International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075, Volume-8, Issue-9S3, July 2019

Challenges of Integrating Blockchain with Internet of Things

Aditya Tandon

Abstract*— There is no doubt that Internet of Things (IoT) and blockchain technology will a major impact in the automated futuristic world. Even though the usage of IoT is increasing rapidly, it is riddled with scalability, security, privacy and integrity issues. Even though blockchain was initially created for managing cryptocurrencies, its decentralised nature, higher security, integrity and privacy has led to being integrated with IoT in order to improve it. There are multiple challenges arising from this integration which increases the complexities. It is necessary to study these challenges involved in this integration before carrying it out. Hence, this paper has carried out a systematic study of the various challenges involved in IoT individually and also the advantages and challenges of integrating it with the blockchain system.

***Keywords*— Blockchain, IoT, challenges, security, integration**

I. INTRODUCTION

Originally invented as the underlying technology for Bitcoin, Blockchain has proved to be a revolutionary technology. IoT envisions a completely associated world, where entities effectively interact with each other. This allows a digital depiction of the actual world conceivable, through which lots of smart devices for different domains and uses can be created. The junction of Blockchain and Bitcoin is one of the most promising use cases for Blockchain. Once data is stored in a Blockchain, it becomes unchangeable. With potential amelioration in Blockchain technology, the new features can be used to potentially solve the convoluted challenges arising from IoT [1]. In spite of the cloud of bewilderment and falsity around blockchain, it has appealing applications in IoT. Ranging from secure to distributed data creation and automated data selling, blockchain applications in IoT have a variety of benefits [2]. Public networks are used to link most IoT devices with one another, making it extremely vulnerable to attacks. Blockchain overcomes this problem by using permanent indexed records. Typically, most of the IoT systems use expensive Client-Server models.

Revised Manuscript Received on July 22, 2019.
Aditya Tandon, Department of Computer Science and Engineering, Krishna Engineering College, Ghaziabad, U.P., India

II. HISTORY OF BLOCKCHAIN TECHNOLOGY

The term "Blockchain" was first introduced to the world when Satoshi Nakamoto released a paper on Bitcoin in 2008 [3]. Blockchain, the technology that runs Bitcoin has developed significantly over the past decade, making it one of the biggest ground-breaking technologies. One cannot talk about Blockchains without talking about Bitcoin, or broadly, cryptocurrencies in general. According to Nakamoto, Blockchain and cryptocurrencies are two intricately linked conceptions, and the technology is meaningless outside the area of digital money. As the concept of cryptocurrencies burgeoned, many people started confusing the terms "Bitcoin" and "Blockchain". When the technology of blockchain came into limelight in 2013, a lot of people realized that this technology could be used for a myriad of applications [4]. A blockchain is an alter-evident ledger that keeps track of transactions in a public or private network. The ledger maintains the records in a contiguous fashion as hash-linked blocks. The blocks are linked right from the first block to the most current block by a chain, and thus this technology is termed blockchain.

Vitalik Buterin, co-founder of Ethereum, being discontented with the limitations in the initial bitcoin codebase, aimed for a more malleable blockchain. He thus set out to construct Ethereum, the second public Blockchain, in 2013. Buterin published a paper on Ethereum in mid-2013 [5]. However, it's significance dropped in mid-2014 when Gavin wood released a new paper, which emphasized on the motive of Ethereum Virtual Machine (EVM) [6]. The Ethereum Blockchain was not strictly restricted to cryptocurrencies. It also encompassed the ability to maintain various types of assets. However, this introduced drawbacks such as scalability, interoperability and sustainability. This led to the creation of "dApps" or Decentralized applications. Then came the third generation Blockchains, by which different Blockchains could converse with one another. A layered-technology called "Cardano" came into existence, and thus introduced flexibility [7]. Other third generation block chains include Aion, ArcBlock and Zilliqa. Thus Blockchain has evolved a lot since it's inception in the past decade. Cryptocurrencies, are now, just one of the several thousand applications that uses Blockchain [8].

III. OVERVIEW OF BLOCKCHAIN TECHNOLOGY [9]

The "blocks" in blockchain typically consist of digital information. They contain three types of information-information about the various transactions, the people participating in them and the information that distinguishes them from other blocks. Owing to the extensive deployment of IoT devices and bulk

Retrieval Number: I33110789S319/2019©BEIESP
DOI: 10.35940/ijitee.I3311.0789S319

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

demands in Blockchain, the existent Blockchain technologies can be inefficient for IoT applications. Constructing a fraud-proof system for transactions is also possible by Blockchain, thus allowing it to be exploited in various other fields.

Transactions are the basic units in blockchain that contains the registry of all the instances followed by the miners. Each transaction is validated by a cryptographic private key. This validation is in a form of virtual signature gets embedded into the transaction permanently. This ensures that the transactions arises from the proprietor of the private key. When the public keys corresponds to these private keys, it is known to verify the integrity of the transaction by the miners [10]. This can be obtained by maintaining the open key as the source address in the respective transaction attaching the public key and its certificates to the signature or preloading the public key at the miners.

The transaction joins the events and its source without any error by using cryptography. There were initially utilised for Bitcoin for capturing the financial exchanges between two parties [11]. They have also been utilised for extensively assigning the ownership and realising the altering events [12] [13]. A neat return linked list for blocks are preserved as a book of transactions for each individual miner in the system [14]. The blocks which are the elements of the ledger contains batches of confirmed transactions. These blocks also have a header that is linked to the existing block. The block header may contain other fields like timestamps based on particular demands. Every block is individually recognised by using a hash value which is created using cryptic hashing algorithms in the header the blocks. This chain of hashes that links the individual blocks to the parent nodes can be used to find the successive parents and finally leading the initial block in the chain. The blocks are linked this way and works as a ledger at each of the nodes. The link from the block to the parent in in the header, hence it affects the hash value of the block. When one block needs to be modified, then its subordinate and its successive subordinate blocks should also be altered to solve the complexities arising from it. Therefore, it is strictly impossible to tamper the chain. Longer chains are more difficult to tamper. Locally maintained block chains can be validated and updated frequently [15]. Out of the multiple chains, only the longest one is considered as the ledger in the public. The other chains that are available locally will be updated based on this.

The headers in the blocks contain fields that have data of the entire transactions from the current block. One such example is the Merkle root [16]. In this technique, the transactions act as leaves of the tree for improving the efficiency of the storage in the block [17]. The tree has a structure where each individual leaf node acts as a transaction and the other nodes act as hashing of the subordinate blocks as shown in fig.1.

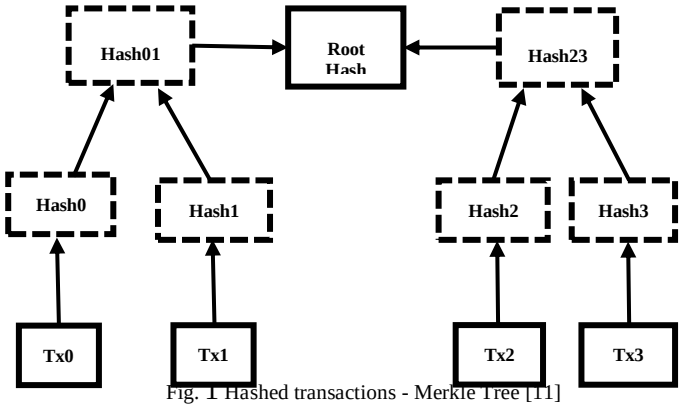

Fig. 1 Hashed transactions - Merkle Tree [11]

The tree's root is known as Merkle root. Its peers in the network can be used to make sure that the transaction was mined by confirming the hash of respective branches. This is because, some other transactions are performed without hashing. By this, the necessity of memory, capacity and the storage may be reduced to a great extent. Transactions and blocks are scattered across the network and then verified for forming distributed consensus. When bitcoin is taken as an example, an individual node creates a legal transaction and it sends a message to the inventory that contains the hash of the transaction (TX ID). It does not contain the actual transaction data of all the intermediate nodes. These intermediate nodes do not have their own transactions and hence answers to the senders. After verification, these transactions are then spread to the other neighbouring nodes. This takes place until the whole network has received the transactions [15]. The miners who solve the problem and create the blocks are responsible for creating and spreading the blocks to the network.

IV. APPLICATIONS OF BLOCK CHAIN TECHNOLOGY

There are lots of application involving blockchains. Different applications are tabulated in table I.

A. *Cryptocurrencies*

Cryptocurrencies are the most well-known applications of the blockchain system. Blockchain completes the user's requests anonymously and therefore guarantees safety. Since financial transactions now take place between the countries that have different laws and regulations among them, the conventional banking system is getting disrupted [18]. The boom in the value of the bitcoin brought awareness of the blockchain to the general public and has brought more confidence on cryptocurrencies [15], [19].

Bitcoin is the most commonly used and the first used cryptocurrency. It is estimated that aggregate value of the entire cryptocurrencies have crossed $200 billion. Bitcoin has earned the nickname "*digital gold*" [15]. The price of these currencies are extremely volatile and can change every second. The value of each bitcoin is around half of the total value of other cryptocurrencies. However, its value peaked in 2017 and dropped back to its current value. The working of cryptocurrencies differ

Retrieval Number: I33110789S319/2019©BEIESP
DOI: 10.35940/ijitee.I3311.0789S319

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

from ordinary currencies. Since it is highly decentralised, the values fluctuates based on the market, therefore, it has gained lots of speculations [20], [21].

It can effectively solve the issues pertaining in the financial world. The costs for transaction handling is high for international transfer which can be eliminated using cryptocurrencies. It can reduce the time taken and red-tapism associated with the transactions. It can also eliminate the third party asset managers thereby eliminating the hazard of losing the money. It can establish guarantees on its own for different parties that do not trust each other due to its effective use identification [15], [19], [22].

B. Internet of Things

The various means by which we interact with the environment and one another has changed tremendously. The Internet of Things (IoT) technology, being an extremely ubiquitous technology, is meant to mould human life, thereby producing enormous economic benefits. Diverse challenges emanate from IoT and the Blockchain technology can be used to solve these challenges [9]. Internet of Things (IoT) provides significantly to a variety of aspects of our everyday lives and drives many applications from numerous sectors like healthcare, manufacturing and so on [23]. IoT plays a pivotal role in transforming homes into smart homes and cities into smart cities. Plentiful intricate challenges innate in the IoT are faced by blockchain. Blockchain is separated among various platforms. Integrating blockchain with IoT builds trust between parties and devices, curtails overhead like removing middlemen and also significantly quickens transactions. In order to work towards Blockchain integration, mainly for IoT purposes, there is a necessity to form connections between various A few issues like scalability, interoperability and security need to be overcome by Blockchain in IoT. Blockchains for them to exploit one-another's strengths. Blockchain and IoT are interdependent one another and are also expanding tremendously. Blockchain is ravenous for the opportunities that IoT provides it and IoT is desperate for the features that Blockchain holds.

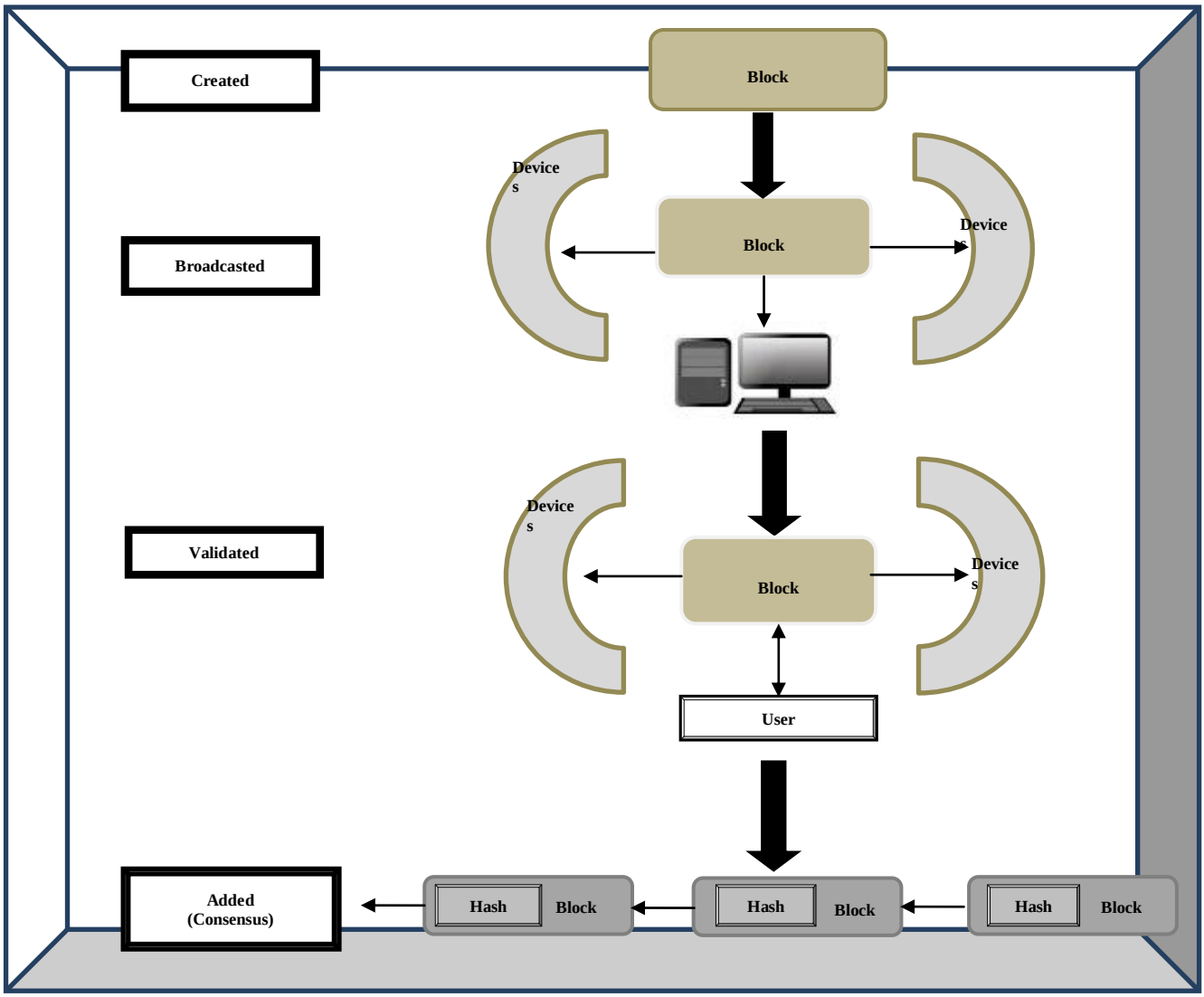

Fig. 2 A typical workflow of blockchain

Retrieval Number: I3311078 9S319/2019©BEIESP
DOI: 10.35940/ijitee.I3311.0789S319

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

TABLE I
SECTOR WISE APPLICATIONS AND USE OF BLOCK CHAIN TECHNOLOGY [24]

Field	Applications in that field
Agricultural sector	Information on the soil, old agricultural records, shipping, seeds, sales, harvests, marketing, etc.
Trade	Information on imports, exports, transactions, old records
Power Sector	Information on power generation, raw materials, resources, suppliers, etc.
Food Industry	Information on food packaging, delivery, shipment, online orders, quality of food, etc.
Financial Sector	Cryptocurrencies, Information on money exchange, deposits, transfers, crowd-funding, smart-securities, contracts, transactional assets, etc.
Health Sector	EMR, medical reports, digitalised version of old data, prescriptions, patient vitals, etc.
Industrial Sector	Information on products, warranty, components, tracking raw materials, etc.
Logistical sector	Logistical records, Information on the shipping and delivery, toll data, GPS data, etc
Smart Entities	Smart cities, smart devices, IoT devices, managing the water, pollution, etc.
Others	Digitalised content, Sharing finances, ownership of goods and precious items, election data, etc.

Blockchain delivers service layers for integrating with the typical IoT framework [25] [26]. Usually, the framework contains three essential roles which are sensor, miner and agent [27]. The IoT sensors obtain information and interacts with the services with the blockchain agents [28]. The sensors do not integrate with the blockchain functions. The transactions in form of sensory data can be interpreted and then broadcaster in the network. These agents also provide security by applying private keys, while the IoT devices do not have this security. Miners who form the network use the core functions of the blockchain by verifying the transactions and placing them into blocks [9].

C. Healthcare

Medical records may contain lots of data and mostly get integrated in big data. Electronic Medical Records (EMR) of large hospital chains may contain millions of patient data and hence sharing it between different branches may require storage at different places with lots of collaboration between different entities [29]. Blockchain can be used to facilitate this exchange and give more power to the patients.

Digital access rues can be managed by improving the interoperability among the patients. Creating rues for managing the medical data is challenging which should be controlled by the owner of the data [30]. A centralised and shared method for managing these perspective rules can be enabled using Blockchain. Smart Properties is a unit of blockchain system where the ownership of the data can be controlled and managed. In this, a digital unit can be assigned an ownership. Since the patient is the owner of his data, he will be able to create the rules and decide who can view and access the data thereby allowing easier sharing.

Another way the blockchain can help patient centric data sharing is through availability of data. When patients gain more ownership of their data, they will access the information from any system that has access. Once the patient gets access, they can manage them. This is virtually impossible without blockchain in the current scenario. The patient's medical history may be broadcasted with high security with an anonymous digital identity. When the same patient's history from different places are merged together, the patient needs to only use one platform and protocol. In addition, patients may publish their own data in to the system. This comes to use when a morbid patient requires regular medical surveillance [25]. Hence the vitals of the patient can be uploaded for getting monitored by the concerned person even away from the patient [26].

Another major factor is the quicker access. The data can gets exchanged once the ledger authorisation is cleared and this takes place rapidly. Even when the information is not kept in the blockchain, but only the metadata is available, the data is still accessed smoothly in a streamlined manner. When the entire medical history is available instantly, past records can be verified by the professionals, thereby improving the data availability and liquidity.

Another application is the patient identification. Since blockchain gives a default address to a user, this can work as a patient identifier. This can be used as a unique ID throughout the world. Currently, there is no such universally accepted identification and data managing system. Resolving these issues is a very much interesting research gap for future study [33]. When two different hospitals use the same patient's data, they must initially connect the unique identifier to the existing identifier in that particular hospital. This may be resolved by using a PKI that can be used across the world. Since blockchains secure the data through different servers, the data will not get lose

Retrieval Number: I33110789S319/2019©BEIESP
DOI: 10.35940/ijitee.I3311.0789S319

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

leading to reduction in loss of data and ensures that the entire medical data is available [34].

V. OVERVIEW OF IOT

IoT is altering the world rapidly in various fields and applications. It consists of latest sensors and actuators embedded in the general devices thereby converting them into smart devices. These devices are linked together and transfer large amounts of data between each other without the need of human interaction [35]. It greatly improves our day to day life with different applications ranging from smart devices to smart grid, smart cities, etc. However, a major threat to this is the privacy and security of the data that is transferred. There have been lots of research and enhancements in the recent past that has been mitigating these risks in IoT.

According to Cisco, an estimated 50 billion objects will be connected to the IoT by the year 2020 [36]. The security issues that are being researched are the confidentiality, privacy [32], integrity [32], key management [37], etc. However, the security challenges keep changing due to different emerging complexities and issues, This must be overcome with more research and improvements by taking the new integrations into consideration. Since centralised framework is the norm, distributed techniques maybe used for dealing with the novel security issues [23].

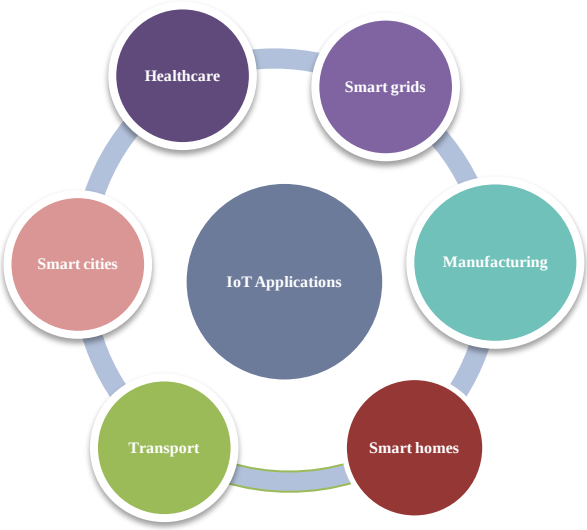

Fig. 3 Internet of Things' applications

VI. CHALLENGES IN IOT

IoT provides many advantages for various problems, however there are some existing challenges that must be overcome. These challenges arise in form of privacy or security. Hence, these different problems are studied in this section in order to provide solutions for these problems. The challenges from Internet Society [38] in the IoT has been summarised and shown in Table II.

VII. INTEGRATION OF IOT IN BLOCKCHAIN

The IoT is changing the various available manual processes into a digitalised version by processing huge amounts of data, which was not possible earlier. This large volume is aiding the creation of smart applications like improving the quality and management of the people's life when the digitalisation takes place [39]. During the last decade, improvement in cloud computing has paved the way for IoT with the necessary functions like data processing in real time actions [40].

TABLE II

CHALLENGES IN IOT

Challenges		Observation
Security	Data inefficiency	There isn't enough data yet to secure the design in the future
	Standardisation	Ineffective metrics and standards for identifying the security problems
	Cost	There isn't enough data on the cost for security features
	Authentication	Absence of a centralised network model for preventing threats and cyber-attacks.
	Firmware Update	Lack of updates to the IoT devices with the latest firmware.
	Regulation	Varied laws or lack of laws leads to security issues.
Privacy	Collection of data	There isn't any regulation to prevent usage of collected data. Also, there aren't models to maintain transparency.
	Data Inefficiency	There aren't enough resources to develop the piracy frameworks,
Legal	Protection of Information	Absence of laws for creating regulations
	Enforcement	Absence of laws for law enforcement agencies to monitor crimes
	Theft	Absence of laws to protect proliferation of data.

The unexpected rapid growth in IoT has started new opportunities like methods to obtain and share data. But, there is a lack of confidence among the general public for this matter since they do not have any clear vision of where the data is being used. Integrating the IoT to cloud technology is seen to be valuable. Similarly, it can be acknowledged that there are many possibilities for blockchain reforming thee IoT. It can make improvements to the IoT by delivering a trusted sharing service where the data is trustworthy and can identified easily. The source of the data can be found at any time and this increases the security. In applications where security is the main requirement, this integration will ensure that data will be shared between the available users. A breach in the data may lead to fraudulent activities or slow down the security features and this could cause

Retrieval Number: I3311078 9S319/2019©BEIESP
DOI: 10.35940/ijitee.I3311.0789S319

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

serious damage or loss to the concerned organisation [41]. Hence, it would be better to improve the way of sharing the data between the designated users, thereby reducing the time taken to search for the necessary data. Sharing the necessary data can also favour including newer people in the ecosystems and improving the services in implementations like smart cars and smart cities. Hence, using the blockchain may aid the IoT with data that is more dependable and added security. Blockchain can be considered as a tool for solving privacy, dependability and scalability issues with respect to IoT paradigm [42]. IoT will be able to help the functions provided by the blockchain and will also aid in development of the existing IoT technologies. However, plethora of issues and problems exist in the existing technologies which must be studied for using and integrating these technologies. There is a great scope of research in this work since it is still in the incubatory development. Mainly, this integration will bring progress to scalability, decentralisation, reliability, autonomy, security, etc.

A. Advantages of Integration

In centralised architecture, there are issues related to bottlenecks and central points of failure. Shifting to a peer to peer based architecture will solve this issue [43]. Since the storage gets decentralised, smaller companies can also control the data and process them contrary to centralised architecture where large companies control the data. It also enables better fault tolerance and scalability in the system. Identity of the connected devices are important since this leads to security and trust issues. By utilising a single blockchain system, all the connected devices can be identified in a unique manner. The identity is also necessary for identifying which data was provided by which device. In addition, the blockchain also provides authentication of the IoT devices [44].

Smart devices with a great amount of autonomy can be made possible thanks to Blockchain technology which helps in integrating futuristic features along with smart hardware [45], [46]. The smart devices will be able to interact with each other even in the absence of servers. This can be utilised by the IoT for decoupled applications. The system is also reliable since there is no scope of loss of data through the blockchain [47]. The users will be able to verify the data authenticity in order to make sure that the data is still intact without any tampering. The system will also be able to trace and account the data. Hence, reliability is the major factor for considering the integration.

The system is also secure since the data is stored as a transaction of the blockchain [48]. It can change in form of transactions which is validated by smart contracts in this way. Secure codes may be deployed to safely embed the codes in the IoT devices [43], [49]. This can allow the companies to track the devices and update them confidentially [48]. It can also create an environment for use in markets, where the transactions between different players can be performed without any authorities, Micro payments can be done instantly even when there is no trust between different people [50]–[52]. This can make improvement in the IoT by granting more data into the blockchain.

When blockchains are integrated, it has to be seen whether the devices within the system can interact with each other. A new layer is included between the IoT devices and the cloud computing for better integration and this is known as fog computing [53].

Communication between two IoT devices are fast and secure and has the ability to work offline. They have the ability to communicate with each other by using routing techniques. They do not need a blockchain for communication since only a small percentage of the data is stored in blockchain. This is used in applications where low latency is a requirement. On the other hand, communication between the IoT and the blockchain requires all the data to pass through the blockchain keeping a record of all the interactions taking place. This makes sure that all the interactions can be traced and recorded. Since this increases the bandwidth usage, this can be considered as a major limitation in blockchain.

Communication using a hybrid technique is where only a small percentage of the data is shared with the blockchain, while the interconnections between the IoT takes place directly. However, it is challenging to select which interactions should pass through blockchain during the run time. These limitations are addressed by the fog computing which uses gateways and other devices for mining [54], [55]. Even though the utilisation of this technique is increasing rapidly, it doesn't have to be used everywhere. It should only be used in applications that demand it. Usually, using blockchain individually may not be good for application requiring high performance, but a hybrid technique may be required for optimising it. Wüst and Gervais [56] have presented a flow where the necessity of blockchain is identified based on their application.

In order to make it easier for integrating the IoT and Blockchain, readily available devices are being sold by major companies by forming alliances amongst themselves [57].

Retrieval Number: I33110789S319/2019©BEIESP
DOI: 10.35940/ijitee.I3311.0789S319

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

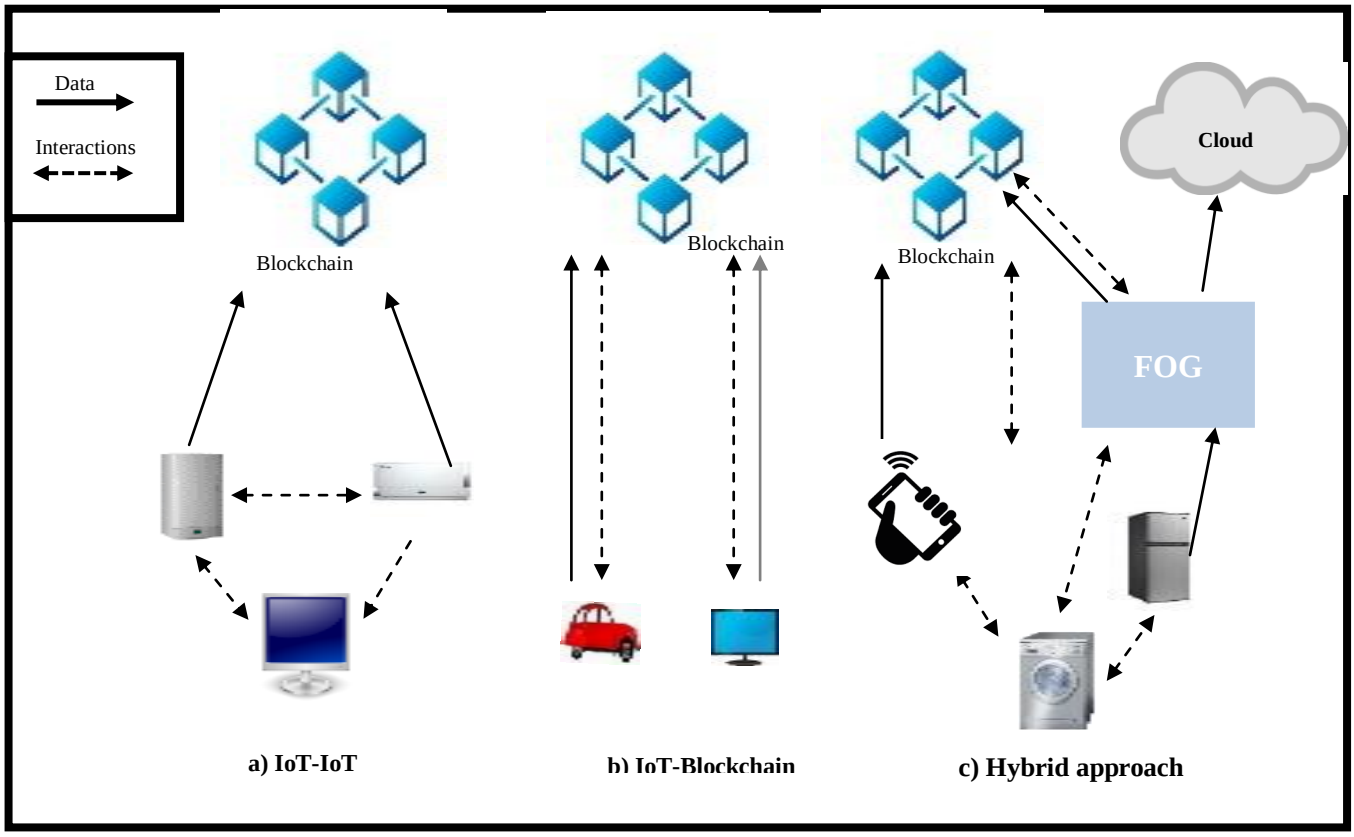

Fig. 4 Types of integration of IoT and blockchains

Some of the IoT devices are being sold with integrated functions to connect to blockchain [54], [55], [58], [59]. EthEmbedded, the company that is responsible for Ethreum allows installing the nodes in various devices like Odroid, Beaglebone and Raspberry Pi. Similarly, EthRaspbian and Raspnode have the capability to install Bitcoins, Litecoins and Ethereum nodes in the Raspberry PI. The Wi-Fi Router. Raspnode also provides support for wallet for Litecoin and Bitcoin. Antrouter R-LTC has this capability too for mining Litecoin. Hence, this router can be easily installed in IoT network as a part of fog computing platform. The different IoT devices ready for market for different blockchains are shown in table III. This is still in the initial stage and lots of research in necessary for further integration. There are also functionalities for mining in some IoT devices. It is not necessary for all the IoT devices to have this capability since it requires high end hardware and becomes void in IoT devices. That is why you don t usually find mining using IoT.

TABLE III

MARKET READY IOT DEVICES FOR THE RESPECTIVE BLOCKCHAINS

Blockchain Technique	Project	IoT Devices
Bitcoin	Raspnode	Raspberry Pi
Ethereum	EthEmbedded	Raspberry Pi, BeagleBone and Odroid
	EthRaspbian	Wandboard and Ethcore Parity
Litecoin	Bitmain	Antrouter

There is another alternative for integrating the blockchain with IoT, which is integrating it with cloud computing [40]. Devices have been integrated in this way for some years for overcoming the drawbacks in IoT like storage, accessing and processing. However, since cloud computing works with a central framework, it isn't reliable and securing while sharing the data with the designated receiver. Therefore, blockchains are preferred over cloud computing for addressing this issue.

VIII. CHALLENGES IN INTEGRATION

The challenges faced when blockchain technology is applied to the IoT domain will be explored in this section. It isn't easy to integrate the IoT devices with blockchain. The origin of blockchain is quite different from the IoT, since blockchain has been designed for exclusively using with Internet through powerful computers. Since the transactions based on blockchain are signed digitally, the functionality should be incorporated in the devices which make use of financial transactions. The integration of IoT with Blockchain is quite challenging. The major challenges faced are described below [39].

A. Storage capacity and scalability

It is still debated whether problems in scalability and storage capability of blockchain is prevalent, and when it is integrated with IoT applications, it is even more challenging.

Retrieval Number: I3311078 9S319/2019©BEIESP
DOI: 10.35940/ijitee.I3311.0789S319

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Although because of this, Blockchain technology might appear to be inappropriate for IoT, but the challenges faced could be avoided or reduced altogether. Some IoT devices can generate huge amount of data which would make it difficult for the integrations since the prevailing blockchains cannot process such large transactions. Hence efforts should be made to solve these problems before integrating these two technologies.

Currently, only a small percentage of the humungous IoT data is useful to extract knowledge and producing actions. Hence, there are different researchers who have proposed methods for filtering, normalising and compressing the IoT data in order to reduce them. IoT comprises of various devices like embedded and communication devices which saves the amount of data provided by IoT to the blockchain. Compressing the data may reduce the data that us transmitted, processed and stored by the IoT. Finally, the agreed protocol may be utilised to boost the bandwidth allocated and reduce the latency in the contracts which improves the integration between the IoT and the blockchain [60].

B. Security

Owing to the dearth of performance and huge non-uniformity of devices, the security challenges in IoT applications have to be dealt at various levels in a more complicated way. Additionally, the IoT environment contains different properties like wireless communication, mobility, etc. which complicates the security challenges. Thorough surveys of exhaustive security analysis in have been performed in found in [61], [62], [63], [64]. Comparison of research on different security solutions in IoT is given in table IV. It is crucial to build an IoT with an extremely strong security, owing to the rise in quantity of attacks and their severe effects. Blockchain is viewed as a decisive technology to cater to the much needed security advancements in IoT. But, authenticity of the data generated by the IoT remains to be the crucial challenge in the integration of two technologies. Blockchain can make sure that data sent through the chain remains intact and can identify their changes, and thus when the data reaches the destination, the data that is already corrupted will remain that way. Apart from suspicious sources, corrupted data in IoT may come from many other sources. The different aspects of security is given in fig. 5.

Factors like vandalism, device failures, environment and the type of participants play a role in the integrity of the IoT framework. At times, the IoT devices may not work well and it is difficult to know this until the device is tested. Sometimes, they may work well at the beginning and then stop working due to hardware or software issues. Eavesdropping, controlling or Denial of Service (DOS) are the major menaces that can have a major impact on the IoT and thus they need to be properly tested before getting integrated. They need to be found and encapsulated correctly in order to prevent physical damages, and also to include mechanisms for detecting any failure in the devices instantly [62].

Retrieval Number: I33110789S319/2019©BEIESP
DOI: 10.35940/ijitee.I3311.0789S319

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

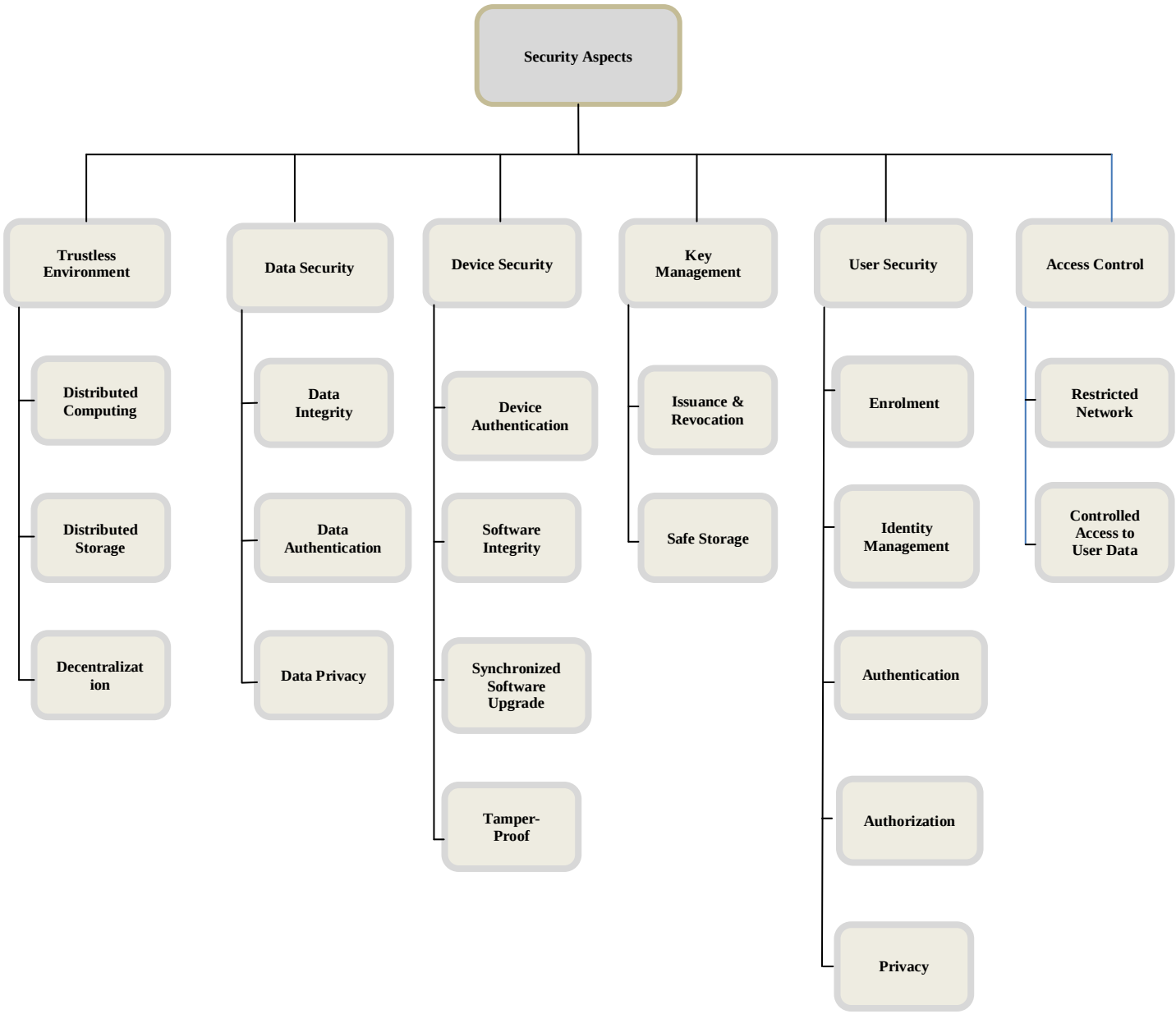

Fig. 5 Security aspects of IoT by Makhdoom et al., [65]

The IoT devices may get hacked very easily due to their limitations in the updates to the firmware leading to prevalence of bugs. Since there are numerous devices, it cannot be deployed in all these devices individually. Hence, there should be some kind of automatic configurations in these devices in order to get updated automatically when they are connected to the internet.

TABLE IV: *COMPARISON OF DIFFERENT SOLUTIONS RELATED TO SECURITY IN IOT*

		Challenges						
Solutions	**Study**	**Computational difficulty**	**Communicati onal difficulty**	**Memory**	**Agility**	**Heterogeneity**	**Scalability**	**Service Quality**
Confidentiality	Touati et al.[66]	Great	Poor	Medium	Medium	Medium	Poor	Poor
	Oualha and Nguyen [67]	Medium	Medium	Poor	Medium	Poor	Medium	Medium
	Guo et al. [68]	Medium	Poor	Great	Medium	Medium	Poor	Poor

Retrieval Number: I3311078 9S319/2019©BEIESP
DOI: 10.35940/ijitee.I3311.0789S319

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

	Yao et al. [69]	Great	Medium	Medium	Medium	Medium	Poor	Medium
	Su et al. [70]	Poor	Medium	Medium	Medium	Poor	Poor	Medium
	Thatmann [71]	Poor	Medium	Medium	Medium	Poor	Medium	Medium
	Chen [72]	Great	Medium	Great	Poor	Poor	Poor	Medium
	Mao et al.,[73]	Medium	Medium	Medium	Medium	Medium	Poor	Medium
Privacy	Evans & Eyers, [74]	Medium	Poor	Great	Medium	Poor	Medium	Medium
	Zhang et al. [75]	Great	Poor	Great	Medium	Medium	Poor	Medium
	Alcaide et al.[76]	Great	Medium	Medium	Medium	Poor	Medium	Medium
	Huang et al. [77]	Medium	Poor	Poor	Medium	Great	Medium	Medium
	Skarmeta et al. [78]	Great	Medium	Medium	Poor	Poor	Medium	Medium
	Tonyali [79]	Medium	Poor	Medium	Poor	Poor	Medium	Medium
Availability	Maleh et al. [80]	Medium	Medium	Poor	Medium	Medium	Poor	Poor
	Kasinathan et al., [81]	Medium	Poor	Medium	Medium	Medium	Medium	Medium
	Almeida et al. [82]	Poor	Medium	Poor	Medium	Medium	Poor	Medium
	Machaka et al., [83]	Medium	Medium	Poor	Poor	Medium	Poor	Poor
	Shreenivas et al., [84]	Medium	Medium	Medium	Medium	Medium	Poor	Poor
Blockchain	Hardjono & Smith [85]	Medium	Poor	Medium	Medium	Great	Great	Poor
	Gaurav et al., [86]	Poor	Poor	Poor	Great	Medium	Great	Medium
	Hashemi et al. [87]		Medium	Poor	Poor	Medium	Great	Medium
	Kokoris-Kogias et al. [88]	Poor	Medium	Poor	Poor	Medium	Great	Medium
	Biswas & Muthukkumarasamy [89]	Poor	Poor	Poor	Medium	Medium	Great	Medium
SDN	Flauzac et al.[90]	Great	Poor	Medium	Poor	Great	Great	Poor
	Bull et al.[91]	Medium	Poor	Medium	Medium	Medium	Poor	Great
	Vandana [92]	Medium	Poor	Medium	Poor	Great	Medium	Medium
	Gonzalez et al. [93]	Medium	Poor	Medium	Poor	Medium	Medium	Great

There are frameworks available that allows these updates to the firmware in real time to make sure that the integration remain safe [94], [95].

There can be several impacts due to this integration [96]. Some application protocols utilise other security protocols like Transport Layer Security (TLS) for providing communication securely. However, these protocols are complicated and requires a central managing system along with a Public Key Infrastructure (PKI). Every IoT device contains its unique identifier when it gets connected to the network. Having this identifier nullifies the need of PKI, hence the exchange of

Retrieval Number: I33110789S319/2019©BEIESP
DOI: 10.35940/ijitee.I3311.0789S319

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

certificates is not necessary thereby allowing low capacity devices to integrate. A prominent improvement in adopting blockchain with respect to security is the device known as Filament [46], which is a functionality that works with both software and hardware and provides security in payments and smart contracts. This device contains crypto-processors which supports various protocols for providing security in a diversified way.

C. Privacy of Information

Confidentiality is a major requirement for IoT applications, especially, when they contain private information, hence it is necessary to ensure anonymity and privacy of data. This is a major concern since all the connected devices may be transmitting private information continuously. Even though there are solutions for these privacy problems, it is difficult for IoT applications since there are many levels of data right from its collection to the application. Therefore securing this private data and to ensure its delivery to the designated person or unit is a challenge while integrating IoT with blockchain. Trust is a major factor in this integration and its importance in IoT applications has been identified by Fernandez-Gago et al. [97].

There have been lots of encryption being used for securing the communication by encrypting the data. However, due to limitations in the devices, it is difficult to provide the latest security protocols. Hence, cryptographic hardware maybe used for performing these work to avoid the use of complicated software protocols.

There are methods to maintain the integrity of data for ensuring safe data transmission also eliminates the need of blockchain handling unnecessary data created by IoT devices. This may lead to a better and effective system in the public with better access control. A dynamic data update and effective authentication using open auditing has been performed in Liu et al [98]. The same authors have also reviewed these verification methods broadly in Liu et al. [99].It has been ensures in Wang et al. [100] that the data content is done using a open auditing system that preserves the privacy.

D. Smart contracts

Smart contracts are agreements between two parties which are directly embedded as a code in the blockchain and gets executed on its own. Embedding in the blockchain makes sure that it is available in a decentralised and distributed matter in the blockchain network. Even though it is advantageous, there are challenges associated with the implementation of this technology. It is useful for IoT applications, however there is no single method of implementation since they are practically only a group of functions and data in a particular blockchain.

The IoT devices can call these functions whenever required. The transactions are regulated by the senders and must get accepted in the network. The devices can identify the contracts and initiate them in the necessary locations throughout the internet [40]. The contract will contain the information as to when to start and stop a particular work, and when to take certain actions. If the measurements cross a certain fixed threshold, then an event will get fired. The application will continuously monitor and listen for these firing. When there is no firing, it can be said that the work has been executed as per the contract. Using this technologies need the users to use oracles which transmit data with better trust. Validation of the contracts may get conceded as the IoT may lose stability.

Gaining access from different data sources may also lead to overloading of these contracts. Since they are decentralised in the blockchain, the resources are not shared among many devices for distributing the tasks, hence a single devices has to handle all the computations. This means that contract execution is done in a single device while the execution of the codes take place in multiple devices. In order to increase the processing power, it uses cloud computing and big data for increasing the processing capability. Data mining can be used for addressing these issues since only the required data may be obtained for the processing. Using big data, large amounts of processing may be performed simultaneously and can be extracted from big datasets which was difficult previously. While integrating, smart contracts must utilise the distributed nature for enabling the processing power using cloud or the big data.

E. Legal issues

Another major roadblock is the presence of laws that cover these privacy techniques which have still not be updated for latest technology. When cryptocurrencies were introduced, there was no law to regulate such a technology even though they were being used for transactions. However, some governments have started to ban the use of cryptocurrencies [101].

While cryptocurrencies are legal in some nations, they are considered to be illegal in some [102]. However, there are no laws to govern them in most of the countries, leading to uncertainty. Even though they haven't been considered to be illegal, it doesn't mean that they are legal there. This has raised lots of complex legal issues in the administration and the finance of the countries. The government financial institutes in China have banned them leading to reduction in mining from Chinese miners [103]. In Russia, even though they are no illegal, the law specifies that only Ruble is a legal tender. This was the case in India too until they were deemed illegal [104]. However, it has since been clarified that they are not entirely illegal in India. The government is creating amendments to bring regulations to the cryptocurrency market [105].

The regulated market of blockchain was the major reason for the popularity of Bitcoin. The usage of IoT has also been affected by the country's laws and regulations. Most of these laws need to be updated since they have become obsolete. Creating better regulations may make develop the security features of the devices and help in ensuring the trust in the devices. Hence, this becomes even a bigger challenge when integrated with blockchain. Lack of regulations is disadvantageous for some organisations since retrieving the private key is not possible. Future regulations may either be advantageous or disadvantageous since they can affect the decentralised and free nature of the blockchain.

Retrieval Number: I3110789S319/2019©BEIESP
DOI: 10.35940/ijitee.I3311.0789S319

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

IX. CONCLUSION AND FUTURE SCOPE

A novel technology almost always generates lots of controversies. With the success of cryptocurrencies, it is anticipated that integration of the blockchains with IoT will create a revolution in a technological sense. The challenges like scalability, storage capacity, privacy and security have to be solved through continuous research. The main drawback of cryptocurrencies is volatility and this has led to people using it unfairly. Integrating IoT to the blockchain will significantly improve this problem and elevate the status of cryptocurrencies on par with the existing trustworthy monetary entities. IoT and blockchain technology will a major impact in the automated futuristic world. However, to cement this achievement, these technologies must attain transformations so that effective integration is possible. Soon, machines will start interacting with each other without human intervention more efficiently and economically. Hence, it is necessary to create more secure integrated system to satisfy the requirements of the digitalised economy. This transformation must be financially viable and possible.

However, modifying existing frameworks without much research and practical implementation is not good since this may lead to failure and thereby lose the support of the public. Hence, the integration of IoT to the blockchain should be performed and analysed carefully by taking into consideration the challenges identified in this work. Government regulations and local laws should be considered while initiating this integration. The major applications and challenges in integrating these two novel technologies are discussed in this paper. Some major solutions for improving this integration is also given in this work. Available preliminary applications were studied for providing a thorough overview of the integration.

There should be ways where the heterogeneous IoT devices will be able to directly send data over the network. It is also necessary to make sure that the IoT devices works in insecure networks without using additional hardware equipment. This can be a major factor since additional equipment will increase the cost of the smart devices. Another issue is the malware problem that are sent over the network. Existing schemes have proposed blockchain based firmware update for protection. However, they do not provide security against the attacks where the hardware gets configured to give way for back door access, hence, it is easy to launch such attacks. Preventing such malware will be the future scope of this work including solving other security issues.

REFERENCES

[1] N. Kshetri, “Can Blockchain Strengthen the Internet of Things?,” IT Prof., vol. 19, no. 4, pp. 68–72, 2017.

[2] H. Orman, “Blockchain: the Emperors New PKI?,” IEEE Internet Comput., vol. 22, no. 2, pp. 23–28, Mar. 2018.

[3] Satoshi Nakamoto, “Bitcoin Whitepaper,” Satoshi Nakamoto, 2019. .

[4] R. Henry, A. Herzberg, and A. Kate, “Blockchain Access Privacy: Challenges and Directions,” IEEE Secur. Priv., vol. 16, no. 4, pp. 38–45, Jul. 2018.

[5] V. Buterin, “A Next Generation Smart Contract and Decentralized Application Platform,” Ethereum, 2014.

[6] G. Wood, “Ethereum: A Secure Decentralised Generalised Transaction Ledger,” gavwood, 2017.

[7] Cardano, “What Is Cardano?,” cardano, 2019.

[8] F. Casino, T. K. Dasaklis, and C. Patsakis, “A systematic literature review of blockchain-based applications: Current status, classification and open issues,” Telemat. Informatics, vol. 36, pp. 55–81, Mar. 2019.

[9] X. Wang et al., “Survey on blockchain for Internet of Things,” Comput. Commun., vol. 136, pp. 10–29, Feb. 2019.

[10] A. Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito, “Blockchain and IoT Integration: A Systematic Survey,” Sensors, vol. 18, no. 8, p. 2575, Aug. 2018.

[11] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008. .

[12] Coindesk, “How do Bitcoin Transactions Work?,” Coindesk, 2018. .

[13] O. Wyman, “Blockchain in capital markets,” 2016.

[14] M. Swan, “Blockchain,” O’Reilly Media, 2015.

[15] F. Tschorsch and B. Scheuermann, “Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies,” IEEE Commun. Surv. Tutorials, vol. 18, no. 3, pp. 2084–2123, 2016..

[16] Bitcoin, “Bitcoin Developer Guide,” Bitcoin, 2017.

[17] R. C. Merkle, “Protocols for Public Key Cryptosystems,” in 1980 IEEE Symposium on Security and Privacy, 1980, pp. 122–122.

[18] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton: Princeton University Press, 2016.

[19] M. Apostolaki, A. Zohar, and L. Vanbever, “Hijacking Bitcoin: Routing Attacks on Cryptocurrencies,” in 2017 IEEE Symposium on Security and Privacy (SP), 2017, pp. 375–392..

[20] W. Mougayar, The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology. New Jersey: John Wiley and Sons, 2016.

[21] M. Iansiti and K. R. Lakhani, “The truth about blockchain,” Harv. Bus. Rev., vol. 95, no. 1, pp. 118–127, 2017.

[22] Y. Lu, “The blockchain: State-of-the-art and research challenges,” J. Ind. Inf. Integr., Apr. 2019.

[23] D. E. Kouicem, A. Bouabdallah, and H. Lakhlef, “Internet of things security: A top-down survey,” Comput. Networks, vol. 141, pp. 199–221, Aug. 2018.

[24] N. M. Kumar and P. K. Mallick, “Blockchain technology for security issues and challenges in IoT,” Procedia Comput. Sci., vol. 132, pp. 1815–1823, 2018.

[25] Fabric, “Join GitHub today,” GitHub, Inc, 2019.

[26] Y. Rahulamathavan, R. C.-W. Phan, M. Rajarajan, S. Misra, and A. Kondoz, “Privacy-preserving blockchain based IoT ecosystem using attribute-based encryption,” in 2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), 2017, pp. 1–6.

[27] A. Dorri, S. Kanhere, and R. Jurdak, “Towards an Optimized BlockChain for IoT,” in 2017 IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI), 2017.

[28] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, “Blockchain for IoT security and privacy: The case study of a smart home,” in 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), 2017, pp. 618–623.

[29] G. Yang and C. Li, “A Design of Blockchain-Based Architecture for the Security of Electronic Health Record (EHR) Systems,” in 2018 IEEE International Conference on Cloud Computing Technology and Science (CloudCom), 2018, pp. 261–265.

[30] L. Mertz, “(Block) Chain Reaction: A Blockchain Revolution Sweeps into Health Care, Offering the Possibility for a Much-Needed Data Solution,” IEEE Pulse, vol. 9, no. 3, pp. 4–7, May 2018.

[31] D. Cohen, S. Keller, G. Hayes, D. Dorr, J. Ash, and D. Sittig, “Integrating patient-generated health data into clinical care settings or clinical decision-making: Lessons learned from project HealthDesign,” JMIR Hum Factors, 2016.

[32] A. E. Chung et al., “Harnessing person-generated health data to accelerate patient-centered outcomes research: the Crohn’s and Colitis Foundation of America PCORnet Patient Powered Research Network (CCFA Partners),” J. Am. Med. Informatics Assoc., vol. 23, no. 3, pp. 485–490, May 2016.

Retrieval Number: I33110789S319/2019©BEIESP
DOI: 10.35940/ijitee.I3311.0789S319

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

[33] E. Joffe et al., "Optimized dual threshold entity resolution for electronic health record databases--training set size and active learning," AMIA ... Annu. Symp. proceedings. AMIA Symp., vol. 2013, pp. 721–30, 2013.
[34] W. J. Gordon and C. Catalini, "Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability," Comput. Struct. Biotechnol. J., vol. 16, pp. 224–230, 2018.
[35] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," IEEE Commun. Surv. Tutorials, vol. 17, no. 4, pp. 2347–2376, 2015.
[36] D. Evans, "The internet of things: How the next evolution of the internet is changing everything," Cisco, 2011. .
[37] S. Sicari, A. Rizzardi, D. Miorandi, and A. Coen-Porisini, "Internet of Things: Security in the Keys," in Proceedings of the 12th ACM Symposium on QoS and Security for Wireless and Mobile Networks - Q2SWinet '16, 2016, pp. 129–133.
[38] Internet Society, "The Internet of Things: An Overview: Understanding the Issues and Challenges of a More Connected World," Internet Society, 2015.
[39] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities," Futur. Gener. Comput. Syst., vol. 88, pp. 173–190, Nov. 2018.
[40] M. Díaz, C. Martín, and B. Rubio, "State-of-the-art, challenges, and open issues in the integration of Internet of things and cloud computing," J. Netw. Comput. Appl., vol. 67, pp. 99–117, May 2016.
[41] J. C. Buzby and T. Roberts, "The Economics of Enteric Infections: Human Foodborne Disease Costs," Gastroenterology, vol. 136, no. 6, pp. 1851–1862, May 2009.
[42] H. Malviya, "How Blockchain will Defend IOT," SSRN, 2016.
[43] P. Veena, S. Panikkar, S. Nair, and P. Brody, "Empowering the edge-practical insights on a decentralized internet of things," 2015.
[44] S. Gan, "An IoT simulator in NS3 and a key-based authentication architecture for IoT devices using blockchain," Kanpur, 2017.
[45] Blockchain of Things, "The Ultimate Blockchain Technology," 2017.
[46] Filament, "Filaments' blockchain technology creates new value for today's businesses," Filament, 2019.
[47] Modum, "Next Generation Supply Chain Automation and Intelligence: Trusted digital ecosystems powered by IoT Sensing and blockchain," 2017.
[48] G. Prisco, "Slock, it to Introduce Smart Locks Linked to Smart Ethereum Contracts, Decentralize the Sharing Economy," BTC, 2019.
[49] M. Samaniego and R. Deters, "Hosting Virtual IoT Resources on Edge-Hosts with Blockchain," in 2016 IEEE International Conference on Computer and Information Technology (CIT), 2016, pp. 116–119.
[50] LO3Energy, "Reshaping The Energy Future," 2018.
[51] Aigang, "Android device dataset," 2017.
[52] Mybit, "Leaders in Distributing Wealth," 2017.
[53] M. Aazam and E.-N. Huh, "Fog Computing and Smart Gateway Based Communication for Cloud of Things," in 2014 International Conference on Future Internet of Things and Cloud, 2014, pp. 464–470.
[54] Ethembedded, "Ethereum Computer Built On Embedded Devices," Ethembedded, 2017.
[55] Raspnode, "DIY Raspberry Pi Cryptocurrency Node," Raspnode, 2017.
[56] K. Wüst and A. Gervais, "Do you need a blockchain?," IACR Cryptol. EPrint Arch., 2017.
[57] Trusted IoT Alliance, "Securing IoT Products With Blockchain," 2017.
[58] Bitmain, "Ant Router R1-LTC The WiFi router that mines Litecoin," Bitmain, 2017.
[59] Ethraspbian, "Ethraspbian custom Image for NANOPC-T4," 2017. .
[60] I. Eyal, A. E. Gencer, E. G. Sirer, and R. van Renesse, "Bitcoin-NG: A Scalable Blockchain Protocol," in 13th USENIX Symposium on Networked Systems Design and Implementation (NSDI '16) is sponsored by USENIX, 2016, pp. 1–16.
[61] R. Roman, J. Lopez, and M. Mambo, "Mobile edge computing, Fog et al.: A survey and analysis of security threats and challenges," Futur. Gener. Comput. Syst., vol. 78, pp. 680–698, Jan. 2018.
[62] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," Comput. Networks, vol. 57, no. 10, pp. 2266–2279, Jul. 2013.
[63] J. Lopez, R. Rios, F. Bao, and G. Wang, "Evolving privacy: From sensors to the Internet of Things," Futur. Gener. Comput. Syst., vol. 75, pp. 46–57, Oct. 2017.
[64] M. Banerjee, J. Lee, and K.-K. R. Choo, "A blockchain future for internet of things security: a position paper," Digit. Commun. Networks, vol. 4, no. 3, pp. 149–160, Aug. 2018.
[65] I. Makhdoom, M. Abolhasan, H. Abbas, and W. Ni, "Blockchain's adoption in IoT: The challenges, and a way forward," J. Netw. Comput. Appl., vol. 125, pp. 251–279, Jan. 2019.
[66] L. Touati, Y. Challal, and A. Bouabdallah, "C-CP-ABE: Cooperative Ciphertext Policy Attribute-Based Encryption for the Internet of Things," in 2014 International Conference on Advanced Networking Distributed Systems and Applications, 2014, pp. 64–69.
[67] N. Oualha and K. T. Nguyen, "Lightweight Attribute-Based Encryption for the Internet of Things," in 2016 25th International Conference on Computer Communication and Networks (ICCCN), 2016, pp. 1–6.
[68] F. Guo, Y. Mu, W. Susilo, D. S. Wong, and V. Varadharajan, "CP-ABE With Constant-Size Keys for Lightweight Devices," IEEE Trans. Inf. Forensics Secur., vol. 9, no. 5, pp. 763–771, May 2014.
[69] X. Yao, Z. Chen, and Y. Tian, "A lightweight attribute-based encryption scheme for the Internet of Things," Futur. Gener. Comput. Syst., vol. 49, pp. 104–112, Aug. 2015.
[70] J. Su, D. Cao, B. Zhao, X. Wang, and I. You, "ePASS: An expressive attribute-based signature scheme with privacy and an unforgeability guarantee for the Internet of Things," Futur. Gener. Comput. Syst., vol. 33, pp. 11–18, Apr. 2014.
[71] D. Thatmann, S. Zickau, A. Forster, and A. Kupper, "Applying Attribute-Based Encryption on Publish Subscribe Messaging Patterns for the Internet of Things," in 2015 IEEE International Conference on Data Science and Data Intensive Systems, 2015, pp. 556–563.
[72] W. Chen, "An IBE-based security scheme on Internet of Things," in 2012 IEEE 2nd International Conference on Cloud Computing and Intelligence Systems, 2012, pp. 1046–1049.
[73] Y. Mao, J. Li, M.-R. Chen, J. Liu, C. Xie, and Y. Zhan, "Fully secure fuzzy identity-based encryption for secure IoT communications," Comput. Stand. Interfaces, vol. 44, pp. 117–121, Feb. 2016.
[74] D. Evans and D. M. Eyers, "Efficient Data Tagging for Managing Privacy in the Internet of Things," in 2012 IEEE International Conference on Green Computing and Communications, 2012, pp. 244–248.
[75] R. Zhang, Y. Zhang, and K. Ren, "Distributed Privacy-Preserving Access Control in Sensor Networks," IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 8, pp. 1427–1438, Aug. 2012.
[76] A. Alcaide, E. Palomar, J. Montero-Castillo, and A. Ribagorda, "Anonymous authentication for privacy-preserving IoT target-driven applications," Comput. Secur., vol. 37, pp. 111–123, Sep. 2013.
[77] X. Huang, R. Fu, B. Chen, and T. Zhang, "User interactive internet of things privacy preserved access control," in in: 2012 International Conference for Internet Technology And Secured Transactions, 2012, pp. 597–602.
[78] A. F. Skarmeta, J. L. Hernandez-Ramos, and M. V. Moreno, "A decentralized approach for security and privacy challenges in the Internet of Things," in 2014 IEEE World Forum on Internet of Things (WF-IoT), 2014, pp. 67–72.
[79] S. Tonyali, O. Cakmak, K. Akkaya, M. M. E. A. Mahmoud, and I. Guvenc, "Secure Data Obfuscation Scheme to Enable Privacy-Preserving State Estimation in Smart Grid AMI Networks," IEEE Internet Things J., vol. 3, no. 5, pp. 709–719, Oct. 2016.
[80] Y. Maleh, A. Ezzati, and M. Belaissaoui, "DoS Attacks Analysis and Improvement in DTLS Protocol for Internet of Things," in Proceedings of the International Conference on Big Data and Advanced Wireless Technologies - BDAW '16, 2016, pp. 1–7.
[81] P. Kasinathan, C. Pastrone, M. A. Spirito, and M. Vinkovits, "Denial-of-Service detection in 6LoWPAN based Internet of Things," in 2013

Retrieval Number: I33110789S319/2019©BEIESP
DOI: 10.35940/ijitee.I3311.0789S319

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), 2013, pp. 600–607.
[82] F. M. de Almeida, A. de R. Ribeir, E. . Moreno, and C. A. Montesco, “Performance evaluation of an artificial neural network multilayer perceptron with limited weights for detecting denial of service attack on internet of things,” in AICT 2016 : The Twelfth Advanced International Conference on Telecommunications, 2016.
[83] P. Machaka, A. McDonald, F. Nelwamondo, and A. Bagula, “Using the Cumulative Sum Algorithm Against Distributed Denial of Service Attacks in Internet of Things,” in ICCASA 2015: Context-Aware Systems and Applications, Springer, 2016, pp. 62–72.
[84] D. Shreenivas, S. Raza, and T. Voigt, “Intrusion Detection in the RPL-connected 6LoWPAN Networks,” in Proceedings of the 3rd ACM International Workshop on IoT Privacy, Trust, and Security - IoTPTS ’17, 2017, pp. 31–38.
[85] T. Hardjono and N. Smith, “Cloud-Based Commissioning of Constrained Devices using Permissioned Blockchains,” in Proceedings of the 2nd ACM International Workshop on IoT Privacy, Trust, and Security - IoTPTS ’16, 2016, pp. 29–36.
[86] K. Gaurav, P. Goyal, V. Agrawal, and S. Rao, “Iot transaction security,” in 8th International Conference on the Internet of Things, 2015.
[87] S. H. Hashemi, F. Faghri, P. Rausch, and R. H. Campbell, “World of Empowered IoT Users,” in 2016 IEEE First International Conference on Internet-of-Things Design and Implementation (IoTDI), 2016, pp. 13–24.
[88] E. Kokoris-Kogias, L. Gasser, I. Khoffi, P. Jovanovic, N. Gailly, and B. Ford, “Managing Identities Using Blockchains and CoSi,” 2016.
[89] K. Biswas and V. Muthukkumarasamy, “Securing Smart Cities Using Blockchain Technology,” in 2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), 2016, pp. 1392–1393.
[90] O. Flauzac, C. Gonzalez, A. Hachani, and F. Nolot, “SDN Based Architecture for IoT and Improvement of the Security,” in 2015 IEEE 29th International Conference on Advanced Information Networking and Applications Workshops, 2015, pp. 688–693.
[91] P. Bull, R. Austin, E. Popov, M. Sharma, and R. Watson, “Flow Based Security for IoT Devices Using an SDN Gateway,” in 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), 2016, pp. 157–163.
[92] C. Vandana, “Security improvement in iot based on software defined networking,” Int. J. Sci. Eng. Technol ogy Res., vol. 5, no. 1, pp. 291–295, 2016.
[93] C. Gonzalez, S. M. Charfadine, O. Flauzac, and F. Nolot, “SDN-based security framework for the IoT in distributed grid,” in 2016 International Multidisciplinary Conference on Computer and Energy Science (SpliTech), 2016, pp. 1–5.
[94] P. Ruckebusch, E. De Poorter, C. Fortuna, and I. Moerman, “GITAR: Generic extension for Internet-of-Things ARchitectures enabling dynamic updates of network and application modules,” Ad Hoc Networks, vol. 36, pp. 127–151, Jan. 2016.
[95] A. Taherkordi, F. Loiret, R. Rouvoy, and F. Eliassen, “Optimizing Sensor Network Reprogramming via In-situ Reconfigurable Components,” ACM Trans. Sens. Networks, vol. 9, no. 2, pp. 1–38, 2013.
[96] M. Khan and K. Salah, “IoT security: Review, blockchain solutions, and open challenges,” Futur. Gener. Comput. Syst., 2018.
[97] C. Fernandez-Gago, F. Moyano, and J. Lopez, “Modelling trust dynamics in the Internet of Things,” Inf. Sci. (Ny)., vol. 396, pp. 72–82, Aug. 2017.
[98] C. Liu, R. Ranjan, C. Yang, X. Zhang, L. Wang, and J. Chen, “MuR-DPA: Top-Down Levelled Multi-Replica Merkle Hash Tree Based Secure Public Auditing for Dynamic Big Data Storage on Cloud,” IEEE Trans. Comput., vol. 64, no. 9, pp. 2609–2622, Sep. 2015.
[99] C. Liu, C. Yang, X. Zhang, and J. Chen, “External integrity verification for outsourced big data in cloud and IoT: A big picture,” Futur. Gener. Comput. Syst., vol. 49, pp. 58–67, Aug. 2015.
[100] C. Wang, Q. Wang, and K. Ren, “Privacy-preserving public auditing for data storage security in cloud computing,” in INFOCOM, 2010 Proceedings IEEE, 2010.
[101] V. Sapovadia, “Legal Issues in Cryptocurrency,” in Handbook of Digital Currency, Elsevier, 2015, pp. 253–266.
[102] R. Böhme, N. Christin, B. Edelman, and T. Moore, “Bitcoin: Economics, Technology, and Governance,” J. Econ. Perspect., vol. 29, no. 2, pp. 213–238, May 2015.
[103] R. Anderson, “Making Bitcoin Legal (Transcript of Discussion),” in Cambridge International Workshop on Security Protocols, Springer, 2018, pp. 254–265.
[104] A. Khanna, “Information Technology Act, 2000: International Perspective with special reference to Bitcoin,” Natl. J. Cyber Secur. Law, vol. 1, no. 1, 2018.
[105] R. Dorbala, O. Gautam, S. Pullabhatla, and G. N. P. V Babu, “The Orphaned Status of Cryptocurrencies in India,” ZENITH Int. J. Multidiscip. Res., vol. 8, no. 10, pp. 364–374, 2018.

Retrieval Number: I33110789S319/2019©BEIESP
DOI: 10.35940/ijitee.I3311.0789S319

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication