iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: YNERGY2018 **Issue:** 2 **Month of publication:** April 2018

DOI:

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 :6.887
Available at www.ijraset.com
SYNERGY-VIT University, Vellore

An Analysis of Use Cases of Blockchain and Trust less Communication Systems

Sangarshanan.V
Computer Science with Specialization in Bioinformatics, VIT University Vellore

Abstract: ***Before the Internet era began we had Usenet wherein the users had to run their own servers in order to communicate and as internet came along a decade later one had to host their website on the server they owned and had to buy a DNS domain to point to their website creating a decentralized system, though this provided privacy which no one expected back then it was also incredibly expensive and hence came the hosting services which promoted a more centralized system which was quite frankly more efficient and cheaper at that time. Centralized systems were more convenient to users but as the number of users kept multiplying it gave immense power to the corporations that own these centralized systems. These corporations own loads of user data and control the internet with the power to influence everything we see and do online. The recent developments in the Blockchain technology have given us a chance to bring back the decentralized systems and it is currently being used by cryptocurrencies and in fintech but with more research blockchain could transform various technological aspects of our life including our government and the current healthcare system. I personally believe that blockchain will pave the way for a new internet where we control our data.***

Keywords: Blockchain, decentralization, ethereum, IPFS, data security

I. INTRODUCTION

Computers and technology have become a part of almost every profession in the past decade and with new advancements and new inventions, it has become essential to stay up to date. As we move forward it becomes impractical to rely on a single technology and so it becomes essential to find a common ground where two or more technological advancements can be combined for a higher purpose. Combining the advancements in the Internet of things, Machine learning, Artificial Intelligence, Big Data and Blockchain can potentially disrupt a lot of industries. It all began with data, accumulation of tons of online data seemed useless at first but slowly corporations started mining these data and discovered incredibly useful hidden treasures but it was like finding a needle in a haystack and thus came big data to help with the problem. Now, this data can also be collected from sensors which can communicate with other devices to give us a smart output. Machine learning and AI make use of this data as training data and have already disrupted the fields of computer vision, speech detection, and natural language processing. We can see that everything stems from data and this data is stored in a centralized manner which becomes a liability and hence we turn to blockchain based decentralized systems.

II. DECENTRALIZED DATA

There have been several advancements in various technological walks of our life in the recent years making our lives easier and simpler. Let me take e-commerce as an example, initially we did not trust these websites as the quality of the product cannot be tested or predicted by the buyer before the transaction is over and the user had to blindly trust the seller on the details of the product but as time went by people found it more convenient to just order their items online because time increases trust just like with people, the more we know a person the more we trust them. Thus these websites gained immense popularity and the more it was being used the more the trust builds up. Initially, these websites had a fairly simpler business model but as the number of competitors and the number of buyers substantially increased these corporations had to come up with better strategies. The advancements in big data and machine learning facilitated the usage the tons of user data collected continuously. The user data collected is analyzed using machine learning algorithms and recommendations are made based on the result. These corporations display the recommendations not only on their websites but also on other websites we tend we visit by monitoring our search activities on a daily basis and by paying other websites for user data. As the number of users increases data becomes more and more valuable to companies. We can only assume what they do with all the abundant data. There has already been a lot of conspiracy theories saying that big corporations use their data and target a particular demographic to manipulate them remotely and get their job done. There have already been several accusations that tech giants have manipulated users for years and have influenced politics,

elections, wars and even our day to day activities. Invasion of privacy has become a major concern for the people since whistleblowers have exposed a ton of illegal exploitation of user privacy. Everyone wants control over their own data and Blockchain can provide users this control and the ability to carry out activities online without fear. User data is controlled by the user and not anybody else. Data is like nuclear energy, productive when harnessed right but when it is misused can lead to huge disasters.

III.BLOCKCHAIN

A Blockchain can be simply defined as a glorified linked list, it is a continuous list of growing records called as blocks. Blockchain can be defined as a shared or a distributed ledger. This technology is still in its infancy and it currently offers strong use cases in fintech. But the more we discuss this concept the more we can understand that this technology could potentially transform many industries and even change the internet as we know it. Blockchain-based trading has gained immense popularity as blockchain removes the need for a middleman and because there is no middleman we can directly trade with individuals which not only increases profit but also ensures privacy and security. Let me illustrate Blockchain trading with the example of export transactions, if we want to export a product to another country then there is a lot of paperwork involved with messy procedures and the problem is that if one person has the paperwork we have to wait until the person has finished editing and also there is a problem with currency exchange which changes continuously but with the introduction of Blockchain all the transactions are distributed and open such that a single version is visible to all the actors involved in the Blockchain and the introduction of a cryptocurrency mitigates the hassles of currency exchange. The data is also safe as a decentralized system does not have a single point of failure i.e. data is replicated on every block of the Blockchain ensuring immutability of the data stored. This is only one of the many advantages of switching to a Blockchain based system.

A. The Basic Model

The blockchain is nothing but blocks of data that are spread across computing systems and connected by cryptographically secured metaphorical chain links forming a peer to peer network. Each block contains a digital signature, a timestamp, the hash of the previous transaction (except the genesis block) and relevant data depending on the purpose of the Blockchain. A digital signature is made up of public and private keys which form the identity of the user and are necessary to establish communication. Private keys (private) are used to sign and validate transactions whereas public keys (distributed) act as the address of the user initiating the transaction. Hashes in Blockchain is a representation of its current state and Hashing provides a way for everyone on the Blockchain to agree on the current state. Digital signatures are generated from the hash and it can be used to verify the authenticity of any particular data on the Blockchain.

The first hash is calculated for the first block or the Genesis block using the transactions inside that block and from then on each block contains the hash of its previous block along with its own hash so that if a block is altered, then its hash is altered ensuring that all the other blocks are alerted. A hash function is used to generate hashes and generally produces a 128 or 256-bit output depending on the hash function used. Hashes are what link the blockchains with one another forming a peer to peer network. These links are secured using cryptography. Ethereum has added the concept of smart contracts to the blockchain technology. Smart contracts are a way to perform actions by the rules defined in the contract. While bitcoin is just a decentralized currency platform, Ethereum scaled up by building the remix ide for building decentralized applications which can run without middlemen. Ethereum is a programmable blockchain.

The smart contract was introduced by ethereum and is basically just a piece of code which defines the conditions that need to be satisfied by every user in the blockchain. The smart contract is present on all the computing systems in the network and they all must execute and get to the same result. This way users can be sure that outcome is correct. Smart contracts are written solidity, a contract-oriented programming language developed by ethereum.

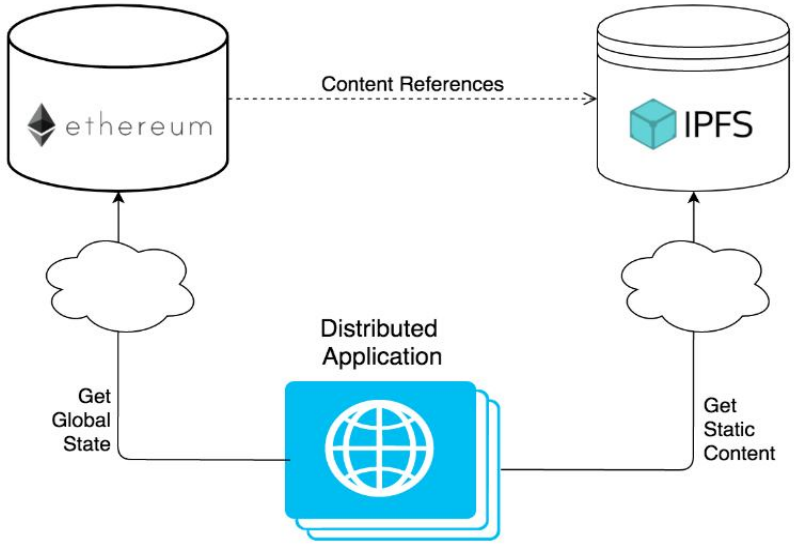
B. Interplanetary File System

Though ethereum provides a platform for developing decentralized applications, it is impossible to store all the data generated in an ethereum blockchain. There is no central server as the data is decentralized. IPFS acts as a server for blockchain but it is peer to peer and decentralized. IPFS uses bit swap a method heavily inspired by the BitTorrent protocol, where a user can discover nearby peers to share data with and when the user needs data, he has to download many small bits of it from several peers thus ensuring that there is no central entity controlling all the data. IPFS uses a Merkle DAG data structure which draws inspiration from the git protocol, Merkle DAG uses a series of nodes connected together as a directed acyclic graph to give structure to the entire network. The data

from the nodes are content addressed and not IP addressed. An IPFS is a distributed hash table which gives out a content hash that is stored in a blockchain.

The data is mapped based on content and is hence secure, unlike IP addresses which can be easily used to track the user. IPFS (peer to peer hypermedia protocol) solves many bottlenecks faced by HTTP (hypertext transfer protocol) and it has the potential to bring about internet democracy.

Decentralized hosting with IPFS also provides many practical benefits by making our content is resistant to DDoS attacks and censorship while maintaining zero downtime. Time has proven that even popular cloud-based hosting services like AWS cannot ensure zero downtime (AWS S3 outage). IPFS is a gateway to a more secure and uncensored internet where no voice can be silenced. It lays the foundation for a permanent web.



IV. ANALYSIS OF USE CASES

A. Healthcare

Healthcare is one of the industries where we cannot afford to make mistakes. Patient history is stored in databases by hospitals and these databases have a central point of failure and moreover, these centralized systems are prone to security breaches, moreover different hospitals use different database systems. Even a small mistake in patient history could mean death. A blockchain based healthcare system would convert the databases an open ledger which is immutable, decentralized and easily accessible. Electronic Medical Records is an IoT gateway that connects the caregiver and the patient to the underlying Information Systems.

The existing IoT systems depend on centralized systems and fairly old communication models which are not entirely reliable. Even a second gap in the communication of information could mean death to the patient. The present IoT based healthcare also depends on central servers which are extremely expensive with tons of maintenance costs. As the connections of various IoT devices that monitor a patient's real-time medical data increases, the entry points for hackers also increase.A decentralized blockchain based system can act as a viable solution to almost all these problems by providing a trustless peer to peer communication system that shares its data among the nodes in the network (distributed open ledger)

The patient prescription is also a very important kind of data to take into account for the treatment of the patient and nowadays the prescription data is forged in many ways by patients and even by doctors or pharmacists but if we control the prescription data of each patients using a blockchain then forging data would become impossible and the information becomes immutable. The doctors could have an accurate and immediate view of a patient's medications, both past, and present, which would result in better, more personalized treatment.

B. Government

The government can leverage blockchain to operate efficiently and improve the delivery of public services. Corruption is a major issue in public services, sometimes citizens feel like they are being cheated by their own government. Blockchain can mitigate this issue by allowing full government transparency. There are many areas in public services where blockchain based solutions can be deployed. Even though we have reached an era where the paper is a waste of resource, public services demand necessary paperwork

from every citizen to ensure its integrity. The government can ensure the identity of every individual by creating a digital identity based on blockchain wherein the data is decentralized and secure. Every citizen can keep updating their digital identity along with the digital paperwork which is added to the blockchain after verification. This system can promote hassle-free services which means that we don't have to carry tons of paperwork just to get a driver's license or to renew our passport. We can run smart contract on top of the blockchain to facilitate tax payment transactions so that no individual can lie about his income and cheat the government. Blockchain-based birth and death certificates with timestamps can help the government keep track of the individuals who are a part of the blockchain. This significantly reduces the chances of identity theft and invasion of privacy. In a blockchain, all the network participants have their own private keys that are assigned to the transactions they make and act as a personal digital signature. This signature is unique and acts as a personal identification for every citizen involved with the government, sort of like a social security number. This signature provides both unique identity and security. If any data in the blockchain is altered then the signature will become invalid and the peer network will know right away that something has happened. This is crucial to preventing further damage to the network. Even if hackers manage to delete content, it can be later retrieved as the data is decentralized and there are copies all over the blockchain.

Georgia's national agency of public registry has elaborate plans to use smart contracts using which citizens can sell or buy land online without spending time on tons of procedures and paperwork. The government of Dubai also has plans to incorporate blockchain based bill payments, VISA applications and license renewals by the year 2020. Various counties also plan to incorporate a blockchain based voting system wherein the votes are transparent and immutable in nature, smart contracts can be used to ensure that voters belong to the constituency and that they vote only once. In the recent years, we have seen several leaks of private and sensitive government information on WikiLeaks, there are also allegations that the 2016 US elections were rigged by Russians. An enormous amount of time and money is being spent by the US government to investigate and mitigate the effects of these attacks. A blockchain based government would be a sustainable solution to all these problems.

There has been a boom in the number of blockchain based start-ups in the Silicon Valley, Even in India, the number of start-ups is increasing exponentially. These efforts will certainly help in making the most of this ground-breaking technology.

Funding of Blockchain based Start-ups in India with respect to different cities (Data: https://goo.gl/w9bDvZ)

Every innovation comes with its own bottlenecks, the same applies to the blockchain industry. There are several drawbacks we need to solve before blockchain becomes a daily use commercial technology.

V. DRAWBACKS

A. The Scalability Issue

In a blockchain, every node has the information regarding every transaction and for incorporating scalability every blockchain protocol must find out a mechanism to limit the nodes that participate in each transaction. If more people start using the blockchain network then the network will slow down and become very expensive but still will not be able to accommodate everyone. Ethereum currently can handle only 15 transactions per second.

Blockchains are decentralized systems across peer to peer networks that are continuously updated and remain in sync with every user assuring equality. As the data is decentralized a hacker needs to hack into more than 51% of the computing systems in order to take control of the blockchain but this would mean that a small scale blockchain is more vulnerable to attack than large-scale ones. Hence we can say that bigger the blockchain, safer the data. This is one of the most important bottlenecks when it comes to blockchain based decentralized systems.

B. The Storage Issue

In normal centralized applications, we tend to use cloud-based services and these are pay per use. We can pay depending on the amount the data and our data is stored till we pay for it but in blockchain based services, the data is immutable and we have to pay for the data up front. This can become troublesome from those who cannot afford the services. A recent research has revealed that in the near future interplanetary databases may cost almost a 100 dollars to store a gigabyte of data.

C. The Interoperability Issue

Interoperability issue arises due to the increasing presence of several types of blockchains and because there is no fixed protocol to communicate between two different blockchains. There are several types of blockchains like the bitcoin blockchain, ethereum blockchain, tezos blockchain, cardano blockchain and so on. Also, there are no protocols for the traditional world to communicate with cryptocurrencies. The main problem with implementing a blockchain based health information exchange networks is also due to interoperability issues. We can implement blockchains effectively only when all health institutes start adhering to a single standard for storing medical and patient information.

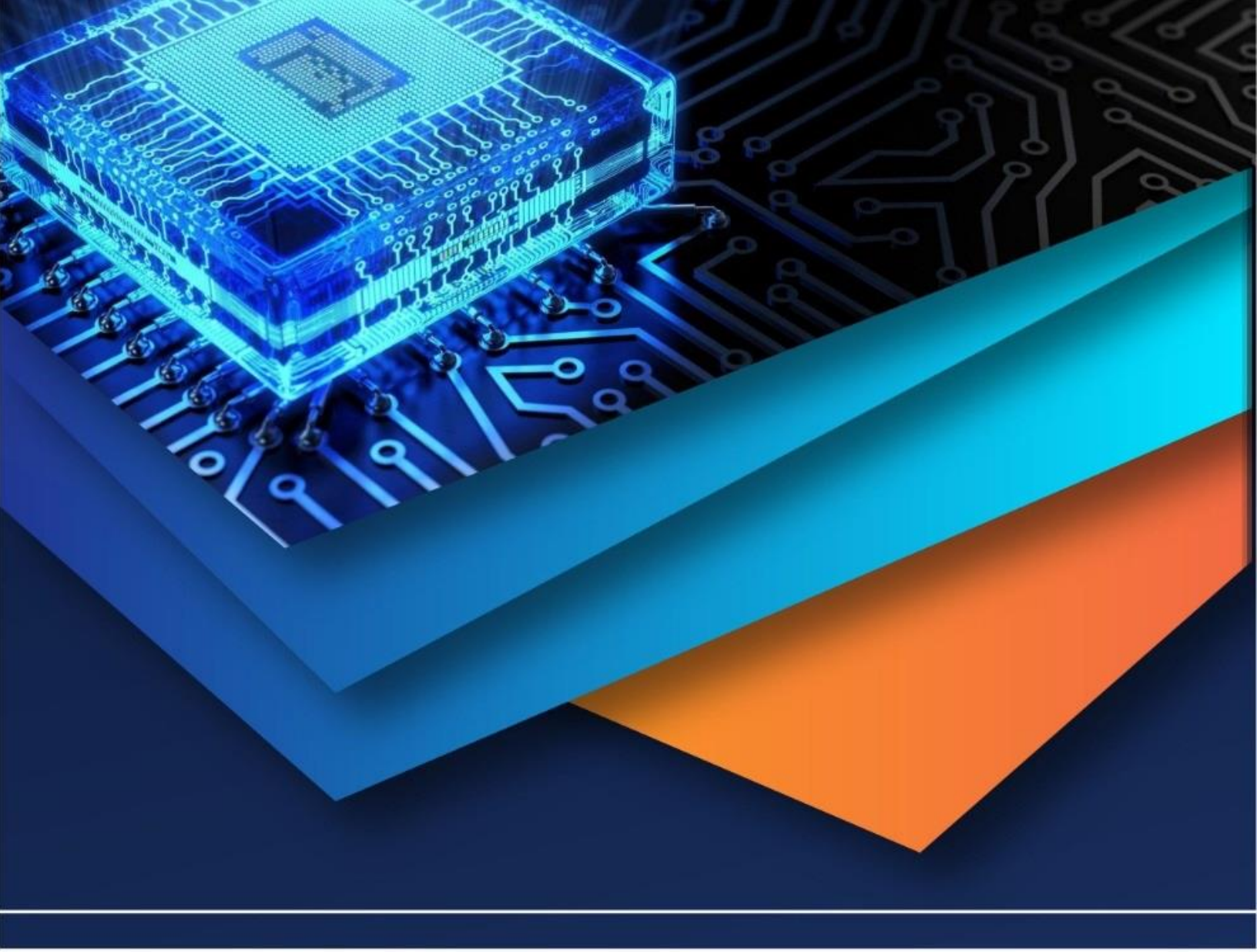
VI. CONCLUSIONS

The blockchain is a fairly new technology and still, a lot of improvements are underway. Combine it with machine learning or internet of things and the possibilities are countless. Data handling and communication are critical when it comes to these technologies. Decentralization ensures power to the users and prevents a single entity from having complete control. It is vaguely similar to moving on from dictatorship to a democracy. There is strong hope that in the future we would be able to overcome bottlenecks and incorporate blockchain based innovation in almost every industry.

REFERENCES

[1] arXiv:1801.03528 Applications of Blockchain Technology beyond Cryptocurrency by Mahdi H. Miraz, Maaruf Ali
[2] Decentralizing IoT networks through blockchain | TechCrunch, Accessed on Jan 14, 2018 https://techcrunch.com/2016/06/28/decentralizing-iot-networks-through-blockchain/
[3] arXiv:1801.03294 A First Look at Identity Management Schemes on the Blockchain by Paul Dunphy, Fabien A.P. Petitcolas
[4] BlockGeeks. (2017). what is Blockchain Technology? A Step-by-Step Guide for Beginners. Accessed on December 30, 2017 from https://blockgeeks.com/guides/what-is-blockchain-technology/
[5] arXiv:1608.05187 Blockchain in internet of things: Challenges and Solutions by Dorri, Ali; Kanhere, Salil S.; Jurdak, Raja
[6] What is blockchain and how can it be used in healthcare? Innovatemedtec Accessed on January 12 2018 https://innovatemedtec.com/digital-health/blockchain
[7] What Are the Applications and Use Cases of Blockchains? – CoinDesk Accessed on Jan 14th 2018 https://www.coindesk.com/information/applications-use-cases-blockchains/
[8] Blockchains don't scale. Not today, at least. But there's hope. hackernoon.com Accessed on January 18, 2018 https://hackernoon.com/blockchains-dont-scale-not-today-at-least-but-there-s-hope-2cb43946551a
[9] Five Issues Preventing Blockchain From Going Mainstream: The Insanely Popular Crypto Game Etheremon Is One Of Them. Accessed on January 10 2018 https://www.forbes.com/sites/outofasia/2017/12/22/five-issues-preventing-blockchain-from-going-mainstream-the-insanely-popular-crypto-game-etheremon-is-one-of-them/#6ceddd576fad
[10] Who Will Build the Health-Care Blockchain? - MIT Technology ReviewAccessed on 25th January 2018 https://www.technologyreview.com/s/603828/deepminds-new-blockchain-style-system-will-track-health-care-records/

[11] SOME SIMPLE ECONOMICS OF THE BLOCKCHAIN by Christian Catalini (MIT Sloan) and Joshua S. Gans (University of Toronto) blockchain.mit.edu accessed on Jan 29, 2018
[12] Pass, R., & Shi, E. (2017, July). Fruitchains: A fair blockchain. In Proceedings of the ACM, Symposium on Principles of Distributed Computing (pp. 315-324). ACM.
[13] 2017arXiv171002951A Transforming face-to-face identity proofing into anonymous digital identity using the Bitcoin blockchain by Augot, Daniel; Chabanne, Hervé; Clémot, Olivier; George, William
[14] It's Time for Governments to Embrace Blockchain – CoinDesk Accessed on jan 15,2018 https://www.coindesk.com/three-questions-governments-embrace-blockchain-2018/
[15] IBM Blockchain Foundation for Developers | Coursera Accessed from December 6th 2017- January 12th 2018 www.coursera.org
[16] Blockchain, AI, ML, robotics to drive tech in 2018: Dimension Data - Business Line Accessed on Feb 3, 2018 https://www.thehindubusinessline.com/info-tech/blockchain-ai-ml-robotics-to-drive-tech-in-2018-dimension-data/article9924966.ece



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY