# BLOCKCHAIN AND INTERNET OF THINGS (BIoT)

A SEMINAR REPORT

submitted by

# AJAL SUNNY

## MGP17CS007

in partial fulfilment of the requirements for the award of the degree of

## Bachelor of Technology in

**Computer Science & Engineering**



**Department of Computer Science and Engineering Saintgits College of Engineering, Pathamuttom**

**APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY** November 2019

# DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING SAINTGITS COLLEGE OF ENGINEERING



**2019-2020**

## CERTIFICATE

***Certified that this is the bona fide record of seminar work entitled***

**Blockchain and Internet of Things (BIoT)**

*Submitted by*

## AJAL SUNNY (MGP17CS007)

**Under the guidance of**

**DR.JUBILANT J KIZHAKKETHOTTAM**

(Assistant Dean)

***In partial fulfilment of the requirements for award of the degree of Bachelor of Technology in Computer Science and Engineering under the APJ Abdul Kalam Technological University during the year 2019-2020***

## 

**HEAD OF DEPARTMENT SEMINAR COORDINATORS SEMINAR GUIDE**

**Dr. Anju Pratap (1) Er. Veena A Kumar Dr. Jubilant J**

**(2) Er. Jinu Thomas**

**ACKNOWLEDGEMENT**

I express my gratitude to our principal, **Dr. Jospehkunju Paul C**, Principal, Saintgits College of Engineering for providing us with excellent ambiance that laid potentially strong foundation for our work.

I express my heartfelt thanks to **Dr. M Wilscy,** Dean of CSE & IT and **Dr. Anju Pratap**, Head of the Department of Computer Science and Engineering, Saintgits College of Engineering who has been a constant support in every step of my seminar and the source of strength in completing this seminar.

I express my sincere thanks to **Er. Veena A Kumar and Er. Jinu Thomas** of the Computer Science and Engineering Department providing us all the facilities, valuable and timely suggestions and constant supervision for the successful completion of my seminar.

I also thank **Dr. Jubilant J,** Assistant Dean, Computer Science and Engineering Department for his supervision, encouragement, help and support.

I am highly indebted to all the faculties of the department for their valuable guidance and instant help and for being with us. I extend my heartfelt thanks to my parents, friends and well wishers for their support and timely help.

Last but not the least I thank Almighty God for helping me in successfully completing this seminar.

# ABSTRACT

The Internet of Things (IoTs) enables coupling of digital and physical objects using worthy communication technologies and introduces a future vision where computing systems, users and objects cooperate for convenience and economic benefits. Such a vision requires seamless security, data privacy, authentication and robustness against attacks. These attributes can be introduced by blockchain, a distributed ledger that maintains an immutable log of network transactions. In this paper, we present a comprehensive review on how to remodel blockchain to the specific IoT needs in order to develop Blockchain based IoT (BIoT) applications and aim to shape a coherent picture of the current state-of-the-art efforts in this direction. After describing the basic characteristics and requirements of IoT, evolution of blockchain is presented. In this regard, we start with the fundamental working principles of blockchain and how such systems achieve auditability, security and decentralization. Further, we describe the most relevant BIoT applications, its architecture design and security aspects. From there, we build our narrative on the centralized IoT challenges followed by recent advances towards solving them. Finally, some future directions are enumerated with the aim to guide future BIoT researchers on challenges that needs to be considered ahead of deploying the next generation of BIoT applications.

**TABLE OF CONTENTS**

## INDEX PAGE NO:

**Abstract**----------------------------------------------------------------------------------------------------------------- 4

List of Tables 6

List of Figures 7

1. Introduction 1
2. [Literature Review 2](#_TOC_250000)
3. **Technologies Used**
   1. IoT 3
   2. Blockchain - 5

## Why Blockchain? \_Proposed Architecture 13

* 1. Integration of Blockchain and IoT 3
  2. The beauty of blockchain - 5
  3. Blockchain platform for IoT 3
  4. Working model of Blockchain - 5
  5. Optimized Blockchain Architecture for IoT Applications 3

## BIoT: applications and current challenges 13

* 1. BIoT applications 3
  2. Current challenges related to BIoT applications - 5
     1. Energy efficiency 3

5.2.2 Security - 5

5.2.3 Privacy 3

5.2.4 Throughput and latency 3

* 1. Future research directions 3

## conclusion 13

**References** 14

**LIST OF TABLES**

**INDEX PAGE NO:**

4.1.4 The characteristic features of various proposed BIoT architecture in the literature------------9

# LIST OF FIGURES

## INDEX PAGE NO:

* 1. Generalized IoT architecture…………………………………………………………………3
  2. Blockchain Transaction Cycle 4

4.1.1 The basic Blockchain characteristics 5

4.1.3 Working model of Blockchain……………………………………………………………...9

4.1.4 Optimized Blockchain architecture for IoT...………………………………………………5

5.1 BIoT applications……………………………………………………………………………..7

# Chapter 1

# INTRODUCTION

A drastic increase in Internet of Things (IoT) devices in the market was reported in the past decade. Roughly the number of IoT devices introduced in market is approaching 25 billion and it is expected that this number may increase to 50 billion by the end of 2025. These devices have sensors to establish network connection and to enable collected information transmission to a remote node [1]. With the emergence of numerous technologies including embedded computing, sensors, actuators, cloud computing and wireless devices, many things in our routine life is becoming wirelessly interoperable with low-powered wireless devices like Radio Frequency Identification (RFID) tags. By enabling easy interaction with a wide range of things (or physical devices) such as monitoring sensors, home appliances, surveillance cameras, actuators, vehicles and so on, the IoT helps in development of many different applications like industrial automation, home automation, medical aids, intelligent energy management, mobile healthcare and smart grids. Enormous amount of data generated by objects are used by these applications to provide new services and serve citizens, public administration and companies. Huge number of events generated by these objects along with heterogeneous technologies of IoT throws light on new challenges in application development making the ubiquitous computing even more difficult [2]. The centralized IoT network architecture faces following challenges.

• In case of failure of the centralized server, there is a risk for the entire network infrastructure to get paralyzed and disrupted.

• Edward Snowden leaks makes it difficult for the adopters of IoT to trust partners who provide control and access allowing them to analyse the collected data.

• Accountability and traceability are not guaranteed for the data stored in centralized clouds as they rely on third party trust for storing and holding data [3].

• Owing to the exponential growth of IoT, the central server is no longer efficient enough for handling large amount of data as well as end to end communications. Moreover, due to existence of innumerable smart devices, maintenance is a problem as distributing regular software updates to all these devices is almost near to impossible.

• Closed source code also widens the lack of trust. Transparency is essential in order to foster security and trust therefore open source approaches needs to be considered for the development of next generation IoT solutions.

• Proposed IoT solutions are expensive owing to its high cost of maintenance and deployment of server farms and a centralized cloud. This cost becomes a burden for the middleman if the supplier does not create such an infrastructure.

These challenges make it necessary to rethink about the structuring of IoT. Currently, the most appropriate candidate technologies that can support a distributed IoT ecosystem is ‘‘blockchain’’. Blockchain technologies can carry out, coordinate and track transactions. These also enable creation of applications that possess no centralized cloud requirement and are able to store huge amount of information generated by several devices. Some companies such as IBM, labelled blockchain as technology that democratizes the future of IoT. Blockchain is a decentralized data management technology that had gained much significance in past few years when a group or anonymous user introduced Bitcoin—a blockchain-based digital currency application. A peer-to-peer self-sovereign blockchain system helps to achieve decentralization by chronologically time-stamping the transactions in a ledger. In [4], blockchain is recognised as the fifth disruptive computer paradigm innovation after internet, mobile networks, personal computers and mainframe. Blockchain based IoT (BIoT) have received enormous research interests and researchers are making efforts to decentralize IoT communications using blockchain. This is so because this integration has following benefits.

• This paradigm shift towards BIoT from the traditional centralized IoT systems enhances the fault tolerance and also prevents the inherent problem of bottleneck in centralized IoT servers.

• The end to end peer communications in a decentralized architecture need not utilize a centralized server for carrying out automation services thereby enabling the IoT device autonomy.

• The information transparency allows faster information exchange and transaction processing as the intermediate layer between the parties are eliminated.

• IoT event and data logs stored on blockchain are immutable and thereby guarantees traceability and accountability.

• Blockchain can treat IoT interactions as separate transactions as it offers programming logic functionality via use of smart contracts that helps to perform access control and enhance security, confidentiality and authentication in BIoT.

• Owing to tamper proof and secure storage, blockchains enable secure deployment of software updates to IoT devices.

# Chapter 2

# LITERATURE REVIEW

2.1 The blockchain mitigates the risk of network attacks, fraud via time stamping entries and single point of failure due to its distributed and decentralized nature. Further, the use of cryptographically linked chains enhances the security level and speed of transaction by manyfold. Owing to the widespread adoption of blockchain technology, there have been a number of previously published surveys that had focused on blockchain and IoT. These surveys are summarized as follows.

Christidis et al. [5] presented an extensive description of smart contracts and blockchain, and also presented a good overview on the deployment and applications of BIoT solutions. Even though the paper brings forth some useful information, it does not consider the possible optimizations that needs to be considered for creation of BIoT application. Zheng et al. [6] provided an extensive review on various mechanisms and the architecture of blockchain. However, it did not focus on applications of blockchain to IoT. Khan et al. [7] discussed how blockchain technology can be a key enabler to solve the most prominent IoT security issues. However, the work did not provide the detailed description of the working model of blockchain technology, phases of operations involved and the architectural design of an optimized blockchain for IoT applications. Reyna et al. [8] investigated the challenges in blockchain IoT integration analysing the unique features of blockchain technology and evaluating the performance of different blockchain in an IoT device.

2.2 There are very few comprehensive studies that sheds light on research and application of blockchain for IoT. In contrast to the works discussed in Sect. 2.1, this paper brings forth a holistic approach for application of blockchain for IoT scenarios and compares the available literature proposals that have focussed on integrating blockchain and IoT using 12 different attributes that are capable of providing an insight into the current research status. To the best of our knowledge, this survey is the first that thoroughly covers the architecture, requirements and threats to the IoT systems, background and working of blockchain, optimized BIoT architecture, Blockchain based IoT security solutions, and focuses on applications and challenges related to BIoT applications. The major contribution of this work is a detailed comprehensive discussion on the recent advances in IoT systems, blockchain technologies and decentralization of IoT systems using blockchain. Apart from exploring the basics of BIoT applications, this work also presents an extensive analysis on its optimization, deployment and development. A summary of contribution of this work is enumerated as below.

• Characteristics and requirements of an IoT ecosystem is discussed along with the analysis and categorization of various security threats with respect to the layered IoT architecture.

• Evolution, basic functioning, classification and working models of blockchain is presented in detail.

• Motivation for blockchain integration with IoT systems is discussed along with BIoT applications and the architecture design of an optimized BIoT applications.

• Recently proposed blockchain based solutions for ensuring privacy and security in IoT is reviewed.

• Current research challenges in decentralization of IoT using blockchain is presented in detail along with future research directions in the field.

# Chapter 3

# TECHNOLOGIES USED

## 3.1 IoT Overview

## Research and study in the field of IoT is in nascent stage as there is not even a single appropriate definition for IoT available yet. Three perspectives can broadly define IoT: Internet-oriented, Semantics-oriented, and Things-oriented [9]. IoT focuses on optimizing and transforming manual processes to make them part of the digital era, thereby facilitating the development of huge range of smart applications. Innovations in IoT has the potential to impact huge range of services and applications, such as industrial IoT, smart cities, smart agriculture, smart transport, smart homes, and retail IoT. The subsections below present a brief description on the generalized IoT architecture and its protocol stack, characteristics of IoT, requirements of IoT and the possible threats that can be launched at various layers of the IoT protocol stack.

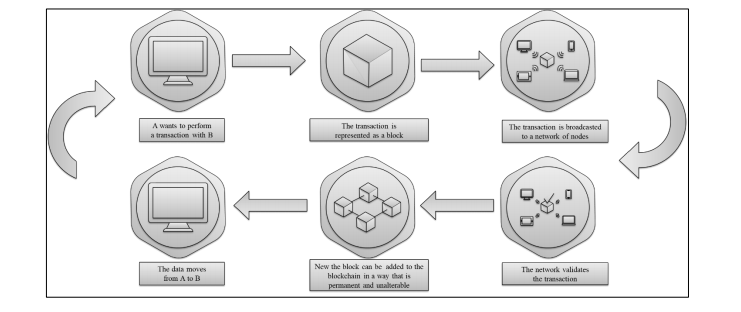
## Owing to the lack of standardization and consistency in IoT solutions across the globe, there are several emerging issues related to manageability, compatibility and interoperability. Non-uniformity in the presentation of layered protocol stack and IoT architecture have been observed in the literature. Kumar et al. presented IoT layers along with only a meagre detail of the associated protocols and their functionalities. Similarly, Granjal et al. [10] focused on communication protocols at different layers of IoT. Whereas, Fuqaha et al. [11] presented a tabular representation of the various technologies and elements that collectively form an IoT. Owing to the existence of this nonstandardization, it is believed that there exists no single universally accepted IoT reference model. In order to mitigate this uniformity, this section presents a generalized IoT architecture.

## 

## Numerous devices called ‘‘things’’ deployed in various topologies such as mesh, tree or clustered comprise an IoT ecosystem. ‘‘Things’’ are connected to gateways with the help of numerous IoT communication protocols such as RFID, BLE (Bluetooth Low Energy), WiFi, ZigBee, SigFox, LoRaWAN and 802.15.4. Connection between these gateway devices and the network server is realized using satellite link, OFC (Optical, Fibre Cable), LTE (Long Term Evolution) and 3G/4G. These network servers facilitate data analytics services to the users and their associated third parties including private and government organizations. Useful information and services such as industrial automation, environment monitoring, business intelligence, smart home autonomous services, health statistics and smart city sharing services are obtained from these processed data.

## 3.2 BLOCKCHAIN

## Blockchain is a digital ledger technology which is used to keep record of all transactions taking place on a peer to peer network.



A blockchain is a collection of blocks, where each block contains a hash of the previous block thereby creating a chain of blocks. The first block in the blockchain is called the genesis block from which the blockchain begins growing up to the most recent block. A single block comprises a series of transactions between various network members. The linked blocks forming a public ledger display all valid transactions. The transactions are mined into a block by miners before including it into blockchain. Individual blocks must include a PoW indicating consensus between the nodes on the transaction validity. A typical Blockchain transaction cycle is shown in Fig.3.1.

The concept behind blockchain is a mutual trust based on cryptographic PoW. A cryptographic proof of computational PoW was proposed in [12] using pricing functions for controlled access over a shared resource. This PoW idea later shaped the concept of mutual trust among several unknown participants sharing the resources. PoW-based micro-payment architecture for peer to peer file sharing was proposed in [13]. The proposed model with PoW was augmented with digital signatures and a ledger in order to keep all the historical record incompatible by malicious actors in the network. Later, Nakamoto introduced a similar PoW-based secured value token, which became popular as bitcoin’s decentralized public ledger-the blockchain. The blockchain has several possible benefits, rendering Bitcoin an electronically successful cash or cryptocurrency. The primary advantages can be listed as: 1) decentralized control and consensus; 2) transaction transparency; 3) distributed information; and 4) tamper-proof as mentioned in [14].

In order to convert new information into a block and include it in the current chain, a standard blockchain network requires a consensus algorithm among the participating nodes. There are different forms of consensus algorithms apart from PoW, such as proof-of-stake (PoS), delegated PoS (dPoS), proof of storage among others [15].

# Chapter 4

# Why Blockchain? \_ Proposed Architecture

# 4.1 Integration of blockchain and IoT

# Brody et al. [16] proposed the ever-expanding IoT device ecosystem to shift towards a decentralized architecture in order to maintain its sustainability. From the consumer’s perspective, there is lack of trust as well as need for ‘‘security through transparency’’ approach. Whereas, from the manufacturer’s side, there is huge maintenance cost associated with the current centralized model. These issues can be effectively countered by blockchain which itself is a trust less, scalable peer-to-peer network model capable of distributing data securely and operating transparently. In order to understand the complete working of this, consider a setup where all IoT devices operate on a single blockchain network. The smart contract deployed by the manufacturer facilitates to store the hash of the latest network firmware update [17]. The devices use the smart contract’s address or other discovery service to query the contract, receive new firmware updates and request them with its hash. The manufacturer’s own node serves the initial file requests but can stop serving once this binary propagates to some good number of nodes. The configured devices are assumed to share their received binary thereby enabling the retrieval of the firmware updates by even those devices that joins the network after the manufacturer has stopped participating. These do not require any user interaction and happens automatically. Furthermore, a cryptocurrency exchanging blockchain network paves a way for easy exchange of service between devices and also provides a convenient billing layer. In order to make some profit or sustain their infrastructure costs, these devices storing the binary copy may charge for serving it. Other examples include EtherAPIs [18] that helps to monetize API calls and Filecoin [19] that facilitates devices to lend their disk space on rent. With a cryptocurrency such as Ethereum or Bitcoin in place, every device receives proper compensation with the help of microtransactions for their usage. This is possible because every device can possess its own personal bank account and expose its resources to other devices.

# Integration of IoT and blockchain also facilitates the sharing of property and services. Slock.it introduces the concept of ‘‘Slocks’’ or smart electronic locks that can only be unlocked by the device that carries the appropriate token. On the same theme, the integration of IoT and blockchain in the energy sector facilitates peer-to-peer market place where machines are capable of buying and selling energy automatically on the basis of some userdefined criteria. For an instance, TransActive Grid brings forth the concept of peer-to-peer market for renewable energy supply in New York. The deployed solar panels record the excess output on a blockchain and sells them in the neighbourhood via smart contracts [20].

# The usefulness of blockchain and IoT integration can be seen in a typical supply chain example in which a container that is released from the manufacturing site (site A), gets consigned to the neighbouring port (site B) via railway, the gets shipped to the destination port (site C), is dispatched again to the distributors address (site D) and finally is received at the retailers site (site E). Therefore, the discussed process involves numerous checks and stakeholders along the way. In order to keep track of the asset, every stakeholder maintains their own database that they update on the basis of inputs received from other parties lying along the chain. A blockchain network introduced to track this asset is a shared database that comprise of cryptographically verified updates that is automatically propagated in order to create an auditable trial of information. Upon reaching the destination port, the shipping carrier sends a signed message to an agreed-upon, predefined smart contract such that everyone on the chain is aware of the current location of the container. The signed transaction acts as cryptographically verifiable receipt for the successful reception of the container at the destination port. The receiver also posts to the same smart contract in order to confirm its own possession with the container.

**4.1.1 The beauty of blockchain**

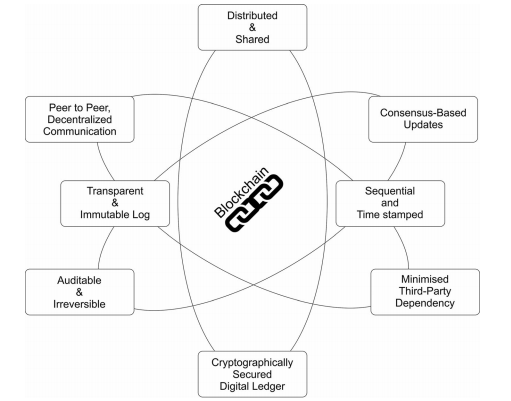
Numerous transformations have been reported in information and communication technology over the past few years that facilitates efficient, quicker, easier and secured data exchange. Digital communications emerged with an advent of internet and it empowers data exchange through financial online transactions for receiving funds and making payments. The entire communication and transactional system pass through a trusted intermediate that guarantees secure delivery of financial transactions. This trusted party is liable for any fraud, delayed data delivery and failures in data updating. Due to existence of one network controller, several questions pop up.

• What will happen if the trusted party is hacked and all its data is seized by the adversary?

• What will happen if the trusted party can no longer remain trusted and become rogue?

• Why not communicate using peer-to-peer (P2P) instead of an intermediary that introduces additional communication delays?

Blockchain provides solution to all these problems by putting forth the premiere decentralized cryptocurrency named bitcoin [21]. The transfer and exchange of bitcoin occurs using a shared distributed ledger that keeps track of all the transactions taking place within the network participants without any need of trusted centralized party. Bitcoin exploits the public key infrastructure of blockchain for controlling access and authenticating anonymous users. Owner digitally signs each transaction using a private key for source identification and authentication [22]. Figure depicts the basic blockchain characteristics.



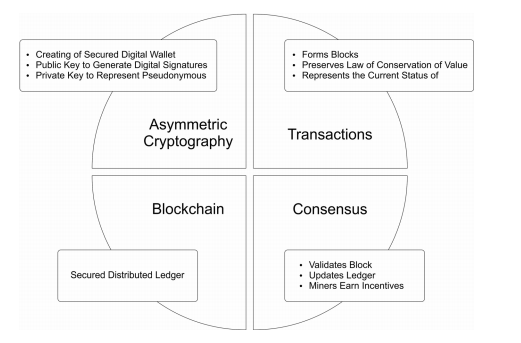
**4.1.2 Blockchain platforms for IoT**

In order to estimate the most suitable blockchain platform for IoT applications, comparison of the most widely accepted and prominent blockchain platforms including IOTA, Hyperledger-Fabric, Ethereum and Bitcoin is presented in this subsection. A block less distributed ledger and successor of blockchain called IOTA is designed specifically for enabling micropayments in industrial IoT. IOTA addresses the issues of high transaction fees and scalability. Before initiating its own transaction, every node in IOTA validates any two previous transactions without the need for miners to mine a valid transaction block. IOTA do not possess consensus finality therefore are prone to latency causing forks in transaction confirmation. Hyperledger fabric and Ethereum have different architecture than blockchain as it is designed for M2M interactions and offers fee-less transactions. The scalability issues of blockchain can also be solved to some extent by using these platforms. IoT systems are designed for numerous applications ranging from industrial control systems to smart watches. Hyperledger fabric and Ethereum can be used in these systems owing to its applicability to multiple blockchain applications.

**4.1.3 Working model of blockchain**

The fundamental components of blockchain network along with their significance are explored in this section. Then, the various phases of blockchain functionality are discussed in which these elements collaboratively carry out secure communication among distrusted nodes. Next, stepwise overview of the network operation is presented. Major blockchain functioning is illustrated considering the example of bitcoin blockchain.

The core components of the blockchain system include asymmetric cryptography, transactions, secured distributed ledger and consensus mechanisms as depicted in Fig



**Asymmetric key cryptography**

Strength of public key cryptography are utilized by the blockchain network for their secure operation. Users possess a digital wallet for data exchange which is secured using user’s private key. Private keys are kept secret from the user and functions to sign transactions digitally. The public key wallet functions as the address of the bitcoin known to all.

**Transactions**

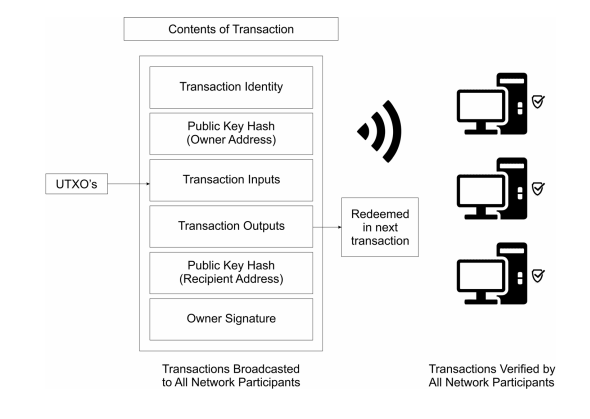
Information exchange and sharing among nodes are enabled by blockchain on a P2P basis. Source generates a file and broadcasts it to the entire network that contains transfer information. These transactions that are generated and congregated in blocks continuously by the nodes represent the current blockchain state.

**Consensus mechanism**

Nodes that utilize the blockchain platform for exchanging and sharing data do no possess a centralized authority to safeguard against security violations and resolve or regulate disputes. In order to ensure an unassailable exchange and keep track of the funds flow, there is a need of mechanism that can avoid frauds such as denial of service attacks and double-spending problem [23]. This mechanism of creating the blocks and adding them to the existing ledger is known as consensus mechanism. After the process of signature verification, the recipients might regain outputs several times in case of bitcoin. The regained outputs might be used in subsequent transactions.

**4.1.4 Optimized blockchain architecture for IoT applications**

Blockchain technology can bring forth numerous benefits to IoT. However, these are not explicitly devised to support IoT environments therefore various blockchain components needs to be optimized to make them adaptable to such environments. Several authors analysed the performance of BIoT under various scenarios by considering some influential aspects especially the consensus algorithms. Generally, IoT applications generate huge amount of traffic therefor the architecture supporting Blockchain based IoT applications must be adapted to handling huge traffic. This problem is more prominent in traditional cloud-based architecture where the node layer forwards the data to the cloud using IoT gateways. Moreover, these architectures also possess inherent vulnerabilities as the cloud is susceptible to failure due to software failures, human errors, external intrusions, maintenance problems or cyber-attacks [24]. Even if a single IoT device is compromised, the entire system breaks down due to Denial of Service attack, data altering, misleading systems or eavesdropping attack.



Following table presents, the characteristic features of various proposed BIoT architectures in the literature

|  |  |
| --- | --- |
| Proposed architecture | Characteristic features |
| Liao et al.[25] | Fully Distributed architecture must be followed by BIoT architectures |
| Dorri et al.[26] | Theoretical lightweight BIoT architecture that considers privacy and security issues |
| Daza et al.[27] | Blockchain based theoretical architecture that focusses on connecting heterogeneous devices and providing IoT services |
| Li et al.[28] | Multi-layered IoT architecture that focused on mitigating the blockchain deployment complexity by introducing different levels in IoT ecosystem |
| Samaniego et al.[29] | Evaluated the use of fog and cloud computing architectures for BIoT applications |

# Chapter 5

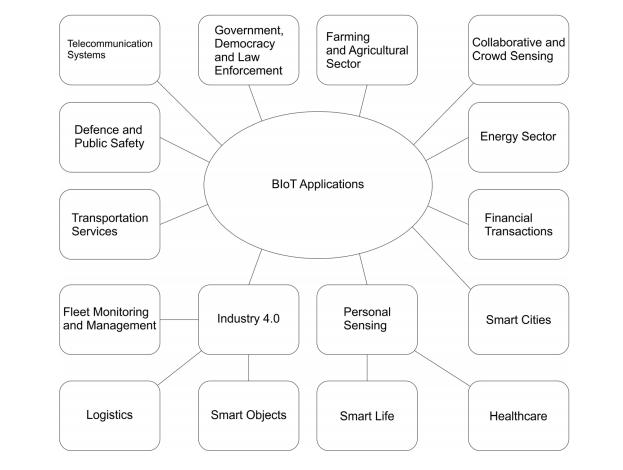
# BIoT: applications and current challenges

**5.1 BIoT applications**

Blockchain technology has the potential to be applied in many use cases and fields. The evolution of blockchain applicability initiated with Version 1.0 of Blockchain (Bitcoin), then evolved towards the Version 2.0 (Smart contracts) and later on shifted to Version 3.0 of Blockchain (Coordination and efficiency applications). Smart contracts can be defined as decentralized self-sufficient code pieces capable of being executed when some predefined conditions are satisfied. These smarts contracts have huge application areas including crowd funding, mortgages or international transfers [30]. Beyond smart contracts and cryptocurrencies, blockchain can be used in IoT application areas like sensing, cyber law, crowd sensing, wearables, timestamping services, identity management, intelligent transportation system [31], healthcare applications and smart living applications. Blockchain is also useful for IoT based agricultural applications. Tian et al. [32] proposed a traceability system based on blockchain and RFID that tracks Chinese agri-food products and aims to enhance the food safety as well as quality. Huh et al. proposed blockchain for managing IoT devices using a system capable of remotely configuring and controlling IoT devices. Authors also highlighted the significance of Ethereum as it facilitates bug corrections and simple maintenance.

Unification of blockchain and IoT also benefits the energy sector or the Internet of Energy (IoE). Lundqvist et al. [33] proposed a blockchain based system facilitating IoE/IoT devices to make payments without any human intervention. They described an implementation showing smart cable connected to smart socket for paying bills of the consumed electricity. Moreover, there is an existence of healthcare BIoT applications. Bocek et al. [34] proposed a traceability application that uses blockchain technology and IoT sensors to verify data accessibility and integrity in pharmaceutical supply chain. Shae et al. [35] proposed another healthcare BIoT application that makes use of blockchain based architecture for precision medicine and clinical trials. Salahuddin et al. [36] proposed a smart generic healthcare system that uses blockchain, fog and cloud computing, IoT devices and message brokers.

Blockchain technology can also enhance the low-level security of IoT. It improves the remote attestation process which is capable of verifying the trustworthiness of the Trusted Computer Base (TCB) associated with the device. This verification process is completed by managing the TCB measurements retrieved using a blockchain that stores these TCB measurements securely. Several other BIoT applications includes industrial processes and smart cities. Following figure depicts the various BIoT applications.



**5.2 Current challenges related to BIoT applications**

Several challenges are faced by emerging IoT ecosystem technologies such as 5G/4G broadband communication [37], telemetry systems, RFID and Cyber Physical Systems (CPSs). These challenges are more prominent and rise additional concerns in case of mission critical applications. Integration of blockchain to this brings forth additional technical and operational requirements owing to the complexity associated with the BIoT applications. The major factors that affect the BIoT application development is described in further subsections.

**5.2.1 Energy efficiency**

Owing to the resource constrained IoT end nodes, energy efficiency is of utmost importance for enabling long-lasting node deployment. However, blockchains are power hungry and incurs high energy consumption due to P2P communication and mining. Blockchains such as bitcoin consumes enormous electricity in the mining process due to involvement of consensus algorithm. P2P communications require continuously powered devices which may lead to energy wastage. Liao et al. [38] proposed energy efficient P2P protocols but this needs to be explored further for making it suitable for IoT networks.

**5.2.2 Security**

Three major security requirements that needs to be fulfilled to guarantee security in any information systems are confidentiality, integrity and availability. Validity of current IoT systems is preserved as long as system remains robust against leaks or attacks and centralized infrastructure administrators remain trusted. In contrast, a blockchain based applications are decentralized and the global system remains working even after some nodes are compromised. Guaranteeing internet security makes use of certificates that use public key infrastructure for preserving third part trusts. However, such authorities fail in certain circumstances. Data integrity is another essential component for IoT applications. Liu et al. [39] proposed integrity service framework that uses blockchain technologies instead of trusting a third party for cloud based IoT applications. Moreover, huge range of attacks in IoT systems might compromise its availability. Majority attack or 51 percent attack is the most feared attack for an IoT system. In such attack, entire blockchain can be controlled by one single miner to perform transactions at wish.

**5.2.3 Privacy**

Anonymity of blockchain users are not guaranteed as all the blockchain users are identified by their hash or public key and the transactions are shared for third parties to infer and analyse the actual user identities. Privacy in IoT environments is even more complex as private user data can be revealed by IoT devices. IoT applications suffer from identity certification problem. Kravitz et al. [40] proposed to use permissioned blockchains for managing and securing the IoT nodes thereby providing an identity management solution with rotating asymmetric keys capable of countering attacks. Access controls in a private blockchain assumes the access controller’s neutrality and reduces exposure. It also introduces added communication complexity. Zero knowledge proof is another scheme that avoids revealing of user identities during any transaction and thereby provides the desired level of authentication. Hayouni et al. [41] proposed to use homomorphic encryption scheme as another privacy preserving solution. It enables the transaction to be processed by third-party IoT services without the need of exposing the unencrypted data to them. However, the resource constrained nature of IoT devices makes the applicability of these techniques limited.

**5.2.4 Throughput and latency**

Deployment of an IoT might need a blockchain based architecture for managing huge number of transactions per unit time. However, this becomes a limitation for several networks such as bitcoins that can support not more than 7 transactions per second. However, Courtois et al. [42] proposed to increase this limit by modifying node behaviour and processing larger aspects. In terms of latency, the blockchain transactions consume more processing time. For an instance, block creation in bitcoin follows Poisson distribution and consumes more time. Even if it is capable of avoiding the double spending problems, merchants need to wait for a long time as before the transaction is confirmed, several blocks need to be added to the chain.

**5.3 Future research directions**

Apart from its huge range of advantages, blockchain also faces numerous challenges in its advances and its adoption in IoT. These challenges can be broadly classified into three categories: scalability, privacy preservation and utilization in resource constrained environment. These administrative trade-offs, challenges and future research scope towards blockchain integration in IoT are:

* Scalability issues in blockchain
* Constrained IoT edge device
* Blockchain infrastructure and complex technical challenges
* Cellular networks and blockchains for IoT
* Privacy concerns related to permission-less blockchains

# Chapter 6

# CONCLUSION

Technological advances of internet enabled world, rising competition for scarce resources and increased societal challenges accelerated the transformation to a data-driven world. Today’s IoT systems are lacking capability to defend themselves and are insecure majorly due to its resource constrained devices, immature standards, resources diversity, and the absence of secure hardware and software design, deployment, and development. In such systems, a centralized authorization, authentication and access models force the end users to trust a third party for processing, handling and managing their IoT data. In such an ecosystem, blockchain can offer a platform for sharing information to IoT that defies non-collaborative organizational structures. Blockchains achieve secure and immutable records using distributed consensus mechanisms thereby providing a trust-less record keeping environment. Further, blockchain is capable of providing a decentralized IoT fabric that needs no authorizing or managing intermediaries. However, one can easily fall into risks like amending any technology without adequately assuring its behaviour or applying it to the frameworks in which cost does not adequately compensate the improvement. Therefore, the benefits of applying blockchains to IoT systems needs careful analysis and caution.

# REFERENCES

[1] Nikoukar, A., Raza, S., Poole, A., Gunes, M., & Dezfouli, B. (2018). Low-power wireless for the internet of things: Standards and applications. IEEE Access, 6, 67893–67926. https://doi.org/ 10.1109/access.2018.2879189.

[2] Zarpela˜o, B. B., Miani, R. S., Kawakani, C. T., & Alvarenga, S. C. D. (2017). A survey of intrusion detection in Internet of Things. Journal of Network and Computer Applications, 84, 25–37. <https://doi.org/10.1016/j.jnca.2017.02.009>

[3] Brous, P., Janssen, M., & Herder, P. (2020). The dual effects of the internet of things (IoT): A systematic review of the benefits and risks of IoT adoption by organizations. International Journal of Information Management, 51, 101952. [https://doi.org/10. 1016/j.ijinfomgt.2019.05.008](https://doi.org/10.%201016/j.ijinfomgt.2019.05.008).

[4] . Swan, M. (2015). Blockchain: Blueprint for a new economy. Sebastopol, CA: O’Reilly Media.

[5] Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. IEEE Access, 4, 2292–2303. <https://doi.org/10.1109/access.2016.2566339>.

[6] . Zheng, Z., Xie, S., Dai, H., Chen, X., Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. In Proceedings of the IEEE international congress on big data (big data congress), Honolulu, United States, 25–30 June 2017 (pp. 557–564). https://doi.org/10.1109/ bigdatacongress.2017.85.

[7] Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems, 82, 395–411. https://doi.org/10.1016/j. future.2017.11.022.

[8] Reyna, A., Martı´n, C., Chen, J., Soler, E., & Dı´az, M. (2018). On blockchain and its integration with IoT. Challenges and opportunities. Future Generation Computer Systems, 88, 173–190. <https://doi.org/10.1016/j.future.2018.05.046>.

[9] Maharaja, R., Iyer, P., & Ye, Z. (2019). A hybrid fog-cloud approach for securing the internet of things. Cluster Computing. <https://doi.org/10.1007/s10586-019-02935-z>.

[10] . Granjal, J., Monteiro, E., & Silva, J. S. (2015). Security for the internet of things: A survey of existing protocols and open research issues. IEEE Communications Surveys & Tutorials, 17(3), 1294–1312. <https://doi.org/10.1109/comst.2015.2388550>

[11] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys & Tutorials, 17(4), 2347–2376. <https://doi.org/10.1109/comst.2015.2444095>.

[12] C. Dwork and M. Naor, "Pricing via processing or combatting junk mail,” in Proc. Annu. Int. Cryptol. Conf., 1992, pp. 139–147.

[13] V. Vishnumurthy, S. Chandrakumar, and E. G. Sirer, “KARMA: A secure economic framework for peer-to-peer resource sharing,” in Proc. Workshop Econ. Peer-to-peer Syst., vol. 35, no. 6, 2003, pp. 1–6.

[14] V. Buterin et al., "A next-generation smart contract and decentralized application platform,” White Paper, 2014.

[15] W. Li, S. Andreina, J.-M. Bohli, and G. Karame, "Securing proof-of-stake blockchain protocols," in Data Privacy Management, Cryptocurrencies and Blockchain Technology. Cham, Switzerland: Springer, 2017, pp. 297–315.

[16] . Brody, P., & Pureswaran, V. (2014). Device democracy: Saving the future of the Internet of Things. IBM Institute for Business Value, technical report, September 2014. [Online]. http:// www935.ibm.com/services/us/gbs/thoughtleadership/internetof things/.

[17] . Benet, J. (2015). Replication on IPFS—or, the backing-up content model. [Online]. <https://github.com/ipfs/faq/issues/47>.

[18] EtherAPIs: Decentralized, Anonymous, Trustless APIs, accessed on March 15, 2019. [Online]. <https://etherapis.io/>.

[19] Filecoin—A cryptocurrency operated file storage network [Online]. http://filecoin.io/. Accessed on March 15, 2019.

[20] . Rutkin, A. (2016). Blockchain-based microgrid gives power to consumers in New York [Online]. https://www.newscientist. com/article/2079334-blockchain-based-microgrid-gives-powerto-consumersin-new-york/.

[21] Jang, H., & Lee, J. (2018). An empirical study on modeling and prediction of bitcoin prices with bayesian neural networks based on blockchain information. IEEE Access, 6, 5427–5437. https:// doi.org/10.1109/access.2017.2779181.

[22] Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2017). A survey on the security of blockchain systems. Future Generation Computer Systems. https://doi.org/10.1016/j.future.2017.08.020.

[23] Karame, G. O., Androulaki, E., & Capkun, S. (2012). Doublespending fast payments in bitcoin. In Proceedings of the 2012 ACM conference on computer and communications security— CCS 12. <https://doi.org/10.1145/2382196.2382292>.

[24] . Wu, T., Tseng, Y., Huang, S., & Lai, Y. (2017). Non-repudiable provable data possession scheme with designated verifier in cloud storage systems. IEEE Access, 5, 19333–19341. https:// doi.org/10.1109/access.2017.2753243.

[25] Liao, C., Bao, S., Cheng, C., & Chen, K. (2017). On design issues and architectural styles for blockchain-driven IoT services. In 2017 IEEE international conference on consumer electronics—Taiwan (ICCE-TW). <https://doi.org/10.1109/iccechina.2017.7991140>.

[26] . Dorri, A., Kanhere, S. S., & Jurdak, R. (2017). Towards an optimized block chain for IoT. Proceedings of the Second International Conference on Internet-of-Things Design and Implementation - IoTDI. https://doi.org/10.1145/3054977. 3055003.

[27] Daza, V., Pietro, R. D., Klimek, I., & Signorini, M. (2017). CONNECT: CONtextual NamE disCovery for blockchain-based services in the IoT. In 2017 IEEE international conference on communications (ICC). https://doi.org/10.1109/icc.2017. 7996641.

[28] Li, C., & Zhang, L. (2017). A blockchain based new secure multi-layer network model for internet of things. In 2017 IEEE international congress on internet of things (ICIOT). https://doi. org/10.1109/ieee.iciot.2017.34.

[29] Samaniego, M., & Deters, R. (2016). Blockchain as a service for IoT. In 2016 IEEE international conference on internet of things (iThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (SmartData). https://doi.org/ 10.1109/ithings-greencom-cpscom-smartdata.2016.102.

[30] Swanson, T., Consensus-as-a-service: A brief report on the emergence of permissioned, distributed ledger system. http:// www.ofnumbers.com/wp-content/uploads/2015/04/Permis sioned-distributed-ledgers.pdf.

[31] Lei, A., Cruickshank, H., Cao, Y., Asuquo, P., Ogah, C. P., & Sun, Z. (2017). Blockchain-based dynamic key management for heterogeneous intelligent transportation systems. IEEE Internet of Things Journal, 4(6), 1832–1843. https://doi.org/10.1109/jiot. 2017.2740569.

[32] Tian, F. (2016). An agri-food supply chain traceability system for China based on RFID & blockchain technology. In 2016 13th international conference on service systems and service management (ICSSSM). https://doi.org/10.1109/icsssm.2016. 7538424.

[33] . Lundqvist, T., Blanche, A. D., & Andersson, H. R. (2017). Thing-to-thing electricity micro payments using blockchain technology. In 2017 global internet of things summit (GIoTS). <https://doi.org/10.1109/giots.2017.8016254>.

[34] . Bocek, T., Rodrigues, B. B., Strasser, T., & Stiller, B. (2017). Blockchains everywhere—A use-case of blockchains in the pharma supply-chain. In 2017 IFIP/IEEE symposium on integrated network and service management (IM). https://doi.org/ 10.23919/inm.2017.7987376. 203. Shae, Z., & Tsai, J. J. (2017)

[35] . Shae, Z., & Tsai, J. J. (2017). On the design of a blockchain platform for clinical trial and precision medicine. In 2017 IEEE 37th international conference on distributed computing systems (ICDCS). <https://doi.org/10.1109/icdcs.2017.61>.

[36] . Salahuddin, M. A., Al-Fuqaha, A., Guizani, M., Shuaib, K., & Sallabi, F. (2017). Softwarization of internet of things infrastructure for secure and smart healthcare. Computer, 50(7), 74–79. <https://doi.org/10.1109/mc.2017.195>.

[37] . Tello-Oquendo, L., Lin, S., Akyildiz, I. F., & Pla, V. (2019). Software-defined architecture for QoS-aware IoT deployments in 5G systems. Ad Hoc Networks. https://doi.org/10.1016/j. adhoc.2019.101911.

[38] . Liao, C., Cheng, S., & Domb, M. (2017). On designing energy efficient Wi-Fi P2P connections for internet of things. In 2017 IEEE 85th vehicular technology conference (VTC Spring). <https://doi.org/10.1109/vtcspring.2017.8108292>.

[39] . Liu, B., Yu, X. L., Chen, S., Xu, X., & Zhu, L. (2017). Blockchain based data integrity service framework for IoT data. In 2017 IEEE international conference on web services (ICWS). <https://doi.org/10.1109/icws.2017.54>.

[40] Kravitz, D. W., & Cooper, J. (2017). Securing user identity and transactions symbiotically: IoT meets blockchain. In 2017 global internet of things summit (GIoTS). https://doi.org/10.1109/ giots.2017.8016280.

[41] Hayouni, H., & Hamdi, M. (2016). Secure data aggregation with homomorphic primitives in wireless sensor networks: A critical survey and open research issues. In 2016 IEEE 13th international conference on networking, sensing, and control (ICNSC). <https://doi.org/10.1109/icnsc.2016.7479039>.

[42] . Courtois, N. T., Emirdag, P., & Nagy, D. A. (2014). Could bitcoin transactions be 100x faster? In Proceedings of the 11th international conference on security and cryptography. https:// doi.org/10.5220/0005102804260431.