capabilities not present in traditional ledgers and other legacy technologies. The distributed architecture of an algorithm rise, the resiliency of the overall network from being exposed to compromise from a single access point or point of failure. Also improve the overall robustness and integrity of shared ledgers. The Merkle tree structure also help participants with enhanced transparency, making it much more difficult to corrupt blockchains through malware. Blockchains hosted on a cloud platform, cloud data owners prefer to outsource documents in an encrypted form for the secure infrastructure. Also the foundation of Bit coin is using blockchain data structure and now it has received extensive attentions recently. In this survey paper of privacy preserving algorithm author point out the advantages and usage of it through existing approach. Lastly, the author discuss the structure and main features of block chain are like Decentralization, Immutability Faster dealings, Transaction and validation happens in seconds etc. In This Survey paper author has discuss one challenge that the relationship between data will be normally concealed in the process of encryption, which will lead to significant search accuracy performance decrease while the volume of data dramatic high. For such challenges author in this paper will suggest some innovate ideas to get the efficient end product outcomes.***

Keywords: cryptography, Blockchain, decentralization, consensus, scalability

I. INTRODUCTION

Today all folks were using advanced technology for communication through net. Voice call, video call, messages, pictures, are travel directly from one destination to receiver destination over the internet. For this transaction, between these sender and receiver, a trusted third party must be maintained. When it comes to cash transaction, individuals in the traditional scheme have to trust a third party to finish this. Because of its decentralized characteristics, Blockchain generates reliability and decreases the danger when searching for an unfamiliar party to enter into a company agreement[2]. The drastic rise in blockchain technology has created many fresh possibilities for implementation, including apps for healthcare [1]. The terms ' blockchain' and' distributed ledger technology'(' DLT') are frequently used interchangeably

Also suggest in [4] a method of securely embedding covert Blockchain messages. We formulate a simplified ideal blockchain model based on existing implementations and develop a protocol that allows two parties to communicate secretly following that model through the blockchain. We also formulate a strict definition on the basis of computational in distinguishability for the safety and coverage of such a protocol. Finally, we're demonstrating our technique satisfied this definition in the random oracle model for the underlying cryptographic hash function.

Blockchain-based applications are turning out, covering various fields together with money services, name system and Internet of Things (IoT), and so on.

The 3 kind of class blockchain reside are public, syndicate and personal. In Table 1 the class and Property are given; to that completely different class have their individual standing may be seen. However, there are still several challenges of blockchain technology like quantify ability and security issues waiting to be overcome [5]. Businesses that need high irresponsibleness and honesty will use blockchain to draw in customers. Besides, blockchain is distributed and may avoid the one purpose of failure state of affairs. The structure utilized by blockchain as a "Merkle tree," that may be an organization that mixes the hash values of transaction-level information into one "tree" that's hold on among the block and among ensuing block.

©IJRASET: All Rights are Reserved

Table 1
Comparisons among public blockchain, consortium blockchain and private blockchain

Property	public	consortium	private
Consensus determination	All miner	Selected set of nodes	One organization
Read permission	public	Could be public or restricted	Could be public or restricted
Immutability	Nearly impossible to tamper	Could be tampered	Could be tampered
Efficiency	Low	high	high
Centralized	No	partial	yes
Consensus process	Permission less	Permissioned	Permissioned

II. RELATED WORK

Here, we take few of the papers associated with block chain algorithm the usage of various main techniques and a number of them proven down.

A. Healthcare

Author in et [1] With higher perception into the deliver chain via right and timely authentication manner, pharmacies and healthcare vendors could be capable of make sure that the float of true drugs continues to reach the ones patients who want it the maximum. In this regard, block chainera holds an amazing promise for establishing a relied on community of vendors that allow healthcare

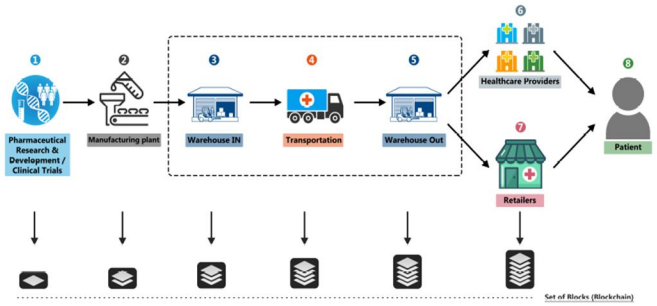


Fig.1 of deliver chain control by means of blockchain

administrators to defend sufferers from disreputable providers. Furthermore, block chain technology guarantees huge enhancement on demand forecasting, information provenance, fraud prevention, and transaction.

B. Method For Healthcare Supply Chain Management Device

1) *Step-1:* A block is created upon the discovery of a brand new medicinal drug or hospital therapy which includes patent safety and a long technique of medical trials. This statistics is recorded inside the virtual ledger as a shape of transaction.
2) *Step-2:* Once the scientific trial is a success, the patent is dispatched to the manufacturing plant for test prototype and mass production. Every product has its very own specific identity this is incorporated with every other transaction or block within the block chain consisting of different applicable facts.
3) *Step-3:* once the mass manufacturing in conjunction with packaging is finished, remedy is collected in a warehouse for future distribution. Records which include, time, lot wide variety, barcode, expiry date are blanketed inside the blockchain.
4) *Step-4:*Transportation records is likewise covered in the blockchain which might also consist of day trip from one warehouse (IN) to other, mode of transportation, legal agent, and other data.
5) *Step-5:* Third- party distribution network is commonly accountable for dispensing drugs and scientific elements to health care providers or stores. A warehouse (OUT) for every third birthday party is used for this purpose from where all distribution endpoints are related. A separate transaction is also incorporate into the blockchain.

©IJRASET: All Rights are Reserved

6) Step-6: Care vendors together with hospitals or clinics want to offer statistics, as an example, batch range, lot range, and product owner, expired date to authenticate, and prevent counterfeit. This is also covered in the blockchain.
7) Step-7: The moves taken with the aid of a store are just like Step-6.
8) Step-8: Sufferers are encouraged to decide authenticity during the whole procedure as blockchain deliver chain offers obvious records for verification to ability shoppers.

C. Internet of Medical Things

IoMT systems play a vital function in the improvement of health and clinical facts systems [13]. With IoMT era, health care equipment together with heart reveal, frame scanners, and wearablegadgetscanaccumulate,processand percentage information over the net in real time. for example, with the advancement of AI, healthcare providers, the use of the IoMT paradigm, can seize an photo, discover malignant elements or even suspicious cells, and percentage such information with the ones who have the proper to get entry to the facts. The subsequent sections difficult mostly on the progress in healthcare IoT and clever clinical gadgets in the AI arena. In Figure 2 is an illustration of IoMT in blockchain.

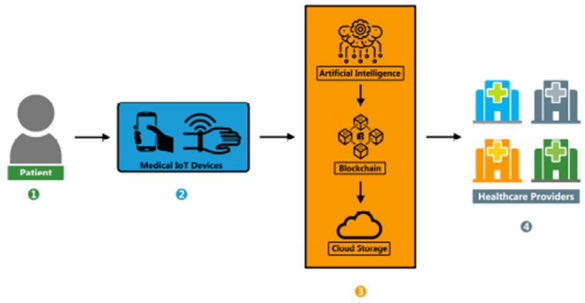


Fig.2 Internet of Medical Things (IoMT) in Blockchain.

1) Step-1: Inside the realm of IoMT, the patient is the source of all statistics.
2) Step2: Scientific IoT gadgets are normally either attached closely orremotely monitoring patients' body, consequently, generati ng big quantity ofinformation.
3) Step-3: Statistics generated in step-2 are stored on blocks or at the cloud garage. AI will assist blockchain to create wise virtual retailers, which in flip can create new ledgers automatically. In case of touchy scientific facts, in which safety is the first precedence, decentralized AI machine could help block chain to attain maximum safety [14].
4) Step-4: Healthcare companies are the end customers who seek get entry to for a safe and sound care transport which is legal by using the proprietor.

D. Search using Privacy Preserving Algorithm

Cloud Data owners choose to outsource documents in an encrypted shape for the motive of private ness preserving. Consequently it is vital to broaden efficient and reliable cipher textual content seek techniques. Creator in [6] discuss One challenge is that the relationship between documents might becommonly concealed in the technique of encryption, so onecanlead to extensive search accuracy overall performancedegradation. Additionally the quantity of records in records centers has skilled a dramatic growth. In Fig.3 architecture of cipher text search on cloud. It carries Merkle Hash tree records shape, HAC and K-means which are explain under.

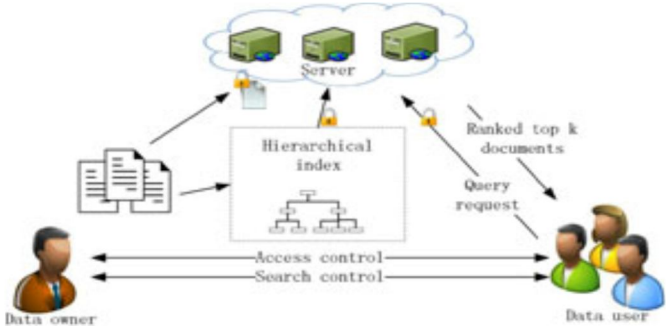


Fig.3 Architecture of cipher text search.

©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue VII, July 2019- Available at www.ijraset.com

E. Merkle Hash tree

Merkle tree (Hash tree) is a data structure that is used for data stored, handled and transferred data in and between computers. In fig.4 the secure scheme of the proposed system has been shown. The data are found of block are encrypted and chain by each other.

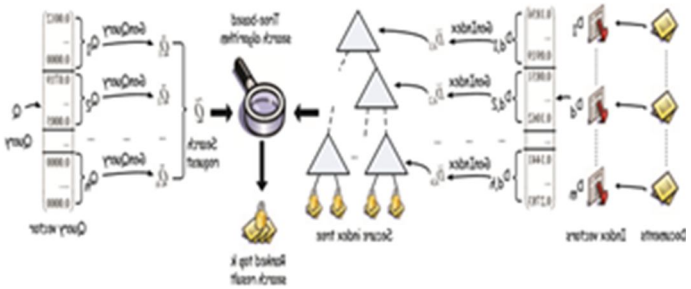


Fig.4 Overview of secure scheme

The encrypted hash index is create in tree form which is having top down approach and store the address of previous node and further node. The advantage of it is prevent from fault tolerance and integrity of data is maintain along with security.

F. Hierarchical Clustering Algorithm

Similar objects grouping into a tree of clusters. HAC classifiedas either agglomerative or divisive, depending upon whether the hierarchical decomposition is formed in a bottom-up or top-down fashion. In bottom-up approach the documents are merged and in top-down approach the documents are splitter.

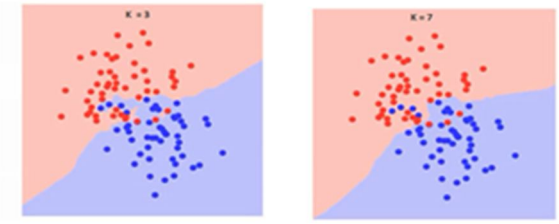


Fig.5 clustering process

K-means algorithm is used for clustering. Time complexity O (kn) Top-down approach used. Dynamic clustering creating is more costly. Searching takes more time. In fig.5 shows categorize and sorting of relevant data before and after using the flat clustering algorithm. Clustering process before k-means the top k ranking document is 3 and after the applying the k-means we can get the accurate and efficient result with top k ranking document result with 7 relevant document.

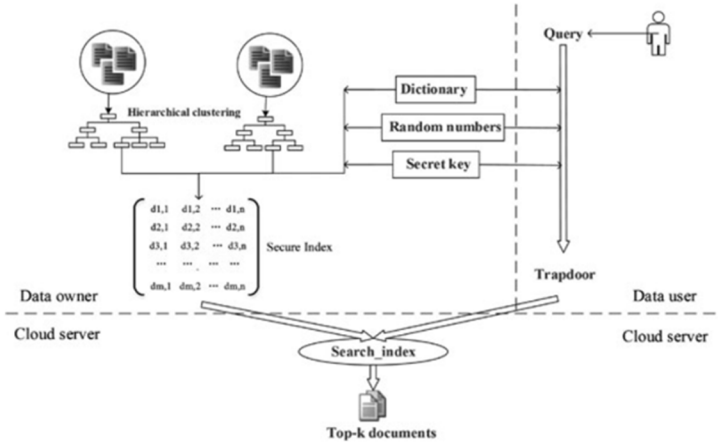


Fig: MRSE-HCI Architecture

©IJRASET: All Rights are Reserved

G. Process of Secure Search with Blockchain

1) The data owner, the records consumer, the cloud server.
2) The information owner has a set of data document F to b outsourced to the cloud server, there the cloud server encrypt it.
3) A licensed consumer acquires a corresponding trapdoor T via seek manipulate mechanism to search the report collection for t given keyword.
4) Upon receiving T from facts consumer, the cloud server is accountable to go looking the index I and go back the corresponding set of encrypted files.
5) For information user, the public key and the non-public key's provided on cloud server.
6) Enter seek question Q, break seek question Q in time period t (t1, t2…).
7) For every term t find cluster identity Cid (Cid1, Cid2,) and hash index (I) from database record F.
8) So that you can preserve control of encrypted index in cloud to keep away from fault tolerance the proposed gadget used merkle hash tree index in the direction of crypt record index facts.
9) Enter for seek arise via some keyword it provide the applicable and green top okay end result for search key-word report.

H. Block Chain for Financial Services Industry

Author in et [3] discuss the financial services industry stands to benefit tremendously from the growth of block chain given the technology's many financial services applications, including in effecting transactions and storing data in a more secure manner. As cyber threats to the industry continue to evolve in complexity and intensity, emerging technologies such as permission block chains can contribute to the important goals of combating cyber security risk and adequately protecting consumers' financial information and the integrity of the global financial system. Permission block chains offer significant cyber security capabilities, share some of the same cyber risks that affect other IT systems, and have unique characteristics, all of which merit further evaluation by regulators and industry. We encourage further conversation about the cyber security benefits of block chain systems and ways to encourage appropriate government policies.

III. STUDY ON SOME FEATURES OF BLOCK CHAINS

Characteristics of Public and Permissioned Block chains	
Distributed ledger	Contributors or "nodes" hold one or extra modern copies of the ledger on their structures. As facts are introduced to the ledger, the nodes acquire same copies of the updated ledger. the use of a shared, distributed ledger gives a measure of resilience by restricting the effect of a cyber security incident skilled with the aid of any unmatched node and stopping a single factor of failure from being used to disable the community, while allowing affected nodes to recover quickly from an incident by means of obtaining copies of the ledger held via other nodes.
Encryption	Block chains rely upon encryption deployed at several special factors in the network. First, player get right of entry to rights are managed via employing public/personal key encryption. Second, the transactional statisticsinsidea block is encrypted the usage of cryptographic hashes. Third, blocks of statistics are connected in chronological order in a block chain the use of a cryptographic hash feature that securely ties each block to the previous and subsequent blocks. For that reason, any try to adjust statistics inside a block would trade the hash values. Cryptographic hashing prevents statistics within a block from being changed without changing the history of all linked or chained blocks of facts. Consequently, could-be attackers focused on a particulartransactionwouldwanttoexchangethecompleteblockchaindue to this form of encryption.
Consensus mechanism or consensus validation procedures	A block chain's regulations setup approaches for validating the integrity of recent blocks of statistics earlier than they're added to the ledger. These guidelines are called consensus mechanisms or consensus validation strategies. In permission block chain, the proprietor members or coping with entity set up the policies for validating the integrity of recent blocks of facts before they are introduced to the ledger. In preferred, a certified player proposes a new block, and other nodes evaluation and verify that the proposed block satisfies network regulations. A mathematical or consensus algorithm monitors whether a precise number or percent of nodes have reached a consensus at the integrity of a proposed block. If the nodes attain a consensus, the new block is delivered to the ledger. Once brought, the new block and the data it contains are immutable. There are various fashions for consensus mechanisms, including evidence-of-work, evidence-of-stake, and evidence of-authority. Evidence-of-authority is the model usually used in permissioned block chains because it requires the events to have a few degree of consider, at the same time as the evidence-of-work and evidence-ofstake fashions do not assume such trust and are more usually used in public blockchains. Consensus mechanisms assist to make certain that new transactions introduced to the blockchain are confirmed by using members and not delivered fraudulently by using cyber-attackers.
Characteristics of Permissioned Blockchains	
Membership, access and participation restrictions	Proprietor-members of a permissioned blockchain setup policies regarding membership, get right of entry to, and participation rights, along with the standards for granting and terminating such rights. The proprietorcontributors typically delegate responsibility for imposing and implementing such policies to a handling entity and might authorize the handling entity to amend the guide line stocope withevolving conditions. Similarly to membership, get right of entry to and participation regulations, records on the network may be compartmentalized to save you intentional or inadvertent get right of entry tothesensitivecommercialandconsumerinformationofother contributors.

©IJRASET: All Rights are Reserved

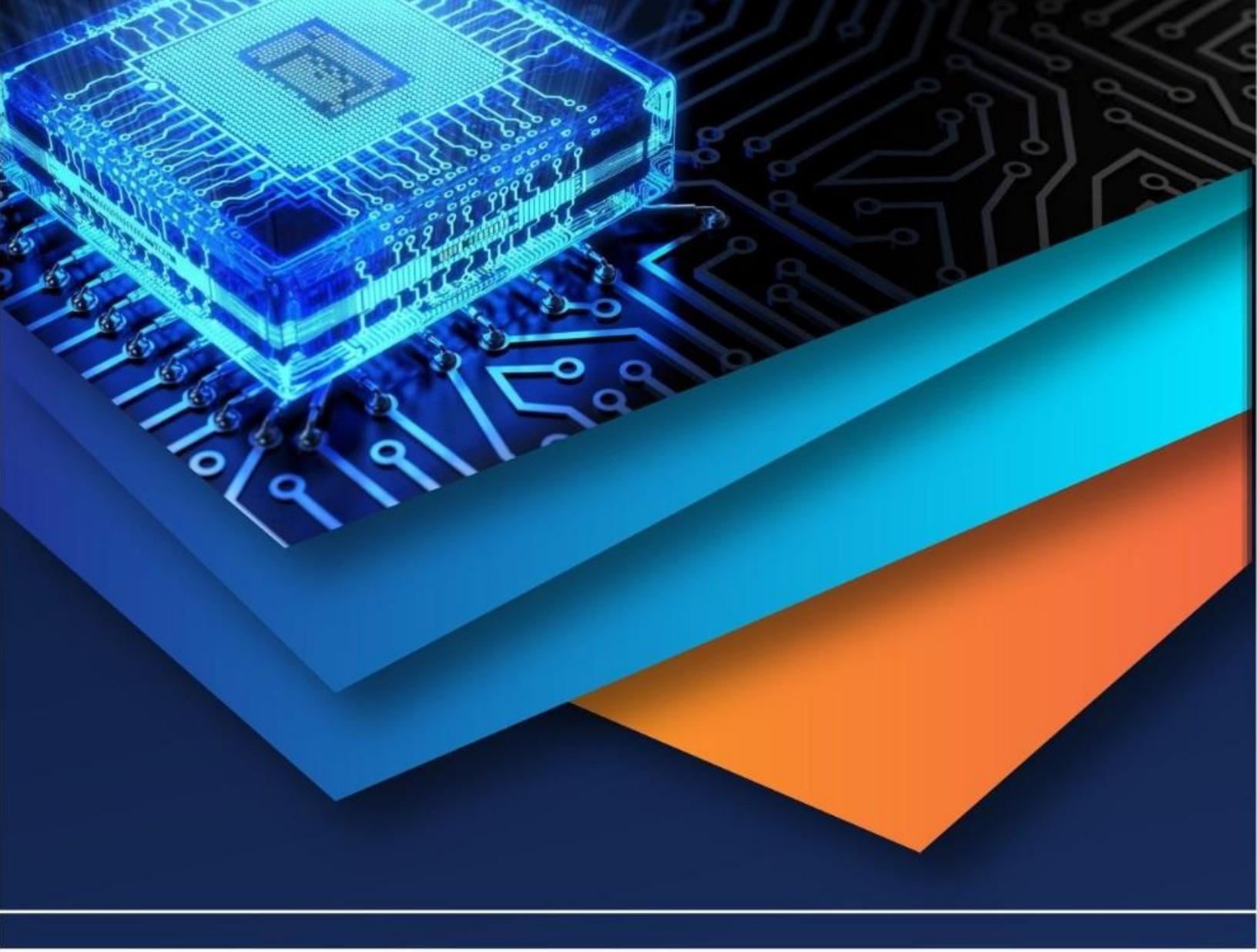
IV. CONCLUSION

Blockchain has proven its capability for reworking conventional enterprise with its key traits: decentralization, persistency, anonymity and audit ability. On this paper, we present acomprehensive overview on blockchain. We first give a top level view of blockchain technology consisting of blockchain structure and key characteristics of blockchain. We then speak the typical consensus algorithms used in blockchain. We analyzed and in comparisonthose protocols in specific respects. Furthermore, we listed a few demanding situations and issues that would avert blockchain improvement and summarized a few current approaches for solving these issues. A few possible destiny instructions also are proposed.Nowadays blockchain based applications are springing up and we plan to conduct in-depth investigations on blockchain-based totally programs within the destiny.

REFERENCES

[1] Seyednima Khezr, Md Moniruzzaman, AbdulsalamYassine and Rachid Benlamri "Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research" Received: 1 April 2019, Accepted: 22 April 2019; Published: 26 April 2019, Applied Sciences Journal, MDPI.
[2] Remya Stephen and Aneena Alex "A Review on BlockChain Security" 2018*IOP Conf. Ser.: Mater. Sci. Eng.* **396** 012030
[3] Erin English, MicrosoftAmy Davine Kim, Chamber of Digital Commerce, Michael Nonaka, Covington and Burling "Advancing Blockchain Cybersecurity: Technical and Policy Considerations for the Financial Services Industry" whitepaper © 2018 Microsoft Corporation.
[4] JuhaPartala "Provably Secure Covert Communication on Blockchain"Received: 29 June 2018; Accepted: 13 August 2018; Published: 20 August 2018 crytography MDPI Journal.
[5] Zibin Zheng1, Shaoan Xie1, Hongning Dai2, Xiangping Chen4, and Huaimin Wang3 "An Overview of Block chain Technology: Architecture, Consensus, and Future Trends" 2017 IEEE 6th International Congress on Big Data.
[6] Chi Chen, Xiaojie Zhu, Peisong Shen, Jiankun Hu, Song Guo, ZahirTari, and Albert Y. Zomaya, "An Efficient Privacy-Preserving Ranked Keyword Search Method", IEEE, 2016.
[7] W. Sun, B. Wang, N. Cao, M. Li, W. Lou, Y. T. Hou, and H. Li, "Privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking", ACM, 2013
[8] N. Cao, C.Wang,M. Li, K. Ren, W.J. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," IEEE, 2011.
[9] D. Cash, S. Jarecki, C. Jutla, H. Krawczyk, M. Rosu, and M. Steiner, "Highly-scalable searchable symmetric encryption with Support for Boolean que-ries," in Proc. Adv. Cryptol, Berlin, Heidelberg, 2013, pp. 353–373.
[10] S. Kamara, C. Papamanthou, and T. Roeder, "Dynamic searchable Symmetric encryption," in Proc. Conf. Comput. Commun. Secure 2012, pp. 965–976.
[11] Santosh I Halpati, D.M.Thakore "Search For Given {Object Set} Based On SpatialLocation From User Query" Volume-2, Issue-12, Dec.-2014, International Journal of Electrical, Electronics and Data Communication, ISSN: 2320-2084.
[12] Santosh I Halpati, D.M.Thakore "Categorize and Efficient: Top k keyword Search of Spatial-Textual data on the Road Network"ISSN:0975-9646, Santosh.I.Halpati et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, 3843-3847.
[13] Chiuchisan, I.; Costin, H.N.; Geman, O. Adopting the internet of things technologies in health care systems. In Proceedings of the 2014 International Conference and Exposition on Electrical and Power Engineering (EPE), Iasi, Romania, 16–18 October 2014; pp. 532–535.
[14] Decentralized AI: Blockchain's Bright Future. Available online: https://espeoblockchain.com/blog/decentralized-ai-benefits/ (accessed on 20 March 2019).

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)